Enterprise Mobility 8.1 Design Guide

Last Updated: 11/21/16

Cisco Systems, Inc.
www.cisco.com

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

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.

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: www.cisco.com/go/trademarks. 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. (1110R)

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

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Cisco Unified Wireless Network Solution Overview** 1-1
- WLAN Introduction 1-1
- WLAN Solution Benefits 1-1
- Requirements of WLAN Systems 1-2
- Cisco Unified Wireless Network 1-5

CHAPTER 2 **Cisco Unified Wireless Technology and Architecture** 2-1
- CAPWAP 2-1
  - Split MAC Architecture 2-3
  - Encryption 2-5
  - Layer 3 Tunnels 2-6
  - CAPWAP Modes 2-9
  - WLC Discovery & Selection 2-11
    - AP Priming 2-13
- Core Components 2-15
  - Cisco Wireless LAN Controllers 2-16
    - Cisco 2504 Wireless Controller 2-18
    - Cisco 5508 Wireless Controller 2-19
    - Cisco 5520 Wireless Controller 2-20
    - Cisco Flex 7500 Wireless Controller 2-21
    - Cisco 8510 Wireless Controllers 2-22
    - Cisco 8540 Wireless Controller 2-23
    - Cisco Wireless Services Module 2 2-24
    - Virtual Wireless LAN Controller 2-25
  - Cisco Aironet Access Points 2-26
    - Indoor 802.11n Access Points 2-26
    - Indoor 802.11ac Access Points 2-33
  - Cisco Prime Infrastructure 2-39
    - Licensing Options 2-40
    - Scaling 2-41
- High Availability 2-43
  - AP / Client Failover 2-43
    - N+1 Wireless Controller Redundancy 2-43

        - N+1 HA Wireless Controller Redundancy 2-44
        - HA Stateful Switchover Wireless Controller Redundancy 2-45
        - HA-SSO and N+1 Redundancy 2-52
    - Fast Restart 2-53
    - Link Aggregation (LAG) 2-53
        - Considerations 2-54
- Mobility Groups, AP Groups, RF Groups 2-55
    - Mobility Groups 2-55
        - Mobility Group Considerations 2-57
        - Mobility Group Applications 2-57
        - Mobility Group Exceptions 2-58
    - AP Groups 2-59
        - AP Group Considerations 2-60
        - AP Group Applications 2-61
    - RF Groups 2-64
- Roaming 2-66
    - IPv6 Client Mobility 2-69
    - Fast Secure Roaming 2-70
        - Cisco Centralized Key Management 2-70
        - Pairwise Master Key Caching 2-71
        - Proactive Key Caching 2-72
        - Opportunistic Key Caching 2-73
        - Fast Secure Roaming with 802.11r 2-74
        - Considerations 2-75
- Broadcast and Multicast on the WLC 2-77
    - WLC Broadcast and Multicast Details 2-78
        - DHCP 2-78
        - VideoStream 2-78
        - Other Broadcast and Multicast Traffic 2-79
- Design Considerations 2-80
    - WLC Location 2-80
        - Distributed WLC Deployment 2-80
        - Centralized WLC Deployment 2-81
        - Reference Architectures 2-82
    - Traffic Load and Wired Network Performance 2-92
        - Volume of CAPWAP Control Traffic 2-93
        - Overhead Introduced by Tunneling 2-93
        - Traffic Engineering 2-93
    - AP Connectivity 2-93

Operation and Maintenance 2-94
  WLC Discovery 2-94
  AP Distribution 2-94
  Best Practices 2-94

CHAPTER 3

WLAN RF Design Considerations 3-1

RF Basics 3-1
  Regulatory Domains 3-3
  Operating Frequencies 3-4
    2.4 GHz - 802.11b/g/n 3-4
    5 GHz - 802.11a/n/ac 3-7
  Understanding the IEEE 802.11 Standards 3-11
    Deployment Considerations 3-12
Planning for RF Deployment 3-18
  Different Deployment Types of WLAN Coverage 3-18
  Coverage Requirements 3-19
    High Density Client Coverage Requirements 3-19
    Roaming and Voice Coverage Requirements 3-21
    Location-Aware Coverage Requirements 3-22
  Power Level and Antenna Choice 3-23
    Omni-Directional Antennas 3-24
    Directional Antenna's 3-26
    RF Deployment Best Practices 3-28
Radio Resource Management - RRM 3-29
  What RRM Does 3-29
    RF Grouping 3-29
    Automatic RF Grouping 3-29
    DCA – Dynamic Channel Assignment 3-32
    TPC – Transmit Power Control 3-36
    CHDM- Coverage Hole Detection and Mitigation 3-38
    Coverage Hole Detection and Mitigation (CHDM) 3-38
  RF Profiles 3-40
  RF Power Terminology 3-48
    dB 3-48
    dBm 3-48
    dBi 3-49
    Effective Isotropic Radiated Power (EIRP) 3-49

CHAPTER 4 **Cisco Unified Wireless Network Architecture—Base Security Features** 4-1

    Secure Wireless Topology 4-1

  WLAN Security Mechanisms 4-2
    Wi-Fi Protected Access (WPA) 4-2
      Wi-Fi Protected Access 2 (WPA2) 4-3

  802.1X 4-3
    Authentication and Encryption 4-3
    Extensible Authentication Protocol 4-4
    Authentication 4-5
    Supplicants 4-5
    Authenticator 4-6
    Authentication Server 4-7

  Encryption 4-8
    TKIP Encryption 4-8
    Removal of TKIP from Wi-Fi® Devices 4-9
    AES Encryption 4-10
    Four-Way Handshake 4-11

  Proactive Key Caching (PKC) and CCKM 4-12

  Cisco Unified Wireless Network Architecture 4-14

  Cisco Unified Wireless Network Security Features 4-16
    Enhanced WLAN Security Options 4-17
      Local EAP Authentication 4-19
    ACL and Firewall Features 4-21
    Layer 2 Access Control Lists 4-24
    DNS-based Access Control Lists 4-25
      Restrictions on DNS-based Access Control Lists 4-26
    DHCP and ARP Protection 4-27
    Peer-to-Peer Blocking 4-27
    Wireless IDS 4-28
    Cisco Adaptive Wireless Intrusion Prevention System 4-29
      wIPS Communication Protocols 4-30
      wIPS Deployment Modes 4-30
      Dedicated Monitor Mode versus ELM 4-31
      On-Channel and Off-Channel Performance 4-32
      ELM Across WAN Links 4-33
      CleanAir Integration 4-33
      ELM wIPS Alarm Flow 4-34
      Cisco Adaptive wIPS Alarms 4-34
    Deployment Considerations - Required Components 4-35

      - How Many wIPS Access Points do I need? **4-36**
      - Access Point Density Recommendations **4-37**
      - wIPS Integrated in a Cisco Unified Wireless Network **4-37**
      - Forensics **4-38**
    - Client Exclusion **4-39**
    - Managing Rogue Devices and Policies **4-40**
      - Rogue Location Discovery Protocol **4-40**
      - Detecting Rogue Devices **4-41**
      - Rogue Detection Policies Parameters **4-42**
    - Rogue AP **4-46**
      - Air/RF Detection **4-47**
      - Location **4-48**
      - Wire Detection **4-48**
      - Switch Port Tracing **4-49**
      - Rogue AP Containment **4-49**
    - Management Frame Protection **4-49**
    - Management System Security Features **4-51**
      - Configuration Verification **4-51**
      - Alarms and Reports **4-52**
    - Cisco TrustSec SXP **4-52**
      - Restrictions for Cisco TrustSec SXP **4-53**
  - Password Policies **4-54**

CHAPTER **5**

Cisco Unified Wireless QoS and AVC **5-1**

- QoS and AVC Overview **5-1**
- Wireless QoS Deployment Schemes **5-2**
  - QoS Parameters **5-3**
  - Radio Upstream and Downstream QoS **5-4**
  - QoS and Network Performance **5-5**
- 802.11 Distributed Coordination Function **5-5**
  - Interframe Spaces **5-6**
  - Random Backoff **5-6**
  - aCWmin, aCWmax, and Retries **5-7**
- Wi-Fi Multimedia **5-8**
  - WMM Access **5-8**
  - WMM Classification **5-9**
  - WMM Queues **5-10**
    - Enhanced Distributed Channel Access **5-12**
    - Unscheduled-Automatic Power-save Delivery **5-14**

        - TSpec Admission Control 5-16
- Advanced QoS Features for WLAN Infrastructure 5-18
    - QoS Profiles 5-18
    - WMM Policy 5-21
    - Voice over IP Phones 5-22
    - Admission Control Parameters 5-23
        - Impact of TSpec Admission Control 5-26
- 802.11e, 802.1P and DSCP Mapping 5-27
    - QoS Baseline Priority Mapping 5-28
        - Deploying QoS Features on CAPWAP-based APs 5-29
        - WAN QoS and FlexConnect 5-29
- Guidelines for Deploying Wireless QoS 5-30
    - QoS LAN Switch Configuration Example 5-30
        - AP Switch Configuration 5-30
        - WLC Switch Configuration 5-30
    - Traffic Shaping, Over the Air QoS, and WMM Clients 5-31
    - WLAN Voice and Cisco Phones 5-31
- CAPWAP over WAN Connections 5-31
    - CAPWAP Traffic Classification 5-32
        - CAPWAP Control Traffic 5-32
        - CAPWAP 802.11 Traffic 5-33
    - Classification Considerations 5-33
        - Router Configuration Examples 5-34
- QoS Mapping in Release 8.1 MR1 5-35
    - Configuring QoS Mapping by Controller administrator 5-36
    - Configuring QoS Mapping from CLI 5-36
        - Configuring QOS Maps on Cisco AireOS Release 8.1 MR1 5-38
- Application Visibility and Control 5-41
    - NBAR Supported Feature 5-42
    - AVC Configuration Options 5-44
    - AVC and QoS Interaction on the WLAN 5-45
    - AVC Operation with Anchor/Foreign Controller Setup 5-45
        - Application Rate Limiting Through AVC 5-46
        - AVC Monitoring 5-47
    - Application Visibility and Control for FlexConnect 5-48
        - How AVC Works on FlexConnect AP 5-48
        - AVC FlexConnect Facts and Limitations 5-49
    - NBAR NetFlow Monitor 5-49

CHAPTER 6 Cisco Unified Wireless Multicast Design 6-1

Introduction 6-1

Overview of IPv4 Multicast Forwarding 6-1
  Wireless Multicast Roaming 6-3
    Asymmetric Multicast Tunneling 6-3

Multicast Enabled Networks 6-4
  CAPWAP Multicast Reserved Ports and Addresses 6-4
  Enabling IPv4 Multicast Forwarding on the Controller 6-5
    Enabling IPv4 Multicast Mode (GUI) 6-5
    Information About Multicast Mode 6-7

Multicast Deployment Considerations 6-8
  Recommendations for Choosing a CAPWAP Multicast Address 6-8
  Fragmentation and CAPWAP Multicast Packets 6-8
    All Controllers have the Same CAPWAP Multicast Group 6-9
    Controlling Multicast on the WLAN Using Standard Multicast Techniques 6-9

How Controller Placement Impacts Multicast Traffic and Roaming 6-11

Additional Considerations 6-12

Information About 802.11v and Directed Multicast 6-12
  Enabling 802.11v Network Assisted Power Savings 6-12
  Directed Multicast Service 6-13
  BSS Max Idle Period 6-13
  Configuring 802.11v Network Assisted Power Savings (CLI) 6-13

Overview of IPv6 Multicast 6-13
  IPV6 Multicast Support on Wireless LAN Controllers 6-15
  Multicast Domain Name System – mDNS/Bonjour 6-16
  Information About Multicast Domain Name System 6-17
  Location Specific Services 6-19
  mDNS AP 6-20
  Restrictions for Configuring Multicast DNS 6-21

Introduction to Bonjour Policies and New Requirements 6-22
  Bonjour Service Groups 6-23
  Wired and Wireless Location Specific Services 6-24
  Device Access Policy Constructs and Rules 6-25
  Client Context Attributes in an mDNS Policy 6-25
  Access Policy Rules 6-26

CHAPTER 7 FlexConnect 7-1

  Supported Platforms 7-2

FlexConnect Terminology **7-2**
  - Switching Modes **7-2**
    - Local Switched **7-2**
    - Central Switched **7-2**
  - Operation Modes **7-3**
  - FlexConnect States **7-3**
    - Authentication-Central/Switch-Central **7-3**
    - Authentication Down/Switching Down **7-3**
    - Authentication-Central/Switch-Local **7-4**
    - Authentication-Down/Switch-Local **7-4**
    - Authentication-local/switch-local **7-5**

Applications **7-5**
  - Branch Wireless Connectivity **7-5**
  - Branch Guest Access **7-6**
  - Public WLAN Hotspot **7-6**
  - Wireless BYOD in Branch sites **7-7**

Deployment Considerations **7-8**
  - WAN Link **7-8**
  - Roaming **7-8**
  - Radio Resource Management **7-9**
  - Location Services **7-9**
  - QoS Considerations **7-10**

FlexConnect Solution **7-10**
  - Advantages of Centralizing Access Point Control Traffic **7-10**
  - Advantages of Distributing Client Data Traffic **7-10**
  - Central Client Data Traffic **7-11**
  - Primary Design Requirements **7-12**

FlexConnect Groups **7-12**
  - Configuring FlexConnect Groups **7-13**
  - Local Authentication **7-15**
  - Local EAP **7-16**
  - Support for PEAP and EAP-TLS Authentication **7-16**
  - CCKM/OKC Fast Roaming **7-16**

FlexConnect VLAN Override **7-17**
  - FlexConnect VLAN Override Summary **7-17**

FlexConnect VLAN Based Central Switching **7-17**
  - FlexConnect VLAN Central Switching Summary **7-17**

VLAN Name Override **7-18**
  - FlexConnect VLAN Name Override Summary **7-18**

FlexConnect ACL 7-19
  FlexConnect ACL Summary 7-19
  FlexConnect ACL Limitations 7-19
  Client ACL Support 7-19
FlexConnect Split Tunneling 7-19
  Split Tunnel Summary 7-20
  Split Tunnel Limitations 7-20
Fault Tolerance 7-20
  Fault Tolerance Summary 7-21
  Fault Tolerance Limitations 7-21
Peer-to-Peer Blocking 7-21
  P2P Summary 7-21
  P2P Limitations 7-21
FlexConnect WGB/uWGB Support for Local Switching WLANs 7-22
  FlexConnect WGB/uWGB Summary 7-22
  FlexConnect WGB/uWGB Limitations 7-22
FlexConnect Smart AP Image Upgrade 7-23
  Smart AP Image Upgrade Summary 7-23
VideoStream for FlexConnect Local Switching 7-23
Application Visibility and Control for FlexConnect 7-24
  AVC Facts and Limitations 7-24
General Deployment Considerations 7-25

CHAPTER 8 **Cisco Wireless Mesh Networking** 8-1
Mesh Access Points 8-2
  Access Point Roles 8-2
  Network Access 8-3
  Network Segmentation 8-4
  Cisco Indoor Mesh Access Points 8-4
  Cisco Outdoor Mesh Access Points 8-5
    Cisco Aironet 1570 Series Access Points 8-6
    Cisco Aironet 1530 Series Access Points 8-8
    Cisco Aironet 1552 Mesh Access Point 8-9
Cisco Wireless LAN Controllers 8-30
Cisco Prime Infrastructure 8-30
Architecture 8-31
  Control and Provisioning of Wireless Access Points 8-31
    CAPWAP Discovery on a Mesh Network 8-31

Dynamic MTU Detection 8-31
XML Configuration File 8-32
Adaptive Wireless Path Protocol 8-33
Mesh Neighbors, Parents, and Children 8-34
Mesh Deployment Modes 8-37
Wireless Backhaul 8-37
Universal Access 8-37
Point-to-Multipoint Wireless Bridging 8-37
Wireless Backhaul Data Rate 8-39
ClientLink Technology 8-39
Controller Planning 8-40
Wireless Mesh Network Coverage Considerations 8-41
Cell Planning and Distance 8-41
For the Cisco 1520 Series Access Points 8-41
Collocating Mesh Access Points 8-42
Collocating AP1500s on Adjacent Channels 8-42
Collocating AP1500s on Alternate Adjacent Channels 8-42
CleanAir 8-42
CleanAir Advisor 8-43
Wireless Mesh Mobility Groups 8-43
Multiple Controllers 8-43
Increasing Mesh Availability 8-44
Multiple RAPs 8-45
Indoor Mesh Interoperability with Outdoor Mesh 8-46
Connecting the Cisco 1500 Series Mesh APs to the Network 8-46
Adding Mesh APs to the Mesh Network 8-47

CHAPTER 9 **VoWLAN Design Recommendations** 9-1
Antenna Considerations 9-1
AP Antenna Selection 9-1
Antenna Orientation 9-2
General Recommendations 9-4
Antenna Positioning 9-5
Handset Antennas 9-5
Channel Utilization 9-6
Dynamic Frequency Selection and 802.11h Requirements of the APs 9-7
5 GHz Band Channels 9-7
Call Capacity 9-9
AP Call Capacity 9-12

Cell Edge Design 9-14
Dual Band Coverage Cells 9-16
Dynamic Transmit Power Control 9-17
  802.11r and 802.11k Features 9-18
  Interference Sources Local to the User 9-19

CHAPTER 10 Cisco Unified Wireless Network Guest Access Services 10-1

Introduction 10-1
Scope 10-2
Wireless Guest Access Overview 10-2
  Guest Access using the Cisco Unified Wireless Network Solution 10-2
WLAN Controller Guest Access 10-3
  Supported Platforms 10-3
  Auto Anchor Mobility to Support Wireless Guest Access 10-4
  Anchor Controller Deployment Guidelines 10-5
    Anchor Controller Positioning 10-5
    DHCP Services 10-6
    Routing 10-6
    Anchor Controller Sizing and Scaling 10-6
    Anchor Controller Redundancy N+1 10-7
  Anchor Controller Redundancy Priority 10-8
    Restrictions 10-8
    Deployment Considerations 10-8
    Examples 10-9
  Web Portal Authentication 10-9
    User Redirection 10-10
  Guest Credentials Management 10-11
    Local Controller Lobby Admin Access 10-12
  Guest User Authentication 10-12
    External Authentication 10-13
    Guest Pass-through 10-13
Guest Access Configuration 10-14
  Anchor WLC Installation and Interface Configuration 10-16
    Guest VLAN Interface Configuration 10-16
  Mobility Group Configuration 10-19
    Defining the Default Mobility Domain Name for the Anchor WLC 10-19
    Defining Mobility Group Members of the Anchor WLC 10-19
    Adding the Anchor WLC as a Mobility Group Member of a Foreign WLC 10-20
  Guest WLAN Configuration 10-21

        - Foreign WLC-Guest WLAN Configuration 10-22
    - Guest WLAN Configuration on the Anchor WLC 10-30
        - Anchor WLC-Guest WLAN Interface 10-31
- Guest Account Management 10-33
    - Guest Management Using the Management System 10-33
        - Using the Add Guest User Template 10-35
        - Using the Schedule Guest User Template 10-40
        - Managing Guest Credentials Directly on the Anchor Controller 10-45
        - Configuring the Maximum Number of User Accounts 10-47
        - Maximum Concurrent User Logins 10-48
        - Guest User Management Caveats 10-48
- Other Features and Solution Options 10-49
    - Web Portal Page Configuration and Management 10-49
        - Internal Web Page Management 10-49
        - Internal Web Certificate Management 10-51
    - Support for External Web Redirection 10-53
    - Anchor WLC-Pre-Authentication ACL 10-54
    - External Radius Authentication 10-56
        - Adding a RADIUS Server 10-56
- Verifying Guest Access Functionality 10-59

CHAPTER 11 **802.11r, 802.11k, 802.11v, 802.11w Fast Transition Roaming** 11-1

- 802.11r Fast Transition Roaming 11-1
    - Methods of Client Roaming 11-1
        - Over-the-Air Fast Transition Roaming 11-1
        - Over-the-Distribution System Fast Transition Roaming 11-4
    - Configuring Fast Transition Roaming using GUI 11-7
    - Configuring Fast Transition Roaming using CLI 11-9
    - Troubleshooting Support 11-10
    - Restrictions for 802.11r Fast Transition 11-10
- 802.11k Assisted Roaming 11-11
    - Assisted Roaming with 802.11k 11-11
        - Assembling and Optimizing the Neighbor List 11-11
        - 802.11k Information Elements (IEs) 11-11
        - Configuring Assisted Roaming using GUI 11-12
        - Configuring Assisted Roaming using CLI 11-13
    - Prediction Based Roaming-Assisted Roaming for Non-802.11k Clients 11-14
        - Configuring Prediction Based Roaming using GUI 11-14
        - Configuring Prediction Based Roaming using CLI 11-15

    - Neighbor List Response **11-16**
    - Troubleshooting Support **11-16**
- 802.11v Max Idle Period, Directed Multicast Service **11-17**
    - Enabling 802.11v Network Assisted Power Savings **11-17**
        - Directed Multicast Service **11-18**
        - Base Station Subsystem Maximum Idle Period **11-18**
    - Configuring 802.11v Network Assisted Power Savings using CLI **11-18**
    - Monitoring 802.11v Network Assisted Power Savings **11-18**
    - Troubleshooting Support **11-18**
- Managing 802.11v BSS Transition **11-19**
    - Configuring 802.11v BSS Transition Management using GUI **11-19**
    - Configuring 802.11v BSS Transition Management using CLI **11-20**
    - Troubleshooting 11v BSS transition **11-20**
    - Restrictions **11-21**
- 802.11w Protected Management Frames **11-21**
    - 802.11w Information Elements (IEs) **11-22**
    - Security Association Teardown Protection **11-23**
    - Configuring Protected Management Frames using GUI **11-24**
    - Configuring Protected Management Frames using CLI **11-27**
    - Monitoring 802.11w **11-28**
    - Troubleshooting Support **11-28**

CHAPTER 1

Cisco Unified Wireless Network Solution Overview

This chapter summarizes the benefits and characteristics of the Cisco Unified Wireless Network for the enterprise. The Cisco Unified Wireless Network solution offers secure, scalable, cost-effective wireless LANs for business critical mobility. The Cisco Unified Wireless Network is the industry's only unified wired and wireless solution to cost-effectively address the wireless LAN (WLAN) security, deployment, management, and control issues facing enterprises. This powerful indoor and outdoor solution combines the best elements of wired and wireless networking to deliver high performance, manageable, and secure WLANs with a low total cost of ownership.

WLAN Introduction

The mobile user requires the same accessibility, security, quality-of-service (QoS), and high availability currently enjoyed by wired users. Whether you are at work, at home, on the road, locally or internationally, there is a need to connect. The technological challenges are apparent, but to this end, mobility plays a role for everyone. Companies are deriving business value from mobile and wireless solutions. What was once a vertical market technology is now mainstream, and is an essential tool in getting access to voice, real-time information, and critical applications such as e-mail and calendar, enterprise databases, supply chain management, sales force automation, and customer relationship management.

WLAN Solution Benefits

Benefits achieved by WLANs include:

- *Mobility within buildings or campus*—Facilitates implementation of applications that require an always-on network and that tend to involve movement within a campus environment.
- *Convenience*—Simplifies networking of large, open people-areas.
- *Flexibility*—Allows work to be done at the most appropriate or convenient place rather than where a cable drop terminates. Getting the work done is what is important, not where you are.
- *Easier to set-up temporary spaces*—Promotes quick network setup of meeting rooms, war rooms, or brainstorming rooms tailored to variations in the number of participants.
- *Lower cabling costs*—Reduces the requirement for contingency cable plant installation because the WLAN can be employed to fill the gaps.

- *Easier adds, moves, and changes and lower support and maintenance costs*—Temporary networks become much easier to set up, easing migration issues and costly last-minute fixes.
- *Improved efficiency*—Studies show WLAN users are connected to the network 15 percent longer per day than hard-wired users.
- *Productivity gains*—Promotes easier access to network connectivity, resulting in better use of business productivity tools. Productivity studies show a 22 percent increase for WLAN users.
- *Easier to collaborate*—Facilitates access to collaboration tools from any location, such as meeting rooms; files can be shared on the spot and requests for information handled immediately.
- *More efficient use of office space*—Allows greater flexibility for accommodating groups, such as large team meetings.
- *Reduced errors*—Data can be directly entered into systems as it is being collected, rather than when network access is available.
- *Improved efficiency, performance, and security for enterprise partners and guests*—Promoted by implementing guest access networks.
- *Improved business resilience*—Increased mobility of the workforce allows rapid redeployment to other locations with WLANs.

Requirements of WLAN Systems

WLAN systems run either as an adjunct to the existing wired enterprise network or as a free-standing network within a campus or branch. WLANs can also be tied to applications, such as location-based services, in the retail, manufacturing, or health care industries. WLANs must permit secure, encrypted, authorized communication with access to data, communication, and business services as if connected to the resources by wire.

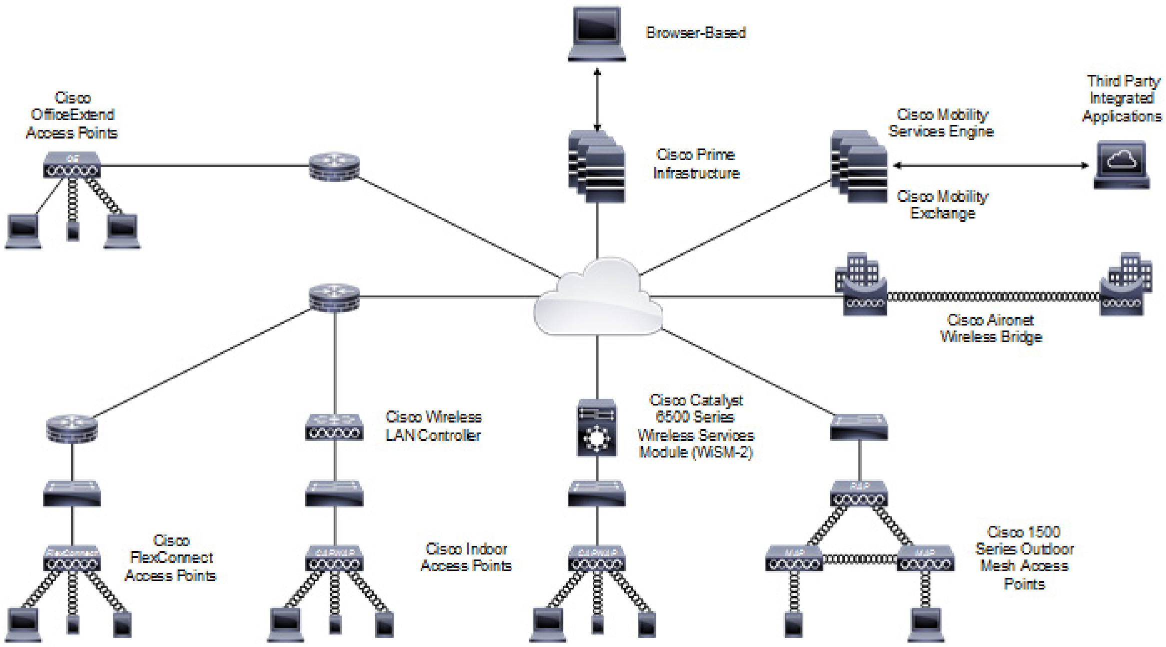
WLANs must be able to do the following:

- *Maintain accessibility to resources while employees are not wired to the network*—This accessibility enables employees to respond more quickly to business needs regardless of whether they are meeting in a conference room with a customer, at lunch with coworkers in the company cafeteria, or collaborating with a teammate in the next building.
- *Secure the enterprise from unauthorized, unsecured, or 'rogue' WLAN access points (APs)*—IT managers must be able to easily and automatically detect and locate rogue APs and the switch ports to which they are connected, active participation of both APs, and client devices that are providing continuous scanning and monitoring of the RF environment.
- *Extend the full benefits of integrated network services to nomadic users*—IP telephony and IP video-conferencing are supported over the WLAN using QoS, which by giving preferential treatment to real-time traffic, helps ensure that the video and audio information arrives on time. Firewall and Intruder Detection that are part of the enterprise framework are extended to the wireless user.
- *Segment authorized users and block unauthorized users*—Services of the wireless network can be safely extended to guests and vendors. The WLAN must be able to configure support for a separate public network—a guest network.
- *Provide easy, secure network access to visiting employees from other sites*—There is no need to search for an empty cubicle or an available Ethernet port. Users should securely access the network from any WLAN location. Employees are authenticated through IEEE 802.1x and Extensible Authentication Protocol (EAP), and all information sent and received on the WLAN is encrypted.

- *Easily manage central or remote APs*—Network managers must be able to easily deploy, operate, and manage hundreds to thousands of APs within the WLAN campus deployments and branch offices or retail, manufacturing, and health care locations. The desired result is one framework that provides medium-sized to large organizations the same level of security, scalability, reliability, ease of deployment, and management that they have come to expect from their wired LANs.
- *Enhanced Security Services*—WLAN Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) control to contain wireless threats, enforce security policy compliance, and safeguard information.
- *Voice Services*—Brings the mobility and flexibility of wireless networking to voice communications via the Cisco Unified Wired and Wireless network and the Cisco Compatible Extensions voice-enabled client devices.
- *Location Services* — Simultaneous tracking of hundreds to thousands of Wi-Fi and active RFID devices from directly within the WLAN infrastructure for critical applications such as high-value asset tracking, IT management, location-based security, and business policy enforcement.
- *Guest Access*— Provides customers, vendors, and partners with easy access to a wired and wireless LANs, helps increase productivity, facilitates real-time collaboration, keeps the company competitive, and maintains full WLAN security.

WLANs in the enterprise have emerged as one of the most effective means for connecting to a larger corporate network or to the internet. Figure 1-1 shows the elements of the Cisco Unified Wireless Network.

Figure 1-1 Cisco Unified Wireless Network Architecture in the Enterprise


Browser-Based
Cisco OfficeExtend Access Points
Cisco Prime Infrastructure
Cisco Mobility Services Engine
Third Party Integrated Applications
Cisco Mobility Exchange
Cisco Aironet Wireless Bridge
Cisco Wireless LAN Controller
Cisco Catalyst 6500 Series Wireless Services Module (WiSM-2)
Cisco FlexConnect Access Points
Cisco Indoor Access Points
Cisco 1500 Series Outdoor Mesh Access Points
FlexConnect
CAPWAP
CAPWAP
RAP
MAP
MAP

The interconnected elements that work together to deliver a unified enterprise-class wireless solution include:

- Client devices
- Access points (APs)
- Network unification through controllers
- World-class network management
- Mobility services

Beginning with a base of client devices, each element adds capabilities as the network needs evolve and grow, interconnecting with the elements above and below it to create a comprehensive, secure WLAN solution.

Cisco Unified Wireless Network

The core components of Cisco Unified Wireless Networks include the:

- Aironet access points (APs)
- Wireless LAN controller (WLC)
- Cisco Prime Infrastructure

For more information about the Cisco Unified Wireless Network, see:

http://www.cisco.com/go/unifiedwireless

Cisco Unified Wireless Technology and Architecture

This chapter discusses the key design and operational considerations associated with the deployment of Cisco Unified Wireless Networks enterprise.

This chapter discusses:

- CAPWAP
- Core Components
- Roaming
- Broadcast and Multicast on the WLC
- Design Considerations
- Operation and Maintenance

Much of the material in this chapter is explained in more detail in later chapters of this design guide. For more information on Cisco Unified Wireless Technology, see the Cisco White Paper on deployment strategies related to the Cisco 5500 Series Wireless LAN Controller at:

http://www.cisco.com/en/US/products/ps10315/prod_white_papers_list.html

CAPWAP

The Internet Engineering Task Force (IETF) standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) is the underlying protocol used in the Cisco Centralized WLAN Architecture (functional architecture of the Cisco Unified Wireless Network solution). CAPWAP provides the configuration and management of APs and WLANs in addition to encapsulation and forwarding of WLAN client traffic between an AP and a WLAN controller (WLC).

CAPWAP is based on the Lightweight Access Point Protocol (LWAPP) but adds additional security with Datagram Transport Layer Security (DTLS). CAPWAP uses the User Datagram Protocol (UDP) and can operate either over Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6). Table 2-1 lists the protocol and ports implemented for each CAPWAP version:

Table 2-1 CAPWAP Protocol and Ports

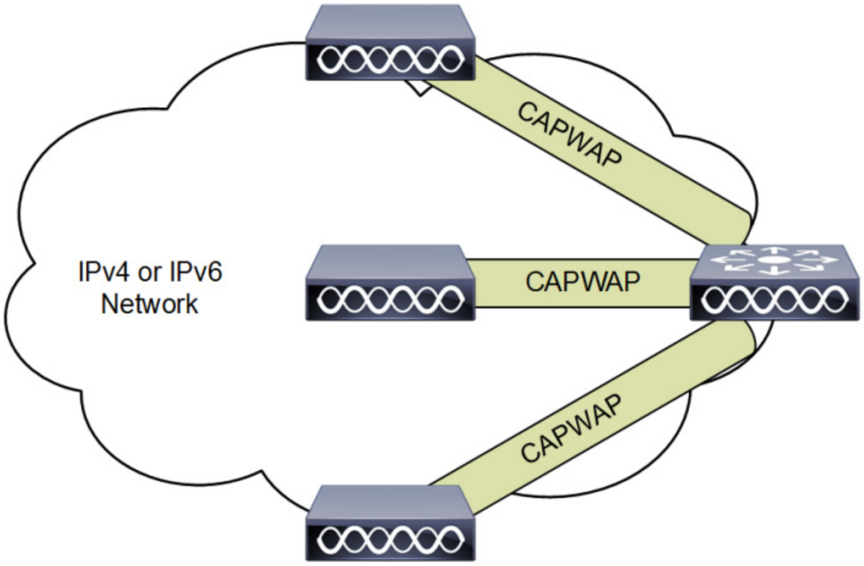
Internet Protocol	IP Protocol	DST Port	Description
Version 4	17 (UDP)	5,246	CAPWAPv4 Control Channel
	17 (UDP)	5,247	CAPWAPv4 Data Channel
Version 6	136 (UDP Lite)	5,246	CAPWAPv6Control Channel
	136 (UDP Lite)	5,247	CAPWAPv6 Data Channel

IPv6 mandates a complete payload checksum for User Datagram Protocol (UDP) which impacts the performance of the AP and the WLC. To maximize performance for IPv6 deployments, the AP and WLC implements UDP Lite that only performs a checksum on the header rather than the full payload.

Note In the Releases 5.2 and later, LWAPP has been depreciated and has been replaced by CAPWAP. Older LWAPP APs joining a WLC running on 5.2 or later will be automatically upgraded to support CAPWAP.

Figure 2-1 shows a high-level diagram of a basic centralized WLAN deployment, where CAPWAP APs connect to a WLC via the CAPWAP protocol. In Releases 8.0 and later, CAPWAP can operate either in an IPv4 or IPv6 transport modes. By default, IPv4 is preferred but is configurable (discussed later in this section).

Figure 2-1 CAPWAP APs connected to a WLC



Note Although CAPWAP is made up of a number of functional components, only those that influence the design and operation of a centralized WLAN network are discussed in this design guide.

Cisco recommends the following guidelines when implementing CAPWAP:

- IP Addressing—APs must be assigned a static or dynamic IPv4 / IPv6 address to be able to successfully discover and communicate with a WLC. Layer 2 mode is not supported by CAPWAP.
- Firewall Rules and ACLs—All firewall rules and ACLs defined on devices placed between the APs and WLCs must be configured to permit the CAPWAP protocol (see Table 2-1).
- IPv6 Deployments—At least one WLC should be configured for both IPv4 and IPv6 to support APs with older firmware that does not support IPv6.

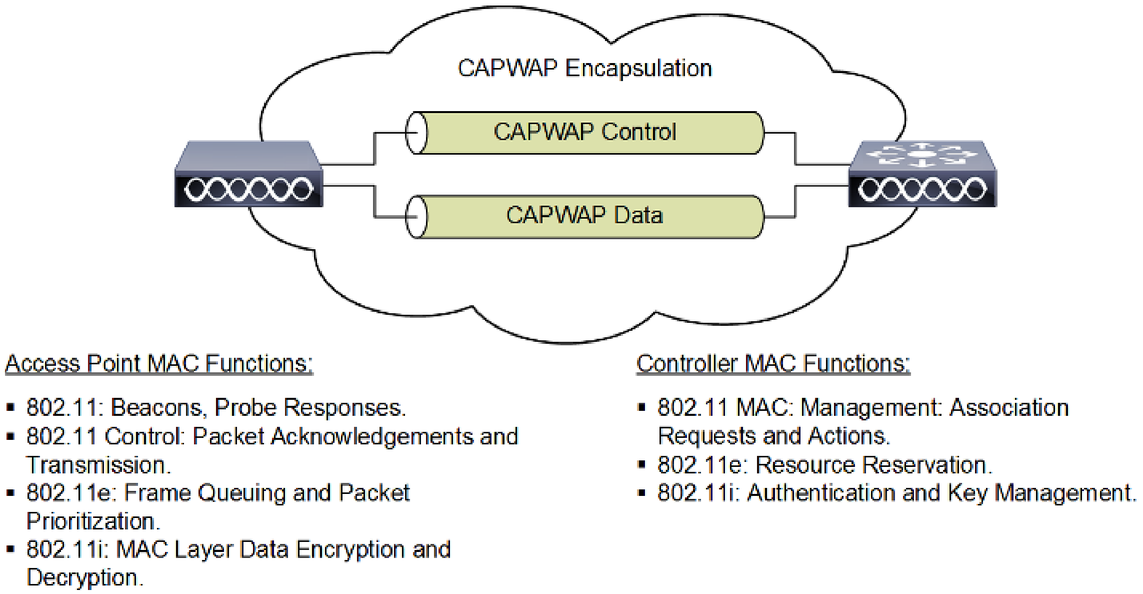
The key features of CAPWAP include:

- Split MAC Architecture
- Encryption
- Layer 3 Tunnels
- WLC Discovery & Selection

Split MAC Architecture

A key component of CAPWAP is the concept of a split MAC, where part of the 802.11 protocol operation is managed by the CAPWAP AP, while the remaining parts are managed by the WLC. Figure 2-2 shows the split MAC concept.

Figure 2-2 Split MAC Architecture



Access Point MAC Functions:

- 802.11: Beacons, Probe Responses.
- 802.11 Control: Packet Acknowledgements and Transmission.
- 802.11e: Frame Queuing and Packet Prioritization.
- 802.11i: MAC Layer Data Encryption and Decryption.

Controller MAC Functions:

- 802.11 MAC: Management: Association Requests and Actions.
- 802.11e: Resource Reservation.
- 802.11i: Authentication and Key Management.

A generic 802.11 AP, at the simplest level as shown in Figure 2-3, is nothing more than an 802.11 MAC-layer radio that bridges WLAN clients to a wired-network, based on association to a Basic Service Set Identifier (BSSID). The 802.11 standard extends the single AP concept (above) to allow multiple APs to provide an Extended Service Set (ESS), as shown in Figure 2-4, where multiple APs use the same ESS Identifier (ESSID, commonly referred to as an SSID) to allow a WLAN client to connect to a common network through more than one AP.

The CAPWAP split MAC concept in Figure 2-5 does all of the functions normally performed by individual APs and distributes them between two functional components:

- CAPWAP AP
- WLC

The two are linked across a network by the CAPWAP protocol and together provide equivalent radio/bridging services in a manner that is simpler to deploy and manage than individual APs.

Note Although split MAC facilitates Layer 2 connectivity between the WLAN clients and the wired interface of the WLC, this does not mean that the CAPWAP tunnel will pass all traffic. The WLC forwards only IP EtherType frames, and its default behavior is to not forward broadcast and multicast traffic. This is important to keep in mind when considering multicast and broadcast requirements in a WLAN deployment.

Figure 2-3 *Single AP*

Figure 2-4 *APs combined into a ESS*

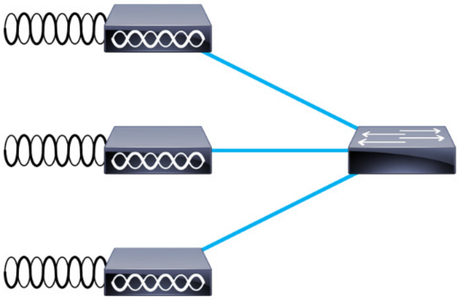
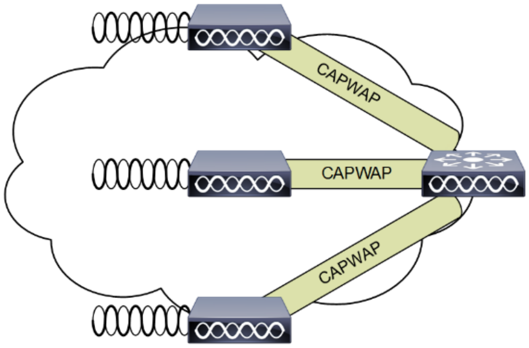


Figure 2-5 *CAPWAP Split-MAC ESS*



The simple, timing-dependent operations are generally managed locally on the CAPWAP AP, while more complex, less time-dependent operations are managed on the WLC.

For example, the CAPWAP AP handles:

- Frame exchange handshake between a client and AP.
- Transmission of beacon frames.
- Buffering and transmission of frames for clients in power save mode.
- Response to probe request frames from clients; the probe requests are also sent to the WLC for processing.
- Forwarding notification of received probe requests to the WLC.
- Provision of real-time signal quality information to the switch with every received frame.
- Monitoring each of the radio channels for noise, interference, and other WLANs.
- Monitoring for the presence of other APs.
- Encryption and decryption of 802.11 frames.

Other functionalities are also handled by the WLC. MAC layer functions provided by the WLC include:

- 802.11 authentication
- 802.11 association and re-association (mobility)
- 802.11 frame translation and bridging
- 802.1X/EAP/RADIUS processing
- Termination of 802.11 traffic on a wired interface, except in the case of FlexConnect APs (discussed later in this guide)

A CAPWAP tunnel supports two categories of traffic:

- CAPWAP control messages—Used to convey control, configuration, and management information between the WLC and APs.
- Wireless client data encapsulation—Transports Layer 2 wireless client traffic in IP EtherType encapsulated packets from the AP to the WLC.

When the encapsulated client traffic reaches the WLC, it is mapped to a corresponding interface (VLAN) or interface group (VLAN pool) at the WLC. This interface mapping is defined as part of the WLAN configuration settings on the WLC. The interface mapping is usually static, however a WLAN client may also be dynamically mapped to a specific VLAN based on the local policies defined on the WLC or RADIUS return attributes forwarded from an upstream AAA server upon successful authentication.

In addition to the VLAN assignment, other common WLAN configuration parameters include:

- SSID Name
- Operational State
- Radio Policies
- Authentication and Security Methods
- QoS / Application Visibility & Control
- Policy Mappings

Encryption

Releases 6.0 and later provide support for encrypting CAPWAP control and data packets exchanged between an AP and a WLC using DTLS. DTLS is an IETF protocol based on TLS. All Cisco access points and controllers are shipped with a Manufacturing Installed Certificate (MIC) which are used by an AP and WLC by default for mutual authentication and encryption key generation. Cisco also supports Locally Significant Certificates (LSC) to provide additional security for enterprises who wish to issue certificates from their own Certificate Authority (CA).

Note By default, DTLS uses a RSA 128-bit AES / SHA-1 cipher suite which is globally defined using the **config ap dtls-cipher-suite** command. Alternative ciphers include 256-bit AES with SHA-1 or SHA-256.

DTLS is enabled by default to secure the CAPWAP control channel but is disabled by default for the data channel. No DTLS license is required to secure the control channel. All CAPWAP management and control traffic exchanged between an AP and WLC is encrypted and secured by default to provide control plane privacy and prevent Man-In-the-Middle (MIM) attacks.

CAPWAP data encryption is optional and is enabled per AP. Data encryption requires a DTLS license to be installed on the WLC prior to being enabled on an AP. When enabled, all WLAN client traffic is encrypted at the AP before being forwarded to the WLC and vice versa. DTLS data encryption is automatically enabled for OfficeExtend APs but is disabled by default for all other APs. Most APs are deployed in a secure network where data encryption is not necessary. In contrast, traffic exchanged between an OfficeExtend AP and WLC is forwarded over an unsecured public network, where data encryption is important.

Note Please consult your Local Government regulations to ensure that DTLS encryption is permitted. For example, DTLS data encryption is currently prohibited in Russia.

The availability of DTLS data encryption on WLCs is as follows:

- Cisco 5508—Orderable with and without DTLS data support. Separate firmware images are provided on cisco.com with and without DTLS support.
- Cisco 2500, 5520, 8540, WiSM2, vWLC—Requires a separate license to activate DTLS data support.
- Cisco Flex 7500 and 8510—Includes DTLS data support built-in. You are not required to purchase or install a separate license to enable DTLS data support.

The availability of DTLS data encryption on APs is as follows:

- Cisco 1130, 1240 series—DTLS data encryption is performed in software.
- Cisco 1040, 1140, 1250, 1522, 1530, 1550, 1552, 1600, 1700, 1850, 2600, 2700, 3500, 3600 and 3700 series—DTLS data encryption is performed in hardware.

Note Enabling DTLS data encryption will impact the performance of both the APs and WLCs. Therefore DTLS data encryption should only be enabled on APs deployed over an unsecured network.

Layer 3 Tunnels

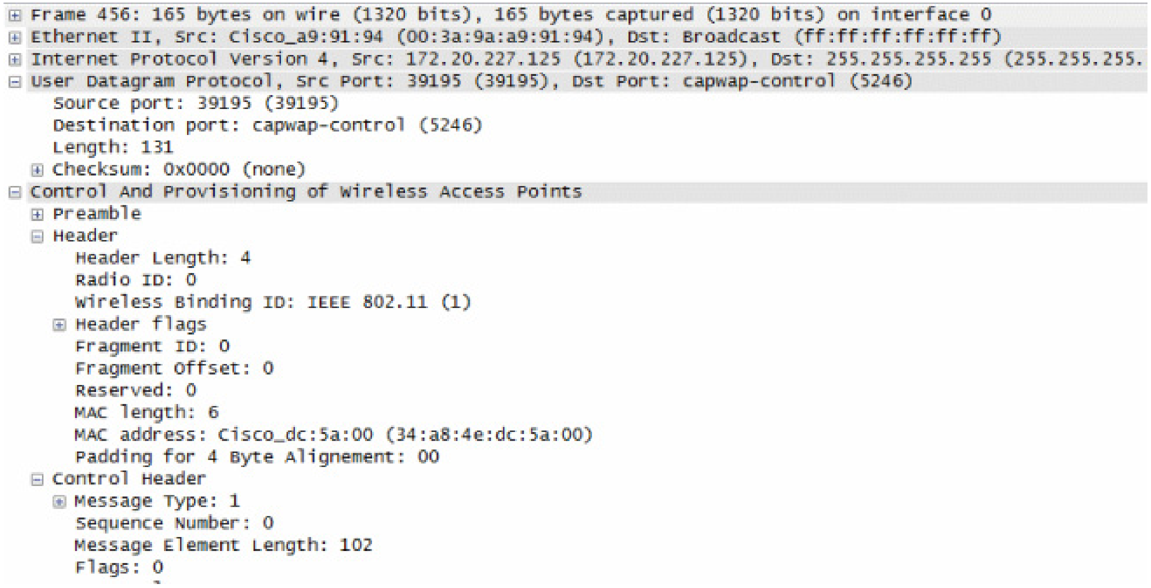
Unlike LWAPP which operated in either a Layer 2 or Layer 3 mode, CAPWAP only operates in Layer 3 and requires IP addresses to be present on both the AP and WLC. CAPWAP uses UDP for IPv4 deployments and UDP or UDP Lite (default) for IPv6 deployments to facilitate communication between an AP and WLC over an intermediate network. CAPWAP is able to perform fragmentation and reassembly of tunnel packets allowing WLAN client traffic to make use of a full 1500 byte MTU without having to adjust for any tunnel overhead.

Note In order to optimize the fragmentation and reassembly process, the number of fragments that the WLC or AP expect to receive is limited. The ideally supported MTU size for deploying the Cisco Unified Wireless Network is 1500 bytes, but the solution operates successfully over networks where the MTU is as small as 500 bytes.

The figures below are of CAPWAP packet captures used to illustrate CAPWAP operation over an IPv4 network. The sample decodes were captured using a Wireshark packet analyzer.

Figure 2-6 shows a partial decode of a CAPWAP control packet. This packet originates from the WLC using UDP destination port 5246 (as do all CAPWAP control packets from the WLC). Control Type 12 represents a configuration command used to pass AP configuration information to the CAPWAP AP by the WLC. CAPWAP control packet payloads are AES encrypted by default using DTLS when an AP joins the WLC.

Figure 2-6 CAPWAP Control Packet



```
⊞ Frame 456: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface 0
⊞ Ethernet II, Src: Cisco_a9:91:94 (00:3a:9a:a9:91:94), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 172.20.227.125 (172.20.227.125), Dst: 255.255.255.255 (255.255.255.
⊟ User Datagram Protocol, Src Port: 39195 (39195), Dst Port: capwap-control (5246)
    Source port: 39195 (39195)
    Destination port: capwap-control (5246)
    Length: 131
  ⊞ Checksum: 0x0000 (none)
⊟ Control And Provisioning of Wireless Access Points
  ⊞ Preamble
  ⊟ Header
      Header Length: 4
      Radio ID: 0
      Wireless Binding ID: IEEE 802.11 (1)
    ⊞ Header flags
      Fragment ID: 0
      Fragment Offset: 0
      Reserved: 0
      MAC length: 6
      MAC address: Cisco_dc:5a:00 (34:a8:4e:dc:5a:00)
      Padding for 4 Byte Alignement: 00
  ⊟ Control Header
    ⊞ Message Type: 1
      Sequence Number: 0
      Message Element Length: 102
      Flags: 0
```

Figure 2-7shows a partial decode of a CAPWAP packet containing an 802.11 probe request. This packet originates from the CAPWAP AP to the WLC using UDP destination port 5246 (as do all CAPWAP encapsulated 802.11 frames). In this example, Received Signal Strength Indication (RSSI) and Signal-to-Noise Ratio (SNR) values are also included in the CAPWAP packet to provide RF information to the WLC. Note that DTLS data encryption is not enabled in this example.

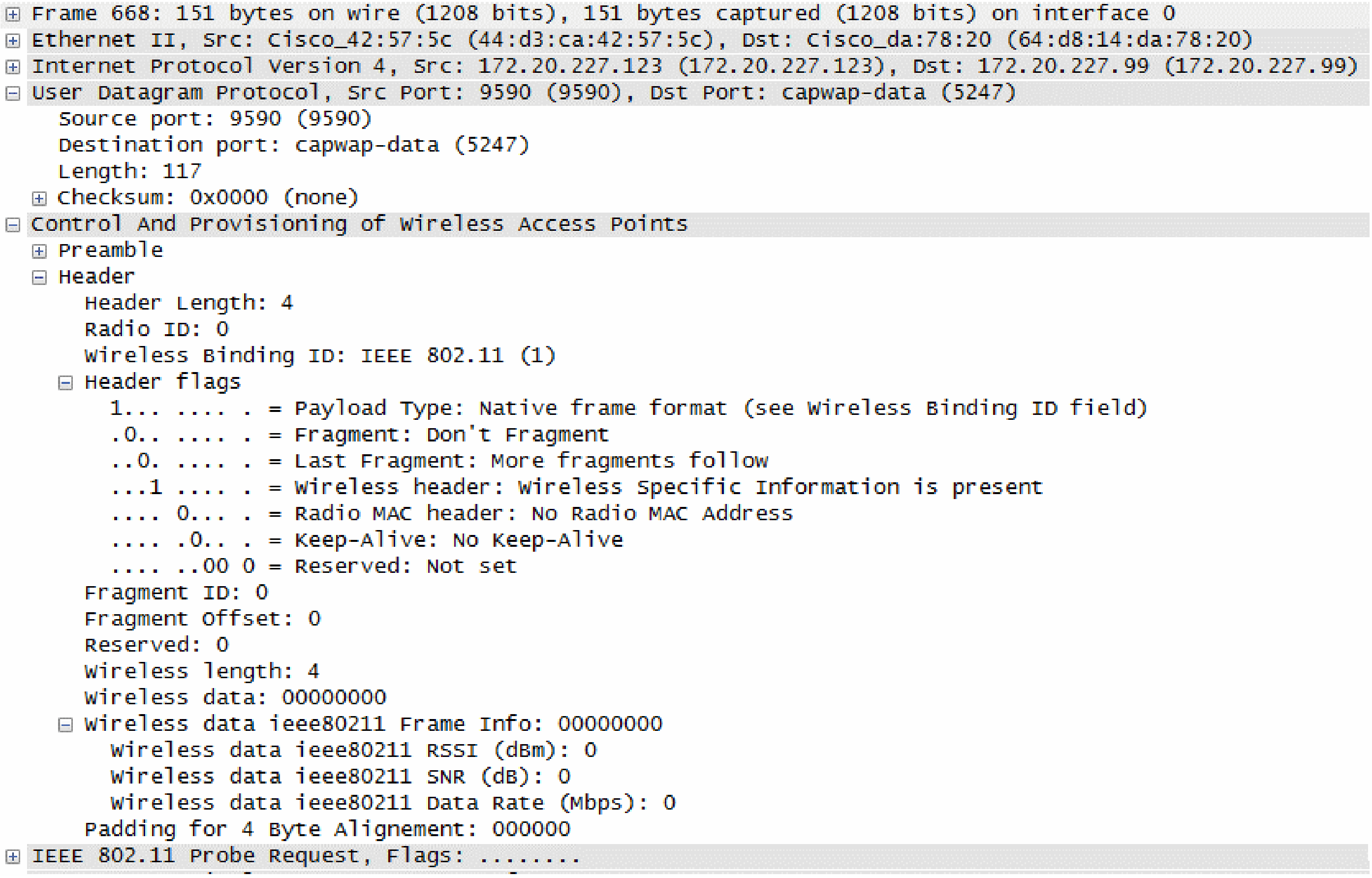


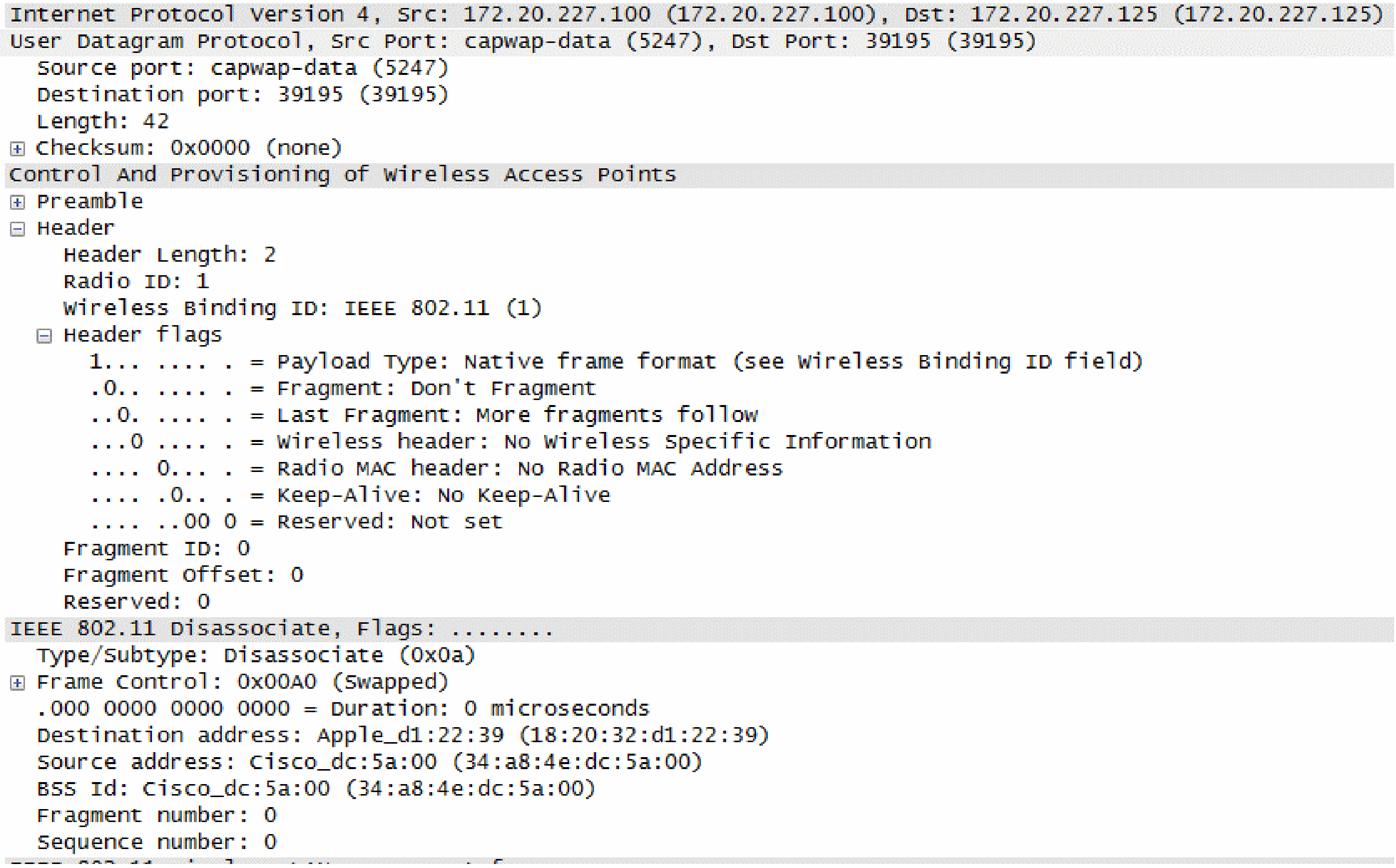
Figure 2-7 CAPWAP 802.11 Probe Request

```
⊞ Frame 668: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface 0
⊞ Ethernet II, Src: Cisco_42:57:5c (44:d3:ca:42:57:5c), Dst: Cisco_da:78:20 (64:d8:14:da:78:20)
⊞ Internet Protocol Version 4, Src: 172.20.227.123 (172.20.227.123), Dst: 172.20.227.99 (172.20.227.99)
⊟ User Datagram Protocol, Src Port: 9590 (9590), Dst Port: capwap-data (5247)
    Source port: 9590 (9590)
    Destination port: capwap-data (5247)
    Length: 117
  ⊞ Checksum: 0x0000 (none)
⊟ Control And Provisioning of Wireless Access Points
  ⊞ Preamble
  ⊟ Header
      Header Length: 4
      Radio ID: 0
      Wireless Binding ID: IEEE 802.11 (1)
    ⊟ Header flags
        1... .... . = Payload Type: Native frame format (see Wireless Binding ID field)
        .0.. .... . = Fragment: Don't Fragment
        ..0. .... . = Last Fragment: More fragments follow
        ...1 .... . = Wireless header: Wireless Specific Information is present
        .... 0... . = Radio MAC header: No Radio MAC Address
        .... .0.. . = Keep-Alive: No Keep-Alive
        .... ..00 0 = Reserved: Not set
      Fragment ID: 0
      Fragment Offset: 0
      Reserved: 0
      Wireless length: 4
      Wireless data: 00000000
    ⊟ Wireless data ieee80211 Frame Info: 00000000
        Wireless data ieee80211 RSSI (dBm): 0
        Wireless data ieee80211 SNR (dB): 0
        Wireless data ieee80211 Data Rate (Mbps): 0
      Padding for 4 Byte Alignement: 000000
⊞ IEEE 802.11 Probe Request, Flags: ........
```

Figure 2-8 shows another CAPWAP-encapsulated 802.11 frame, but in this case it is an 802.11 data frame, similar to that shown in Figure 2-7. It contains a complete 802.11 frame, as well as RSSI and SNR information for the WLC. This figure is shown to illustrate that an 802.11 data frame is treated the same by CAPWAP as the other 802.11 frames. Figure 2-8 highlights that fragmentation is supported for CAPWAP packets to accommodate the minimum MTU size between the AP and the WLC.

Note In the Wireshark decode, the frame control decode bytes have been swapped; this is accomplished during the Wireshark protocol analysis of the CAPWAP packet to take into account that some APs swap these bytes. DTLS data encryption is not enabled in this example.

Figure 2-8 CAPWAP Data Frame



```
Internet Protocol Version 4, Src: 172.20.227.100 (172.20.227.100), Dst: 172.20.227.125 (172.20.227.125)
User Datagram Protocol, Src Port: capwap-data (5247), Dst Port: 39195 (39195)
  Source port: capwap-data (5247)
  Destination port: 39195 (39195)
  Length: 42
⊞ Checksum: 0x0000 (none)
Control And Provisioning of Wireless Access Points
⊞ Preamble
⊟ Header
    Header Length: 2
    Radio ID: 1
    Wireless Binding ID: IEEE 802.11 (1)
  ⊟ Header flags
      1... .... . = Payload Type: Native frame format (see Wireless Binding ID field)
      .0.. .... . = Fragment: Don't Fragment
      ..0. .... . = Last Fragment: More fragments follow
      ...0 .... . = Wireless header: No Wireless Specific Information
      .... 0... . = Radio MAC header: No Radio MAC Address
      .... .0.. . = Keep-Alive: No Keep-Alive
      .... ..00 0 = Reserved: Not set
    Fragment ID: 0
    Fragment offset: 0
    Reserved: 0
IEEE 802.11 Disassociate, Flags: ........
  Type/Subtype: Disassociate (0x0a)
⊞ Frame Control: 0x00A0 (Swapped)
  .000 0000 0000 0000 = Duration: 0 microseconds
  Destination address: Apple_d1:22:39 (18:20:32:d1:22:39)
  Source address: Cisco_dc:5a:00 (34:a8:4e:dc:5a:00)
  BSS Id: Cisco_dc:5a:00 (34:a8:4e:dc:5a:00)
  Fragment number: 0
  Sequence number: 0
```

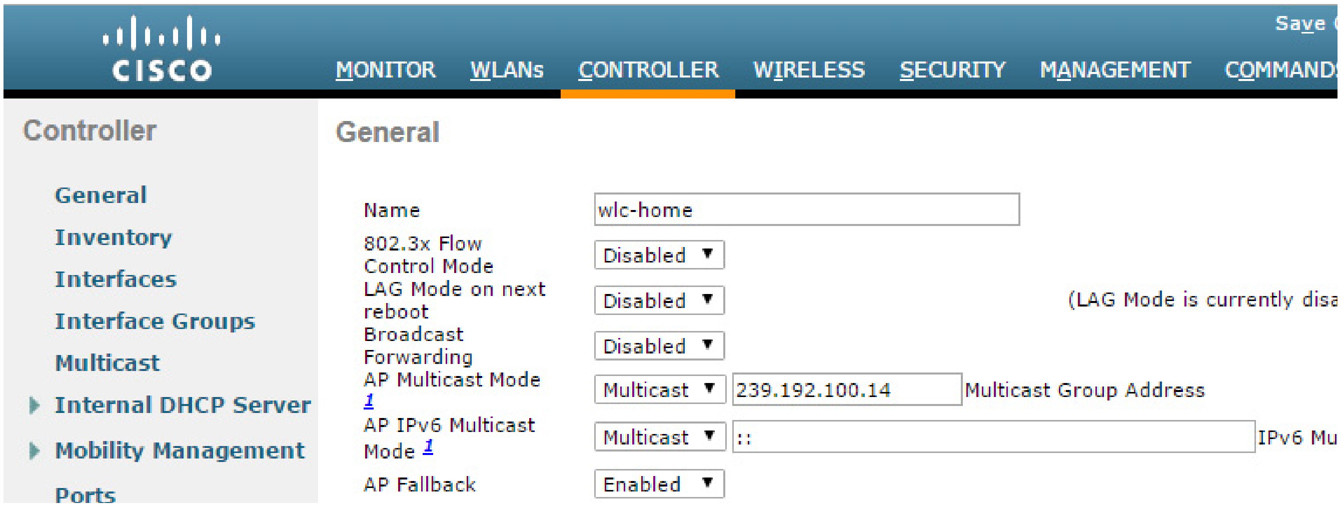
CAPWAP Modes

In the Releases 8.0 and later, Cisco Unified Wireless Network (CUWN) supports access points and controllers using IPv4 and/or IPv6 addressing. Network administrators can deploy APs and WLCs over a pure IPv4 or IPv6 network as well as dual-stack network to facilitate the transition from an IPv4 to IPv6. As part of the 8.0 Release, the CAPWAP protocol and discovery mechanisms have been enhanced to support IPv6. CAPWAP can now operate in IPv4 (CAPWAPv4) or IPv6 (CAPWAPv6) modes to suit the specific network environment.

To support both IP protocol versions, network administrators can configure a preferred CAPWAP mode (CAPWAPv4 or CAPWAPv6) through which an AP joins the WLC. The prefer-mode can be defined at two levels:

- Global Configuration (Figure 2-9)
- AP Group Specific (Figure 2-10)

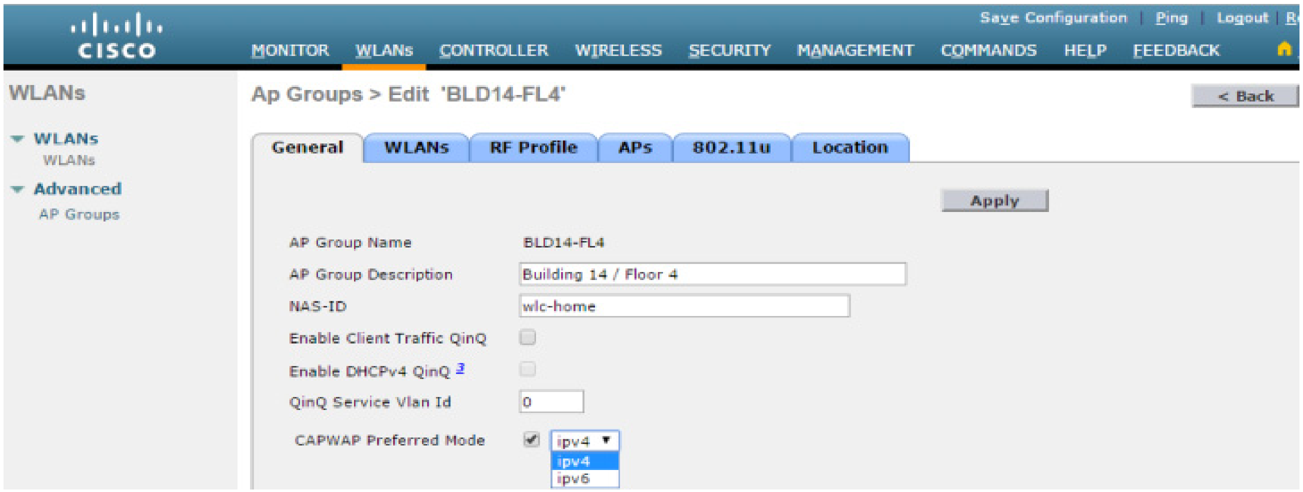
Figure 2-9 CAPWAP Prefer-Mode (Global Configuration)



General

Name: wlc-home
802.3x Flow Control Mode: Disabled
LAG Mode on next reboot: Disabled (LAG Mode is currently disa
Broadcast Forwarding: Disabled
AP Multicast Mode [1]: Multicast 239.192.100.14 Multicast Group Address
AP IPv6 Multicast Mode [1]: Multicast :: IPv6 Mu
AP Fallback: Enabled

Figure 2-10 CAPWAP Prefer-Mode (AP Group Specific)



Ap Groups > Edit 'BLD14-FL4'

AP Group Name: BLD14-FL4
AP Group Description: Building 14 / Floor 4
NAS-ID: wlc-home
Enable Client Traffic QinQ: ☐
Enable DHCPv4 QinQ [3]: ☐
QinQ Service Vlan Id: 0
CAPWAP Preferred Mode: ☑ ipv4 (ipv4, ipv6)

In the CAPWAP mode, the AP selects is dependent on various factors including the IP address versions implemented on both the AP and WLC, the primary / secondary / tertiary WLC addresses defined on the AP and the prefer-mode pushed to the AP.

The following outlines the CAPWAP operating mode configurations that are available:

- Default—The Global prefer-mode is set to IPv4 and the default AP Group prefer-mode is set to un-configured. By default an AP will prefer IPv4 unless the AP has been primes with a primary, secondary or tertiary WLC IPv6 address.
- AP-Group Specific—The prefer-mode (IPv4 or IPv6) is pushed to an AP only when the prefer-mode of an AP-Group is configured and the AP belongs to that group. If no prefer-mode is defined, the Global prefer-mode is inherited.
- Global—The prefer-mode is pushed to the default AP Group and all other AP-Groups on which the prefer-mode is not configured. Note that the prefer-mode cannot be manually defined on for the default AP Group.

- Join Failure—If an AP with a configured prefer-mode attempts to join the controller and fails, it will fall back to the other mode and attempt to join the same controller. When both modes fail, AP will move to the next discovery response.
- Static Configuration—Static IP configuration will take precedence over the Global or AP Group Specific prefer-mode. For example, if the Global prefer-mode is set to IPv4 and the AP has a static Primary Controller IPv6 address defined, the AP will join the WLC using the CAPWAPv6 mode.

AP Group Specific prefer-mode provides flexibility as it allows the administrator to specifically influence the CAPWAP transport mode utilized by different groups of APs. This allows APs deployed across different buildings or sites to operate using different CAPWAP modes. For example, APs within a campus that have already migrated to IPv6 can join a WLC using CAPWAPv6 while APs at remote sites that are yet to transition to IPv6 can join a WLC using CAPWAPv4. An individual WLC with a dual-stack configuration can support CAPWAP APs operating in both CAPWAPv4 and CAPWAPv6 modes.

Note An AP running an older image that is not IPv6 capable can join an IPv6 capable WLC only if the WLC has an IPv4 address assigned. The same is true for an IPv6 capable AP joining an IPv4 capable WLC (assuming the AP has an IPv4 address assigned). For IPv6 deployments, it is recommended that at least one discoverable WLC be configured to support IPv4.

For a full overview of the IPv6 enhancements introduced in 8.0, see the Cisco Wireless LAN Controller IPv6 Deployment Guide.

WLC Discovery & Selection

In a CAPWAP environment, a lightweight AP discovers a WLC by using a CAPWAP discovery mechanism and then sends the controller, a CAPWAP join request. When an AP joins a WLC, the WLC manages its configuration, firmware, control transactions, and data transactions. A CAPWAP AP must discover and join a WLC before it can become an active part of the Cisco Unifies Wireless Network.

Each Cisco AP supports the following discovery processes:

Step 1 Broadcast Discovery—The AP sends a CAPWAP discovery message to the IPv4 broadcast address (255.255.255.255). Any WLC connected to the same VLAN will see the discovery message and will in turn reply with a unicast IPv4 discovery response.

Step 2 Multicast Discovery—The AP sends a CAPWAP discovery message to the all controllers multicast group address (FF01::18C). Any WLC connected to the same VLAN will see the discovery message and will in turn reply with IPv6 discovery response.

Step 3 Locally Stored Controller IPv4 or IPv6 Address Discovery—If the AP was previously associated to a WLC, the IPv4 or IPv6 addresses of the primary, secondary, and tertiary controllers are stored in the APs non-volatile memory (NVRAM). This process of storing controller IPv4 or IPv6 addresses on an AP for later deployment is called *priming the access point*.

Step 4 DHCP Discovery—DHCPv4 and/or DHCPv6 servers are configured to advertise WLC IP addresses to APs using vendor-specific options:

  - DHCPv4 Discovery using Option 43—DHCPv4 servers use option 43 to provide one or more WLC management IPv4 addresses to the AP. Option 43 values are supplied to an AP in the DHCPv4 offer and acknowledgment packets.

- DHCPv6 Discovery using Option 52—DHCPv6 servers use option 52 to provide one or more WLC management IPv6 addresses to the AP. Option 52 values are supplied to an AP in the DHCPv6 advertise and reply packets.

Step 5 DNS Discovery—The AP sends a DNS query to the DNSv4 and/or DNSv6 servers to attempt to resolve cisco-capwap-controller.*localdomain* (where localdomain is the AP domain name provided by DHCP):

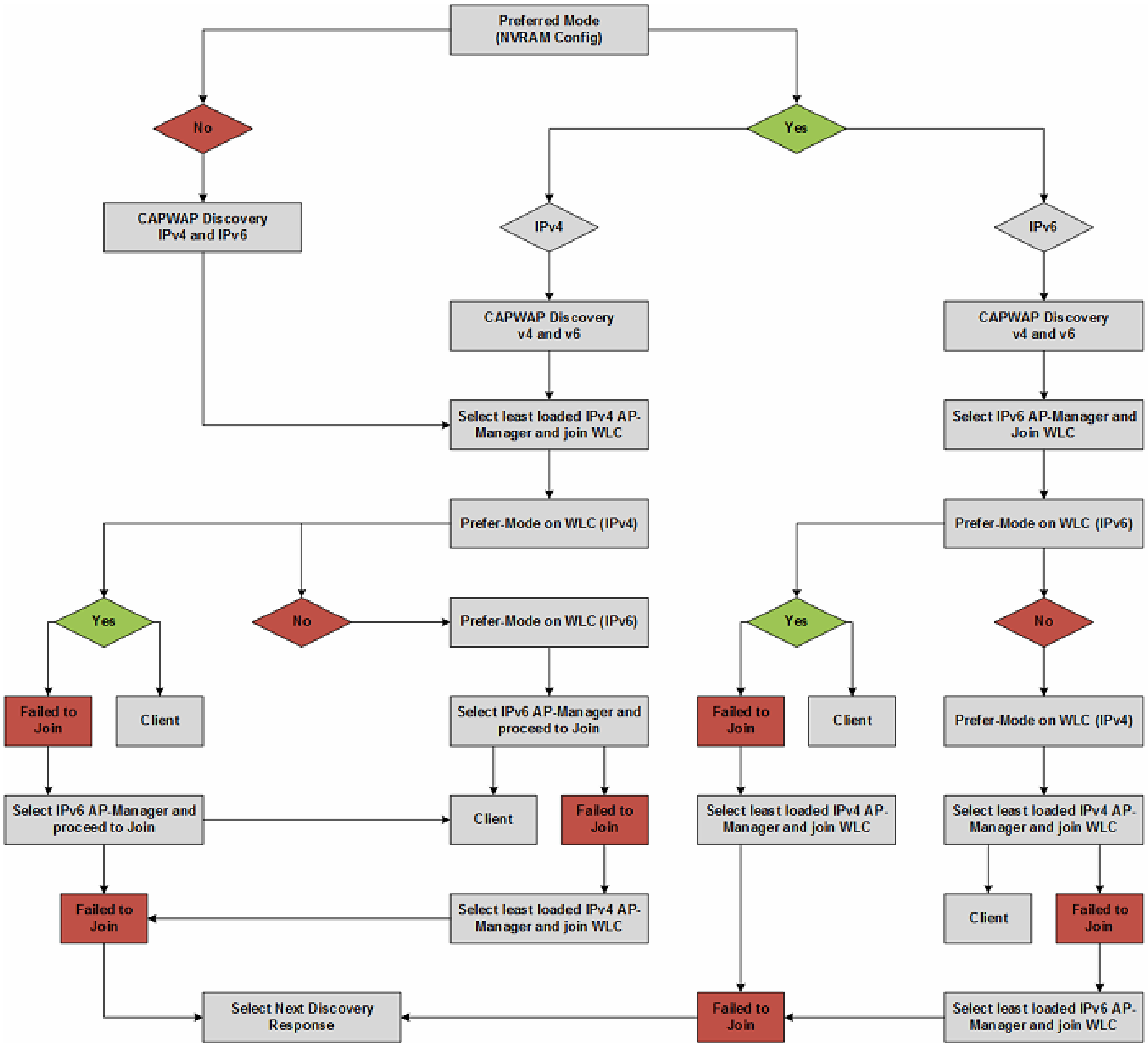
- DNSv4 Discovery—Address records are defined on the name servers for the cisco-capwap-controller hostname for each WLC managed IPv4 address to be supplied to the AP. When queried, the name server will respond with a list of IPv4 addresses for each A record that was defined.
- DNSv6 Discovery—Address records are defined on the name server for the cisco-capwap-controller hostname for each WLC managed IPv6 address to be supplied to the AP. When queried, the name server will respond with a list of IPv6 addresses for each AAAA record that was defined.

Up to three address records can be defined on the DNSv4 or DNSv6 name servers to be supplied to an AP. Each record corresponds to the primary, secondary and tertiary WLC IPv4 or IPv6 addresses.

Step 6 If after steps 1 – 5 no CAPWAP discovery response is received, the AP resets and restarts the discovery process.

Once the AP selects a WLC, the AP chooses to join through CAPWAPv4 or CAPWAPv6, depending on the CAPWAP prefer-mode pushed to the AP.

Figure 2-11 AP CAPWAP Discovery Diagram

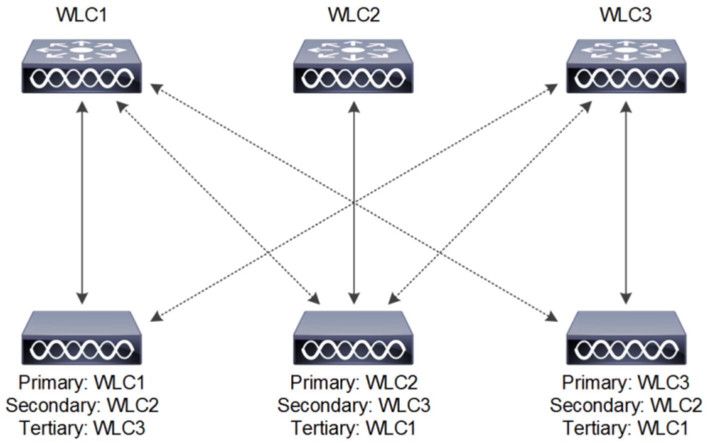

Preferred Mode (NVRAM Config)
No
Yes
CAPWAP Discovery IPv4 and IPv6
IPv4
IPv6
CAPWAP Discovery v4 and v6
CAPWAP Discovery v4 and v6
Select least loaded IPv4 AP-Manager and join WLC
Select IPv6 AP-Manager and Join WLC
Prefer-Mode on WLC (IPv4)
Prefer-Mode on WLC (IPv6)
Yes
No
Prefer-Mode on WLC (IPv6)
Yes
No
Failed to Join
Client
Select IPv6 AP-Manager and proceed to Join
Failed to Join
Client
Prefer-Mode on WLC (IPv4)
Select IPv6 AP-Manager and proceed to Join
Client
Failed to Join
Select least loaded IPv4 AP-Manager and join WLC
Select least loaded IPv4 AP-Manager and join WLC
Failed to Join
Select least loaded IPv4 AP-Manager and join WLC
Client
Failed to Join
Select Next Discovery Response
Failed to Join
Select least loaded IPv6 AP-Manager and join WLC

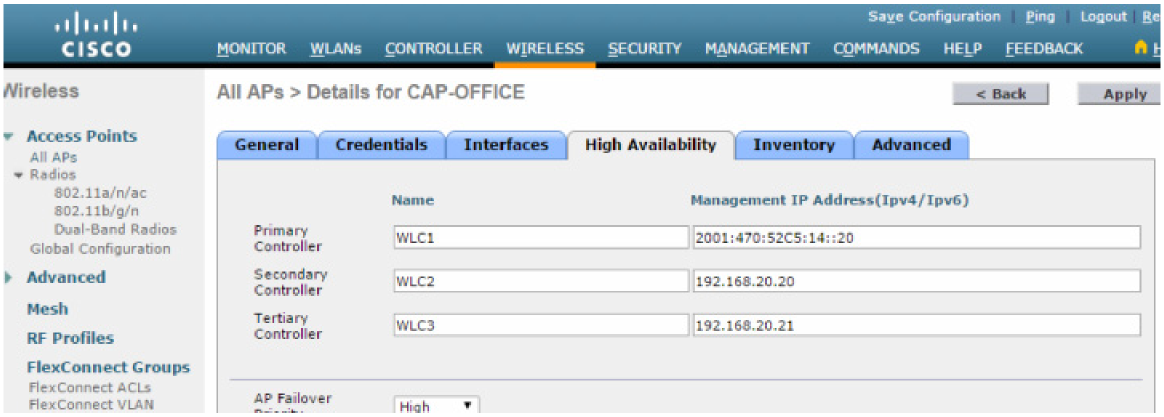
AP Priming

For most deployments, DHCP or DNS discovery is used to provide one or more seed WLC addresses. A subsequent WLC discovery response provides the AP with a full list of WLC mobility group members. An AP is normally configured with a list of one to three WLC management IP addresses (Primary, Secondary and Tertiary) that represent the preferred WLCs.

If the preferred WLCs become unavailable or are over-subscribed, the AP chooses another WLC from the list of WLCs learned in the CAPWAP discover responsei.e., the least-loaded WLC.

Figure 2-12 AP Priming Example





All APs > Details for CAP-OFFICE

	Name	Management IP Address(Ipv4/Ipv6)
Primary Controller	WLC1	2001:470:52C5:14::20
Secondary Controller	WLC2	192.168.20.20
Tertiary Controller	WLC3	192.168.20.21

AP Failover Priority: High

Note When priming an AP, the Primary Controller, Secondary Controller and Tertiary Controller management addresses can either be IPv4 or IPv6. It does not matter as long as the defined address is reachable by the AP. However, it is not possible to define both IPv4 and IPv6 addresses for a single entry. Each entry can contain only one IPv4 or IPv6 address.

Core Components

The Cisco Unified Wireless Network (CUWN) is designed to provide a high performance and scalable 802.11ac wireless services for enterprises and service providers. A Cisco wireless solution simplifies the deployment and management of large-scale wireless LANs in centralized or distributed deployments while providing a best-in-class security, user experience and services.

The Cisco Unified Wireless Network consists of:

- Cisco Wireless LAN Controllers (WLCs)
- Cisco Aironet Access Points (APs)
- Cisco Prime Infrastructure (PI)
- Cisco Mobility Services Engine (MSE)

This section describes available product options for the WLCs, APs and PI. For additional information, see the Cisco Mobility Services Engine.

Note For convenience and consistency, this document refers to all Cisco Wireless LAN Controllers as WLCs, Aironet Access Points as APs and Cisco Prime Infrastructure as PI.

Cisco Wireless LAN Controllers

Cisco Wireless LAN Controllers are enterprise-class, high-performance, wireless switching platforms that support 802.11a/n/ac and 802.11b/g/n protocols. They operate under control of the operating system, which includes the Radio Resource Management (RRM), creating a CUWN solution that can automatically adjust to real-time changes in the 802.11 RF environment. Controllers are built around high-performance network and security hardware, resulting in highly reliable 802.11 enterprise networks with unparalleled security.

This section describes the various models of Cisco WLCs and their capabilities supported in the 8.1 Release.

Table 2-2 Summary of Cisco Wireless Controllers

	Cisco 2504 Wireless Controller	**Cisco 5508 Wireless Controller**	**Cisco 5520 Wireless Controller**	**Cisco Flex 7510 Wireless Controller**	**Cisco 8510 Wireless Controller**	**Cisco 8540 Wireless Controller**	**Wireless Services Module 2 (WISM2)**	**Virtual Wireless Controller**
Form Factor	1U Appliance	1U Appliance	1U Appliance	1U Appliance	1U Appliance	2U Appliance	Module	Software
Platform Integration	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Scalability	75 x Access Points 1,000 x Clients 1 Gbps Throughput	500 x Access Points 7,000 x Clients 8 Gbps Throughput	1500 x Access Points 20,000 x Clients 20 Gbps Throughput	6000 x Access Points 64,000 x Clients 2000 x FlexConnect Groups	6000 x Access Points 64,000 x Clients 10 Gbps Throughput	6000 x Access Points 64,000 x Clients 40 Gbps Throughput	1000 x Access Points 15,000 x Clients 8 Gbps Throughput	200 x Access Points 6,000 x Clients 200 x FlexConnect Groups
Base AP Licenses	0.5, 15, 25 and 50 APs	0, 12, 25, 50, 100 and 250 AP Increments (CISL Based)	0 and 50 APs	0, 300, 500, 1000, 2000, 3000 and 6000 APs	0, 300, 500, 1000, 2000, 3000 and 6000 APs	0 and 1000 APs	0, 100, 300, 500 and 1000 APs	5 APs
AP Adder Licenses	1.5 and 25 AP Increments (CISL Based)	5, 25, 50, 100 and 250 AP Increments (CISL Based)	1 AP Increment (Right to Use)	100, 200, 500 and 1000 AP Increments (Right to Use)	100, 200, 500 and 1000 AP Increments (Right to Use)	1 AP Increments (Right to Use)	100 and 200 AP Increments (CISL Based)	1,5 and 25 AP Increments (Right to Use)
High Availability	N+1	N+1 SSO	N+1 SSO	N+1 SSO	N+1 SSO	N+1 SSO	N+1 SSO	N+1
Uplink Interfaces	4 x1G Ethernet Ports (RJ45)	8 x 1G Ethernet Ports (SFP)	2x1G/10G Ethernet Ports (SFP/SFP+)	1x10G Ethernet Ports (SFP+)	1x10G Ethernet Ports (SFP+)	4x1G/10G Ethernet Ports (SFP/SFP+)	8x1G Ethernet Ports (Internal Port-Channel	1 X virtual

Table 2-2 Summary of Cisco Wireless Controllers (continued)

	Cisco 2504 Wireless Controller	Cisco 5508 Wireless Controller	Cisco 5520 Wireless Controller	Cisco Flex 7510 Wireless Controller	Cisco 8510 Wireless Controller	Cisco 8540 Wireless Controller	Wireless Services Module 2 (WISM2)	Virtual Wireless Controller
Power	External AC Power Supply	AC (Redundant PSU Option)	AC (Redundant PSU Option)	AC/DC (Dual Redundant)	AC/DC (Dual Redundant)	AC/DC (Dual Redundant)	AC/DC (Catalyst Chassis)	Host Dependant
Positioning	Branch, Small Office	Enterprise, Campus & Full service branch	Enterprise, Campus & Full service branch	Central Site Controller for Large Number of Distributed Controller-less Branches	Enterprise, Large Campus, SP Wi-Fi, Full Scale Branch	Enterprise Large Campus, SP Wi-Fi, Full Scale Branch	Enterprise Campus	SP-Wi-Fi, Controller less branches, Small Office.

Cisco 2504 Wireless Controller

The Cisco 2504 Wireless Controller enables system-wide wireless functions for small to medium-sized enterprises and branch offices. Designed for 802.11n and 802.11ac performance, the Cisco 2504 Wireless Controllers are entry-level controllers that provide real-time communications between Cisco Aironet access points to simplify the deployment and operation of wireless networks.

Cisco 2504 Wireless Controller	**Deployment Type**	Branch, Small Office
	Operational Modes	All Modes
	Maximum Scale	75 APs 1,000 Clients
	AP Count Range	5 - 75
	License Entitlement	CISL Based
	Connectivity	4 x 1G Ethernet Ports (RJ-45)
	Power	External AC Power Supply
	Max Throughput	1 Gbps
	Max FlexConnect Groups	30
	Max APs / FlexConnect Group	20
	Max Rogue APs	2,000
	Max Rogue Clients	2,500
	Max RFID Tags	500
	Max APs / RF Group	500
	Max AP Groups	75
	Max Interface Groups	64
	Max Interface / Interface Group	64
	Max VLANs	16
	Max WLANs	16
	Fast Secure Roaming Clients / PMK Cache	700

For more information on Cisco 2504 Wireless Controller, see the Cisco 2500 Series Wireless Controllers.

Cisco 5508 Wireless Controller

Cisco 5508 Wireless Controllers deliver reliable performance, enhanced flexibility, and zero service-loss for mission-critical wireless. Interactive multimedia applications, such as voice and video, can now perform flawlessly over the wireless network, and clients can conveniently roam with no service interruption. Flexible licensing allows you to easily add access point support or premium software features.

Cisco 5508 Wireless Controller	**Deployment Type**	Enterprise Campus and Full Service Branch
	Operational Modes	All AP Modes
	Maximum Scale	500 APs 7,000 Clients
	AP Count Range	12 - 500
	License Entitlement	CISL Based
	Connectivity	8 x 1G Ethernet Ports (SFP)
	Power	AC (Redundant PSU Option)
	Max Throughput	8 Gbps
	Max FlexConnect Groups	100
	Max APs / FlexConnect Group	25
	Max Rogue APs	2,000
	Max Rogue Clients	2,500
	Max RFID Tags	5000
	Max APs / RF Group	1000
	Max AP Groups	500
	Max Interface Groups	64
	Max Interface / Interface Group	64
	Max VLANs	512
	Max WLANs	512
	Fast Secure Roaming Clients / PMK Cache	14,000

For more information about the Cisco 5508 Wireless Controller, see the Cisco 5500 Series Wireless Controllers.

Cisco 5520 Wireless Controller

The Cisco 5520 Series Wireless LAN Controller is a highly scalable, service-rich, resilient, and flexible platform that is ideal for medium-sized to large enterprise and campus deployments. As part of the Cisco Unified Access Solution, the 5520 is optimized for the next generation of wireless networks, 802.11ac Wave 2.

Cisco 5520 Wireless Controller	**Deployment Type**	Enterprise Campus and Full Service Branch
	Operational Modes	All AP Modes
	Maximum Scale	1,500 APs 20,000 Clients
	AP Count Range	1 - 1,500
	License Entitlement	Right to Use (EULA)
	Connectivity	2 x 10G Ethernet Ports (SFP+)
	Power	AC (Redundant PSU Option)
	Max Throughput	20 Gbps
	Max FlexConnect Groups	1, 500
	Max APs / FlexConnect Group	100
	Max Rogue APs	24,000
	Max Rogue Clients	32,000
	Max RFID Tags	25,000
	Max APs / RF Group	3000
	Max AP Groups	1,500
	Max Interface Groups	512
	Max Interface / Interface Group	64
	Max VLANs	4,095
	Max WLANs	512
	Fast Secure Roaming Clients / PMK Cache	40,000

For more information about the Cisco 5520 Wireless Controller, see the Cisco 5500 Series Wireless Controller.

Cisco Flex 7500 Wireless Controller

The Cisco Flex 7500 Wireless Controller is available in a model designed to meet the scaling requirements to deploy the FlexConnect solution in branch networks. FlexConnect is designed to support wireless branch networks by allowing the data to be switched locally within the branch site, while the access points are being controlled and managed by a centralized controller. The Cisco Flex 7500 Series Cloud Controller aims to deliver a cost effective FlexConnect solution on a large scale.

Cisco 5520 Wireless Controller	**Deployment Type**	Central Site Controller for Large Number of Distributed, Controller-less Branches
	Operational Modes	FlexConnect, Flex+Bridge
	Maximum Scale	6,000 APs 64,000 Clients
	AP Count Range	300 – 6,000
	License Entitlement	Right to Use (EULA)
	Connectivity	2 x 10G Ethernet Ports (SFP+) / 1 Active
	Power	AC/DC (Dual Redundant)
	Max Throughput	—
	Max FlexConnect Groups	2,000
	Max APs / FlexConnect Group	100
	Max Rogue APs	32,000
	Max Rogue Clients	24,000
	Max RFID Tags	50,000
	Max APs / RF Group	6000
	Max AP Groups	6000
	Max Interface Groups	512
	Max Interface / Interface Group	64
	Max VLANs	4,095
	Max WLANs	512
	Fast Secure Roaming Clients / PMK Cache	64,000

For more information, see the Cisco Flex 7500 Series Wireless Controllers.

Cisco 8510 Wireless Controllers

The Cisco 8510 Wireless Controller is a highly scalable and flexible platform that enables mission-critical wireless networking for enterprise and service provider deployments.

Cisco 8510 Wireless Controller	**Deployment Type**	Enterprise Large Campus, SP Wi-Fi, Full Scale Branch
	Operational Modes	All AP Modes
	Maximum Scale	6,000 APs 64,000 Clients
	AP Count Range	300 – 6,000
	License Entitlement	Right to Use (EULA)
	Connectivity	2 x 10G Ethernet Ports (SFP+) / 1 Active
	Power	AC/DC (Dual Redundant)
	Max Throughput	10 Gbps
	Max FlexConnect Groups	2,000
	Max APs / FlexConnect Group	100
	Max Rogue APs	32,000
	Max Rogue Clients	24,000
	Max RFID Tags	50,000
	Max APs / RF Group	6000
	Max AP Groups	6000
	Max Interface Groups	512
	Max Interface / Interface Group	64
	Max VLANs	4,095
	Max WLANs	512
	Fast Secure Roaming Clients / PMK Cache	64,000

For more information about the Cisco 8510 Wireless Controller, see the Cisco 8500 Series Wireless Controllers.

Cisco 8540 Wireless Controller

Optimized for 802.11ac Wave2 performance, the Cisco 8540 Wireless Controller is a highly scalable, service-rich, resilient, and flexible platform that enables next-generation wireless networks for medium-sized to large enterprise and campus deployments.

Cisco 8540 Wireless Controller	**Deployment Type**	Enterprise Large Campus, SP Wi-Fi, Full Scale Branch
	Operational Modes	All AP Modes
	Maximum Scale	6,000 APs 64,000 Clients
	AP Count Range	1 – 6,000
	License Entitlement	Right to Use (EULA)
	Connectivity	4 x 10G Ethernet Ports (SFP+)
	Power	AC/DC (Dual Redundant Hot-Swappable PSU)
	Max Throughput	40 Gbps
	Max FlexConnect Groups	2,000
	Max APs / FlexConnect Group	100
	Max Rogue APs	32,000
	Max Rogue Clients	24,000
	Max RFID Tags	50,000
	Max APs / RF Group	6000
	Max AP Groups	6000
	Max Interface Groups	512
	Max Interface / Interface Group	64
	Max VLANs	4,095
	Max WLANs	512
	Fast Secure Roaming Clients / PMK Cache	64,000

For more information about the Cisco 8540 Wireless Controller, see the Cisco 8500 Series Wireless Controllers.

Cisco Wireless Services Module 2

The Cisco Wireless Services Module 2 (WiSM2) for the Catalyst 6500 Series switches ideal for mission-critical wireless networking for medium-sized to large single-site WLAN environments where an integrated solution is preferred. The WiSM2 helps to lower hardware costs and offers flexible configuration options that can reduce the total cost of operations and ownership for wireless networks.

Cisco Wireless Services Module 2 (WiSM2)	**Deployment Type**	Enterprise Campus
	Operational Modes	All AP Modes
	Maximum Scale	1,000 APs 15,000 Clients
	AP Count Range	100 – 1,000
	License Entitlement	CISL Based
	Connectivity	Internal to Catalyst Backplane
	Power	AC/DC (Catalyst Chassis with Redundant PSU Option)
	Max Throughput	10 Gbps
	Max FlexConnect Groups	100
	Max APs / FlexConnect Group	25
	Max Rogue APs	4,000
	Max Rogue Clients	5,000
	Max RFID Tags	10,000
	Max APs / RF Group	2,000
	Max AP Groups	500
	Max Interface Groups	64
	Max Interface / Interface Group	64
	Max VLANs	512
	Max WLANs	512
	Fast Secure Roaming Clients / PMK Cache	30,000

For more information, see the Cisco Wireless Services Module 2.

Virtual Wireless LAN Controller

The controller allows IT managers to configure, manage, and troubleshoot up to 200 access points and 6000 clients. The Cisco Virtual Wireless Controller supports secure guest access, rogue detection for Payment Card Industry (PCI) compliance, and in-branch (locally switched) Wi-Fi voice and video.

Cisco Virtual Wireless Controller (vWLC)	**Deployment Type**	SP Wi-Fi, Controller-less Branches, Small Office
	Operational Modes	FlexConnect, Flex+Bridge
	Maximum Scale	200 APs 6,000 Clients
	AP Count Range	5 – 200
	License Entitlement	Right to Use (EULA)
	Connectivity	1 (Virtual)
	Power	Host Dependent
	Max Throughput	Not Applicable
	Max FlexConnect Groups	200
	Max APs / FlexConnect Group	100
	Max Rogue APs	800
	Max Rogue Clients	1,500
	Max RFID Tags	3,000
	Max APs / RF Group	1,000
	Max AP Groups	200
	Max Interface Groups	—
	Max Interface / Interface Group	—
	Max VLANs	4,094
	Max WLANs	512
	Fast Secure Roaming Clients / PMK Cache	6,000

For more information, see the Cisco Virtual Wireless Controller.

Note The Cisco Virtual Wireless Controller is supported on industry-standard virtualization infrastructure including VMWare’s ESXi (4.x/5.x) and KVM, in addition to the Cisco Unified Computing System Express (UCS Express) platform for the second generation of Integrated Services Routers.

Cisco Aironet Access Points

Cisco Aironet Series wireless access points can be deployed in a distributed or centralized network for a branch office, campus, or large enterprise. To ensure an exceptional end-user experience on the wireless network, these wireless access points provide a variety of capabilities, including:

- Cisco CleanAir Technology—For a self-healing, self-optimizing network that avoids RF interference.
- Cisco ClientLink 2.0 or 3.0—To improve reliability and coverage for clients.
- Cisco BandSelect—To improve 5 GHz client connections in mixed client environments.
- Cisco VideoStream—Leverages multicast to improve multimedia applications.

Note Cisco 1500 series MESH APs are mentioned briefly below, but this design guide does not address wireless MESH applications or MESH deployment guidelines. For more information about the Cisco MESH solution, see the Cisco Mesh Networking Solution Deployment Guide.

Indoor 802.11n Access Points

The following section describes the various models of Cisco indoor 802.11n APs and their capabilities supported in the 8.1 release.

	Cisco Aironet 600 Series	Cisco Aironet 700W Series	Cisco Aironet 1600 Series	Cisco Aironet 2600 Series	Cisco Aironet 3600 Series
Wi-Fi Standard	802.11a/b/g/n	802.11a/b/g/n	802.11a/b/g/n	802.11a/b/g/n	802.11a/b/g/n/ac
Number of Radios	Dual (2.4Ghz and 5 Ghz)	Dual (2.4Ghz and 5 Ghz)	Dual (2.4Ghz and 5 Ghz)	Dual (2.4Ghz and 5 Ghz)	Tri (2.4Ghz and 5 Ghz)
Max data Rate	300 Mbps	300 Mbps	300 Mbps	450 Mbps	450 Mbps (802.11n) 1.3Gbps (802.11ac Module)
MIMO Radio Design	2x3	2x2	3x3	3x4	802.11n: 4x4 802.11ac: 3x3
Spatial Streams	2 Spatial Streams	2 Spatial Streams	2 Spatial Streams	3 Spatial Streams	3 Spatial Streams
Antennas	Internal	Internal	1600i Internal 1600e External	2600i: Internal 2600e: External	3600i: Internal 3600e: External 3600p: External
CleanAIR 2.0	—	—	CleanAir Express	Yes	Yes
ClientLink 2.0	—	—	Yes	Yes	Yes
Cisco Innovations	—	BandSelect Videostream	BandSelect Videostream	BandSelect Videostream	BandSelect Videostream

	Cisco Aironet 600 Series	Cisco Aironet 700W Series	Cisco Aironet 1600 Series	Cisco Aironet 2600 Series	Cisco Aironet 3600 Series
Modularity	USB*	—	—	—	802.11ac Wave 1 Module USC Small Cell Module Wireless Security Module (WSM)
Power	AC	DC, 802.3afPoE, 802.3at PoE+	DC, 802.3afPoE	DC, 802.3afPoE	DC, 802.3afPoE, 802.3at PoE+, Enhanced PoE, Universal PoE
Interfaces	5x1G Ethernet Ports (RJ-)45 1x1G Ethernet WAN Ports (RJ-45)	1x1G Ethernet Uplink Port (RJ-45) 4x1G Ethernet User Ports (RJ-45)	1x1G Ethernet Uplink Port (RJ-45)	1x1G Ethernet Uplink Port (RJ-45)	1x1G Ethernet Uplink Port (RJ-45)

Cisco Aironet 600 Series OfficeExtend

The Cisco Aironet 600 Series OfficeExtend Access Points provide highly secure enterprise wireless coverage to home. These dual-band, 802.11n access points extend the corporate network to home tele-workers and mobile contractors. The access point connects to the home's broadband internet access and establishes a highly secure tunnel to the corporate network so that remote employees can access data, voice, video, and cloud services for a mobility experience consistent with that at the corporate office. The dual-band, simultaneous support for 2.4 GHz and 5 GHz radio frequencies helps assure that corporate devices are not affected by congestion caused by common household devices that use the 2.4 GHz band. The Cisco Aironet 600 Series OfficeExtend Access Points are purposely designed for the teleworker by supporting secure corporate data access and maintaining connectivity for personal home devices with segmented home traffic.

Cisco Aironet 600 Series	**Wi-Fi Standard**	802.11a/b/g/n
	Operational Modes	OfficeExtend
	Number of Radios	Dual (2.4GHz and 5GHz)
	Max Data Rate	300 Mbps
	MIMO Design	2x3
	Spatial Streams	2
	Max Client Count	15
	Max ClientLink Count	—
	ClientLink 2.0	—
	ClearAir	—
	VideoStream	—
	BandSelect	—
	Rogue AP Detection	—
	Adaptive WIPS	—
	Power	AC
	Antennas	Internal

For more information about the Cisco Aironet 600 Series, see the Cisco Aironet 600 Series OfficeExtend Access Point.

Cisco Aironet 700W Series

The Cisco Aironet 700W Series offers a compact wall-plate mountable access point for hospitality and education-focused customers looking to modernize their networks to handle today's increasingly complex wireless access demands.

With 802.11n dual-radio 2 x 2 Multiple-Input Multiple-Output (MIMO) technology providing at least six times the throughput of existing 802.11a/g networks, the Cisco Aironet 700W Series offers the performance advantage of 802.11n quality at a competitive price.

As part of the Cisco Unified Wireless Network, the 700W Series Access Point provides low total cost of ownership and investment protection by integrating seamlessly with the existing network.

Cisco Aironet 700W Series	**Wi-Fi Standard**	802.11a/b/g/n
	Operational Modes	Centralized, FlexConnect
	Number of Radios	Dual (2.4GHz and 5GHz)
	Max Data Rate	300 Mbps
	MIMO Design	2x2
	Spatial Streams	2
	Max Client Count	100 Wireless / 4 Wired
	Max ClientLink Count	—
	ClientLink 2.0	—
	ClearAir	—
	VideoStream	Yes
	BandSelect	Yes
	Rogue AP Detection	Yes
	Adaptive WIPS	Yes
	Power	DC, 802.3af PoE, 802.3af PoE+
	Antennas	Internal

For more information, see the Cisco Aironet 700W Series.

Cisco Aironet 1600 Series

The new Cisco Aironet 1600 Series Access Point is an enterprise-class, entry-level, 802.11n based access point designed to address the wireless connectivity needs of small and medium-sized enterprise networks.

The Aironet 1600 Series delivers great performance at an attractive price for customers, while providing advanced functionality such as CleanAir Express for better cover through spectrum intelligence and Clientlink 2.0 for entry level networks that have a mixed client base. In addition to these features, the Aironet 1600 series includes 802.11n based 3x3 MIMO technology with two spatial streams, making it ideal for small and medium-sized enterprises.

The Aironet 1600 Series also provides at least six times the throughput of existing 802.11a/g networks. As part of the Cisco Aironet Wireless portfolio, the Cisco Aironet 1600 Series access point provides low total cost of ownership and investment protection by integrating seamlessly with the existing network. With an entry-level path to 802.11n migration, the Aironet 1600 Series can add capacity to the network for future growth for expanding applications and bandwidth.

Designed with rapidly evolving mobility needs in mind, the Cisco Aironet 1600 Series Access Point addresses the Bring-Your-Own-Device (BYOD) trend by providing advanced functionality at the right price point.

Cisco Aironet 1600 Series	**Wi-Fi Standard**	802.11a/b/g/n
	Operational Modes	Centralized, FlexConnect, Indoor Mesh, OfficeExtend
	Number of Radios	Dual (2.4GHz and 5GHz)
	Max Data Rate	300 Mbps
	MIMO Design	3x3
	Spatial Streams	2
	Max Client Count	128
	Max ClientLink Count	32
	ClientLink 2.0	Yes
	ClearAir	Yes – CleanAir Express
	VideoStream	Yes
	BandSelect	Yes
	Rogue AP Detection	Yes
	Adaptive WIPS	Yes
	Power	DC, 802.3af PoE
	Antennas	1600i: Internal 1600e: External

For more information, see the Cisco Aironet 1600 Series.

Cisco Aironet 2600 Series

The Cisco Aironet 2600 Series Access Point delivers the most advanced features in its class with great performance, functionality, and reliability at a great price. The 802.11n based Aironet 2600 Series includes 3x4 MIMO, with three spatial streams, Cisco CleanAir, ClientLink 2.0, and VideoStream technologies, to help ensure an interference-free, high-speed wireless application experience. Next to the Cisco Aironet 3600 Series in performance and features, the Aironet 2600 Series sets the new standard for enterprise wireless technology.

Designed with rapidly evolving mobility needs in mind, the Aironet 2600 Series access point is packed with more BYOD-enhancing functionality than any other access point at its price point. The new Cisco Aironet 2600 Series sustains reliable connections at higher speeds farther from the access point than competing solutions resulting in more availability of 450 Mbps data rates. Optimized for consumer devices, the Aironet 2600 Series accelerates client connections and consumes less mobile device battery power than competing solutions.

Cisco Aironet 2600 Series	**Wi-Fi Standard**	802.11a/b/g/n
	Operational Modes	Centralized, FlexConnect, Indoor Mesh, OfficeExtend
	Number of Radios	Dual (2.4GHz and 5GHz)
	Max Data Rate	450 Mbps
	MIMO Design	3x4
	Spatial Streams	3
	Max Client Count	200
	Max ClientLink Count	128
	ClientLink 2.0	Yes
	ClearAir	Yes
	VideoStream	Yes
	BandSelect	Yes
	Rogue AP Detection	Yes
	Adaptive WIPS	Yes
	Power	DC, 802.3af PoE, 802.3af PoE+
	Antennas	2600i: Internal 2600e: External

For more information, see the Cisco Aironet 2600 Series.

Cisco Aironet 3600 Series

Delivering up to three times more coverage versus competition for tablets, smartphones, and high-performance laptops, the industry's first 4x4 MIMO, three-spatial-stream access point delivers mission critical reliability. Current solutions struggle to scale to meet demands on the wireless networks from the influx of diverse mobile devices and mobile applications. The Cisco Aironet 3600 Series sustains reliable connections at higher speeds further from the access point than competing solutions, resulting in up to three times more availability of 450 Mbps rates, and optimizing the performance of more mobile devices. Cisco Aironet 3600 Series is an innovative, modular platform that offers unparalleled investment protection with future module expansion to support incoming 802.11ac clients with 1.3 Gbps rates, or offer comprehensive security and spectrum monitoring and control.

Cisco Aironet 3600 Series includes Cisco ClientLink 2.0 to boost performance and range for clients and includes Cisco CleanAir spectrum intelligence for a self-healing, self-optimizing network.

Cisco Aironet 3600 Series	**Wi-Fi Standard**	802.11a/b/g/n 802.11ac (with module)
	Operational Modes	Centralized, FlexConnect, Indoor Mesh, OfficeExtend
	Number of Radios	Tri (2.4GHz, 5GHz and Module)
	Max Data Rate	802.11n: 450 Mbps 802.11ac: 1.3Gbps
	MIMO Design	802.11n: 4x4 802.11ac: 3x3
	Spatial Streams	3
	Max Client Count	802.11n: 200 802.11ac: 50
	Max ClientLink Count	802.11n: 128 802.11ac: 7 (ECBF)
	ClientLink 2.0	Yes (ECBF with 802.11ac clients)
	ClearAir	Yes
	VideoStream	Yes
	BandSelect	Yes
	Rogue AP Detection	Yes
	Adaptive WIPS	Yes
	Power	DC, 802.3af PoE, 802.3at (PoE+), Enhanced PoE, Universal PoE (UPOE)
	Antennas	3600i: Internal 3600e: External 3600p: External

For more information, see the Cisco Aironet 3600 Series.

Indoor 802.11ac Access Points

The following section describes the various models of Cisco indoor 802.11ac APs and their capabilities supported in the 8.1 Release.

	Cisco Aironet 1700 Series	**Cisco Aironet 1850 Series**	**Cisco Aironet 2700 Series**	**Cisco Aironet 3700 Series**
Wi-Fi Standard	802.11a/b/g/n/ac (Wave 1)	802.11a/b/g/n/ac (Wave 2)	802.11a/b/g/n/ac (Wave 1)	802.11a/b/g/n/ac (Wave 1)
Number of Radios	Dual (2.4Ghz and 5 Ghz)	Dual (2.4Ghz and 5 Ghz)	Dual (2.4Ghz and 5 Ghz)	Dual (2.4Ghz and 5 Ghz)
Max data Rate	867 Mbps	1.7 Gbps	1.3 Gbps	1.3 Gbps
MIMO Radio Design	3x3	4x4	3x4	4x4
Spatial Streams	2 Spatial Streams	4 Spatial Streams (SU MIMO) 3 Spatial Streams (MU MIMO)	3 Spatial Streams	3 Spatial Streams
Antennas	1700i:internal	1850i Internal 1850e: External	2700i Internal 2700e External	3700i: Internal 3700e: External 3700p: External
CleanAIR 2.0	CleanAir Express	CleanAir Express	Yes	Yes
ClientLink 3.0	Tx Beam Forming	Tx Beam Forming	Yes	Yes
Cisco Innovations	BandSelect Videostream	BandSelect Videostream	BandSelect High Density Experience Videostream	BandSelect StadiumVision High Density Experience Videostream
Modularity	—	USB 2.0*	—	802.11ac Wave 2 Module USC Small Cell Module Hyperlocation Module Wireless Security Module (WSM)
Power	DC, 802.3afPoE,+, Enhanced PoE	DC, 802.3afPoE,+, Enhanced PoE	DC, 802.3afPoE,+, Enhanced PoE	DC, 802.3afPoE,802.3at PoE+, Enhanced PoE, Universal PoE
Interfaces	1x1G Ethernet Uplink Port (RJ-45) 1x1G Ethernet Aux Port (RJ-45)	1x1G Ethernet Uplink Port (RJ-)45w/AutoLAG 1x1G Ethernet AUX Port (RJ-45)w/AutoLAG	1x1G Ethernet Uplink Port (RJ-45) 1x1G Ethernet Aux Port (RJ-45)	1x1G Ethernet Uplink Port (RJ-45)

Cisco Aironet 1700 Series

If you operate a small or medium-sized enterprise network, deploy the Cisco Aironet 1700 Series Access Point for the latest 802.11ac Wi-Fi technology at an attractive price. The 1700 Series meets the growing requirements of wireless networks by delivering better performance than 802.11n and providing key RF management features for improved wireless experiences.

The 1700 Series supports 802.11ac Wave 1 standard capabilities. That includes a theoretical connection rate up to 867 Mbps.

Cisco Aironet 1700 Series	**Wi-Fi Standard**	802.11a/b/g/n/ac (Wave 1)
	Operational Modes	Centralized, FlexConnect, Indoor Mesh, OfficeExtend
	Number of Radios	Dual (2.4GHz and 5GHz)
	Max Data Rate	867 Mbps
	MIMO Design	3x3
	Spatial Streams	2
	Max Client Count	200
	Max ClientLink Count	—
	ClientLink 2.0	Yes – Transmit Beamforming (TxBF)
	ClearAir	Yes – CleanAir Express
	VideoStream	Yes
	BandSelect	Yes
	Rogue AP Detection	Yes
	Adaptive WIPS	Yes
	Power	DC, 802.3af PoE, 802.3at PoE+, Enhanced PoE
	Antennas	1700i: Internal 1700e: External

For more information, see the Cisco Aironet 1700 Series.

Cisco Aironet 1850 Series

Ideal for small and medium-sized networks, the Cisco Aironet 1850 Series delivers industry-leading performance for enterprise and service provider markets through enterprise-class 4x4 MIMO, four-spatial-stream access points that support the IEEE's new 802.11ac Wave 2 specification. The Aironet 1850 Series extends support to a new generation of Wi-Fi clients, such as smartphones, tablets, and high-performance laptops that have integrated 802.11ac Wave 1 or Wave 2 support.

Cisco Aironet 1850 Series	**Wi-Fi Standard**	802.11a/b/g/n/ac (Wave 2)
	Operational Modes	Centralized, FlexConnect (Future)
	Number of Radios	Dual (2.4GHz and 5GHz)
	Max Data Rate	1.7 Gbps
	MIMO Design	4x4
	Spatial Streams	4 (SU-MIMO) 3 (MU-MIMO)
	Max Client Count	200
	Max ClientLink Count	—
	ClientLink 3.0	Yes – Transmit Beamforming (TxBF)
	ClearAir 2.0	Yes
	VideoStream	Yes
	BandSelect	Yes
	Rogue AP Detection	Yes
	Adaptive WIPS	Yes
	Power	DC, 802.3af PoE, 802.3af PoE+, Enhanced PoE
	Antennas	1850i: Internal 1850e: External

For more information, see the Cisco Aironet 1850 Series.

Cisco Aironet 2700 Series

The Cisco Aironet 2700 Series of Wi-Fi access points (APs) delivers industry-leading 802.11ac performance at a price point ideal for plugging capacity and coverage gaps in dense indoor environments. The Aironet 2700 Series extends 802.11ac speed and features to a new generation of smartphones, tablets, and high-performance laptops now shipping with the faster, 802.11ac Wi-Fi radios.

The Aironet 2700 series supports 802.11ac Wave 1 in its first implementation, providing a theoretical connection rate of up to 1.3 Gbps. That's roughly triple the rates offered by today's high-end 802.11n APs. The boost helps you stay ahead of the performance and bandwidth expectations of today's mobile worker, who usually uses multiple Wi-Fi devices instead of just one. As such, users are adding proportionally larger traffic loads to the wireless LAN, which has outpaced ethernet as the default enterprise access network.

Cisco Aironet 2700 Series	**Wi-Fi Standard**	802.11a/b/g/n/ac (Wave 1)
	Operational Modes	Centralized, FlexConnect, Indoor Mesh, OfficeExtend
	Number of Radios	Dual (2.4GHz and 5GHz)
	Max Data Rate	1.3 Mbps
	MIMO Design	3x4
	Spatial Streams	3
	Max Client Count	200
	Max ClientLink Count	128
	ClientLink 3.0	Yes
	ClearAir 2.0	Yes
	VideoStream	Yes
	BandSelect	Yes
	Rogue AP Detection	Yes
	Adaptive WIPS	Yes
	Power	DC, 802.3af PoE, 802.3at PoE+, Enhanced PoE
	Antennas	2700i: Internal 2700e: External

For more information, see the Cisco Aironet 2700 Series Access Point.

Cisco Aironet 3700 Series

With the industry's only enterprise class 4x4 MIMO, three-spatial-stream access points that support the IEEE's 802.11ac Wave 1 specification, the Cisco Aironet 3700 Series delivers industry-leading performance and a High Density (HD) experience for both the enterprise and service provider markets. The Aironet 3700 Series extends support to a new generation of Wi-Fi clients, such as smartphones, tablets, and high-performance laptops that have integrated 802.11ac support.

In its first implementation, 802.11ac wave 1 provides a rate of up to 1.3 Gbps, roughly triple the rates offered by today's high-end 802.11n access points. This provides the necessary foundation for enterprise and service provider networks alike to stay ahead of the performance and bandwidth expectations and needs of their wireless users.

Due to its convenience, wireless access is increasingly the preferred form of network connectivity for corporate users. Along with this shift, there is an expectation that wireless should not slow down user's day-to-day work, but should enable a high-performance experience while allowing users to move freely around the corporate environment by utilizing a purpose-built innovative Chipset with the best-in-class RF Architecture for a HD experience.

Cisco Aironet 3700 Series	**Wi-Fi Standard**	802.11a/b/g/n/ac (Wave 1)
	Operational Modes	Centralized, FlexConnect, Indoor Mesh, OfficeExtend
	Number of Radios	Tri (2.4GHz, 5GHz and Module)
	Max Data Rate	1.3 Mbps
	MIMO Design	4x4
	Spatial Streams	3
	Max Client Count	200
	Max ClientLink Count	128
	ClientLink 3.0	Yes
	ClearAir 2.0	Yes
	VideoStream	Yes
	BandSelect	Yes
	Rogue AP Detection	Yes
	Adaptive WIPS	Yes
	Power	DC, 802.3af PoE, 802.3at PoE+, Enhanced PoE, Universal PoE (UPOE)
	Antennas	3700i: Internal 3700e: External 3700p: External

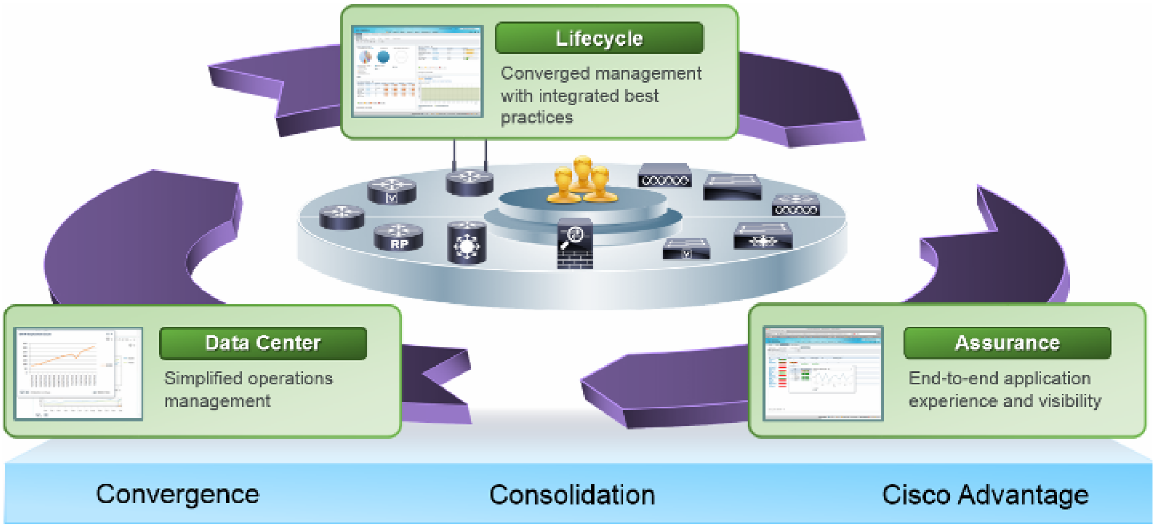
For more information, see the Cisco Aironet 3700 Series.

Cisco Prime Infrastructure

Change is the new phenomenon. Mobile device proliferation, pervasive voice and video collaboration, and cloud and data center virtualization are transforming the network as never before. Yet along with the new opportunities comes a host of new challenges. There's the need for higher service levels, assured application delivery, and simplified end-user experiences, while maintaining business continuity and controlling operating expenses.

To address these challenges, IT professionals need a comprehensive solution that enables them to manage the network from a single graphical interface and the solution is Cisco Prime Infrastructure. It provides lifecycle management and service assurance networkwide, from the wireless user in the branch office, across the WAN, through the access layer, and now to the data center. We call it One Management (Figure 2-13).

Figure 2-13 Cisco Prime Infrastructure: One Management


Lifecycle
Converged management with integrated best practices
Data Center
Simplified operations management
Assurance
End-to-end application experience and visibility
Convergence
Consolidation
Cisco Advantage

Cisco Prime Infrastructure is a network management that connects the network to the device to the user to the application, end-to-end and all in one. Its capabilities permit:

- Single-pane-of-glass management—Delivers a single, unified platform for day-0 and day-1 provisioning and day-n assurance. It accelerates device and services deployment and helps you to rapidly resolve problems that can affect the end-user experience. Minimize the amount of time you spend managing the network so you can maximize the time you spend using it to grow your business.
- Simplified deployment of Cisco value-added features—Makes the design and fulfillment of Cisco differentiated features and services fast and efficient. With support for technologies such as Intelligent WAN (IWAN), Distributed Wireless with Converged Access, Application Visibility and Control (AVC), Zone-Based Firewall, and Cisco TrustSec 2.0 Identity-Based Networking Services, it helps you get the most from the intelligence built-in to your Cisco devices as quickly as possible.
- Application visibility—Configures and used as a source of performance data embedded Cisco instrumentation and industry-standard technologies to deliver networkwide, application-aware visibility. These technologies include NetFlow, Network-Based Application Recognition 2 (NBAR2), Cisco Medianet technologies, Simple Network Management Protocol (SNMP), and more. The innovative coupling of application visibility and lifecycle management of Cisco Prime Infrastructure makes it easier to find and resolve problems by providing insight into the health of applications and services in the context of the health of the underlying infrastructure.

- Management for mobile collaboration—Answers the who, what, when, where, and how of wireless access. It includes 802.11ac support, correlated wired-wireless client visibility, unified access infrastructure visibility, spatial maps, converged security and policy monitoring and troubleshooting with Cisco Identity Services Engine (ISE) integration, location-based tracking of interferers, rogues, and Wi-Fi clients with Cisco Mobility Services Engine (MSE) and Cisco CleanAir integration, lifecycle management, RF prediction tools, and more.
- Management across network and compute—Delivers powerful lifecycle management and service assurance to help you manage and maintain the many devices and services running on your branch-office, campus, and data center networks. It provides key capabilities such as discovery, inventory, configuration, monitoring, troubleshooting, reporting, and administration. With a single view and point of control, it lets you reap the benefits of One Management across both network and computer.
- Centralized visibility of distributed networks—Large or global organizations often distribute network management by domain, region, or country. Cisco Prime Infrastructure Operations Center lets you visualize up to 10 Cisco Prime Infrastructure instances, scaling your network-management infrastructure while maintaining central visibility and control.

Licensing Options

Cisco Prime Infrastructure is a single installable software package with licensing options to expand and grow functions and coverage as needed.

- Lifecycle—Simplifies the day-to-day operational tasks associated with managing the network infrastructure across all lifecycle phases (design, deploy, operation, and report) for Cisco devices including routers, switches, access points, and more.
- Assurance—Provides application performance visibility using device instrumentation as a source of rich performance data to help assure consistent application delivery and an optimal end-user experience.
- Cisco UCS Server Management—Offers lifecycle and assurance management for Cisco UCS B- and C-Series Servers.
- Operations center—Enables visualization of up to 10 Cisco Prime Infrastructure instances from one central management console. One license is required for each Cisco Prime Infrastructure supported instance.
- High-Availability Right to Use (RTU)—Permits high-availability configuration with one primary and one secondary instance in a high-availability pair.
- Collector—Increases the NetFlow processing limit on the Cisco Prime Infrastructure management node. This license is used in conjunction with the Assurance license.
- Ready-to-use gateway RTU—Entitles you to deploy a separate gateway for use with the ready-to-use feature, where new devices can call in to the gateway to receive their configuration and software image.

Note Cisco Prime Infrastructure 2.2 is available for new customers, and upgrade options are available for existing customers running on prior versions. Upgrade options are also available for Cisco Network Control System (NCS), Cisco Wireless Control System (WCS), and Cisco Prime LAN Management Solution (LMS) customers. For details refer to: http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/datasheet-listing.html.

Scaling

Cisco Prime Infrastructure 2.2 is available for purchase as a virtual or physical appliance. The virtual appliance can be installed on top of VMware's industry-standard hypervisor and is available in multiple versions to support networks of different sizes. A physical appliance is also available for large network deployments, when dedicated CPU and memory resources are required.

- Physical Appliance (Second Generation)—Based on the Cisco UCS C220 M4 Rack Server.
- Virtual Appliance—ESXi Version 5.0, 5.1 or 5.5.

Table 2-3 provides a scaling matrix for Cisco Prime Infrastructure 2.2 for both the virtual and physical appliances:

Table 2-3 Cisco Prime Infrastructure 2.2 Scaling Matrix

Parameter		**Express Virtual Appliance**	**Express Plus Virtual Appliance**	**Standard Virtual Appliance**	**Pro Virtual Appliance**	**Physical Appliance (Gen 1)**	**Physical Appliance (Gen 2)**
Devices	Max Unified APs	300	2,500	5,000	20,000	5,000	20,000
	Max Autonomous APs	300	500	3,000	3,000	3,000	3,000
	Max WLAN Controllers	5	25	500	1,000	500	1,000
	Max Wired	300	1,000	6,000	13,000	6,000	13,000
	Max NAMs	5					
	Max Devices	1,000	4,000	15,000	20,000	15,000	20,000
Clients	Max Wired Clients	6,000	50,000	50,000	5=20,000	15,000	20,000
	Max Wireless Clients	4,000	30,000	75,000	200,000	75,000	200,000
	Transient Wireless Clients (Clients / 5 min Interval)	1,000	5,000	25,000	40,000	25,000	40,000
Monitoring	Sustained Events/Sec	100	100	300	1,000	300	1,000
	Netflow (Flows/Sec)	3,000	3,000	16,000	80,000	16,000	80,000
	Max Interfaces	12,000	50,000	250,000	350,000	250,000	350,000
	Max. NAM Data Poling Enabled	5	5	20	40	20	40

Table 2-3 Cisco Prime Infrastructure 2.2 Scaling Matrix

Parameter		Express Virtual Appliance	Express Plus Virtual Appliance	Standard Virtual Appliance	Pro Virtual Appliance	Physical Appliance (Gen 1)	Physical Appliance (Gen 2)
System	Max Sites / Campus	200	500	2,500	2,500	2,500	2,500
	Max Groups	50	100	150	150	150	150
	Max Virtual Domains	100	500	1,200	1,200	1,200	1,200
	Max GUI Clients	5	10	25	50	25	50
	Max API Clients	2	2	5	5	5	5

High Availability

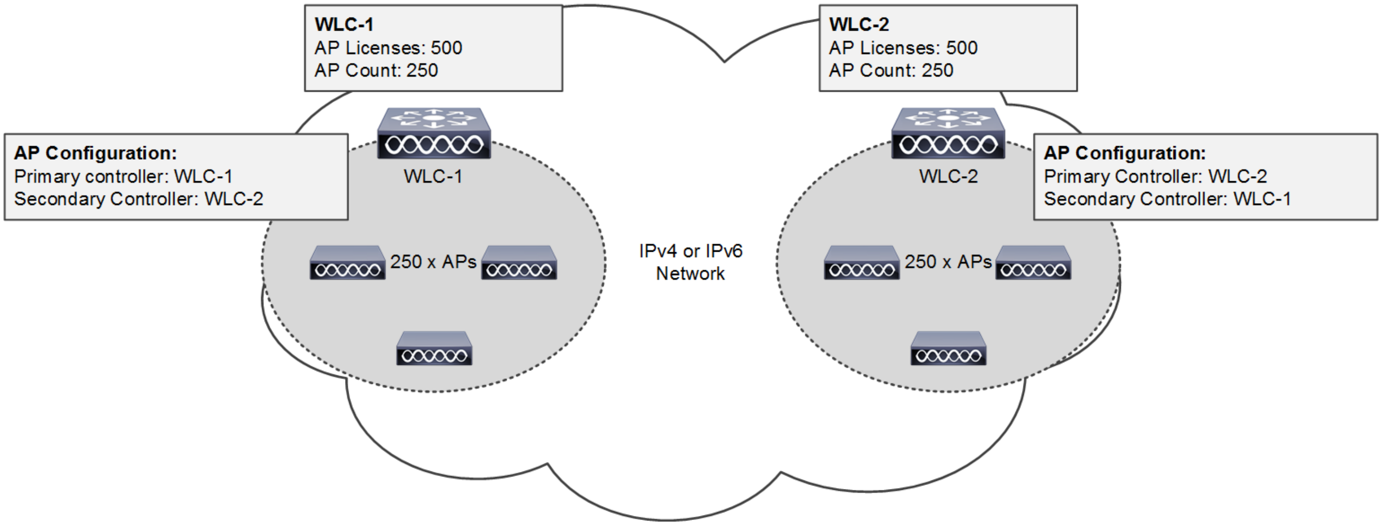
The following section provides an overview of the High Availability (HA) deployment options available for a Cisco Unified Wireless Network.

AP / Client Failover

N+1 Wireless Controller Redundancy

WLC redundancy has been around for a long time and is well understood. Redundancy is provided by deploying multiple controllers on the network which provide backup and share load. Each AP is configured with the IP address and name of their preferred primary, secondary and tertiary WLCs. If a APs primary WLC becomes unreachable, the AP will failover to its configured secondary WLC (and so forth). This redundancy model is called N+1 meaning an extra WLC is available to support the APs and load if one (or more) of the primary WLCs becomes unreachable (see Figure 2-14).

Figure 2-14 N+1 Wireless Controller Redundancy



The N+1 redundancy model requires additional permanent AP licenses are purchased for each backup WLC. A backup WLC can either be dedicated for redundancy or support APs during normal operation. Each WLC is managed independently and does not share configuration. The necessary WLANs, AP Groups and RF Groups must be defined on each backup WLC to ensure seamless operation during a failure.

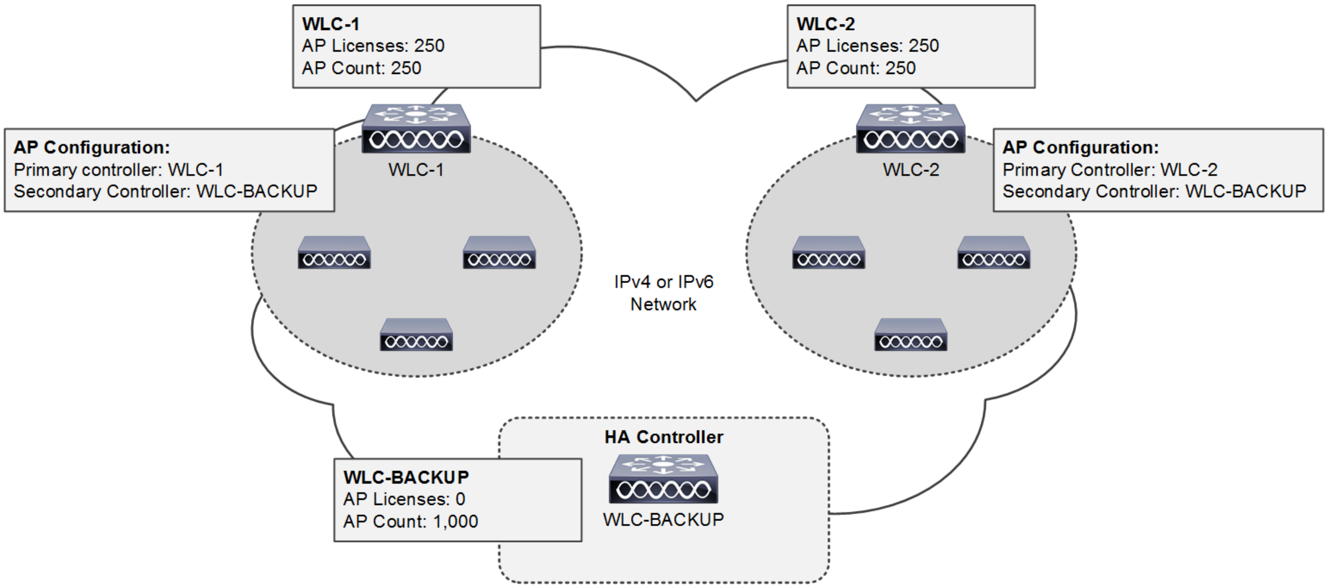
The example shown in Figure 2-14 demonstrates a simple N+1 deployment with two WLCs each supporting 250 x APs during normal operation. To provide redundancy each WLC has 500 permanent AP licenses installed to ensure that all of the APs are supported in the event that one of the WLCs becomes unreachable. APs connected to WLC-1 are configured to use WLC-2 as their secondary WLC while APs connected to WLC-2 are configured to use WLC-1 as their secondary WLC.

Note For large deployments, if the preferred WLCs are unavailable or over-subscribed, the AP chooses another WLC from the list of WLCs within the mobility group learned in the CAPWAP discover response that is the least-loaded WLC.

N+1 HA Wireless Controller Redundancy

The N+1 HA feature builds upon the N+1 redundancy model by allowing a single WLC to be deployed as a backup for multiple primary WLCs. As previously mentioned an N+1 deployment requires additional AP licenses to be purchased for the backup WLCs which are unused during normal operation. With an N+1 HA deployment a HA-SKU WLC is deployed as the backup WLC for multiple primary WLCs without any additional permanent AP licenses being required (seeFigure 2-15).

Figure 2-15 N+1 HA Wireless Controller Redundancy



The N+1 HA architecture can provide redundancy for both centralized and FlexConnect AP deployments. WLC redundancy can be provided within the same campus/site or between geographically separate data centers. The HA WLC is managed independently and does not share configuration with the primary WLCs. Each WLC needs to be configured and managed separately. The necessary WLANs, AP Groups and RF Groups must be defined on the HA WLC to ensure seamless operation during a failover.

If a primary WLC becomes unreachable or fails, the affected APs failover to the HA WLC. A HA WLC is only licensed to support APs for up to 90-days. As soon as an AP joins the HA WLC a 90-day timer will start. A warning message will be displayed if APs are still present on the HA WLC after the 90-day interval expires. A HA WLC can only be used as a secondary WLC for 90 days without a warning message.

The example shown in Figure 2-15 demonstrates a simple N+1 HA deployment for a 500 AP deployment. Both of the primary WLCs have 250 permanent AP licenses installed. The HA WLC model is selected to initially support 500 APs and provide room for future growth. APs connected to WLC-1 and WLC-2 are configured to use WLC-BACKUP as their secondary WLC.

Note HA-SKUs are available for the 2500 series, 5500 series, 7500 series, 8500 series wireless controllers as well as the WiSM2. An N+1 HA deployment can consist of WLCs of different models (for example 5508 WLCs operating as primary and a 5520 WLC HA-SKU operating as a backup.

HA Stateful Switchover Wireless Controller Redundancy

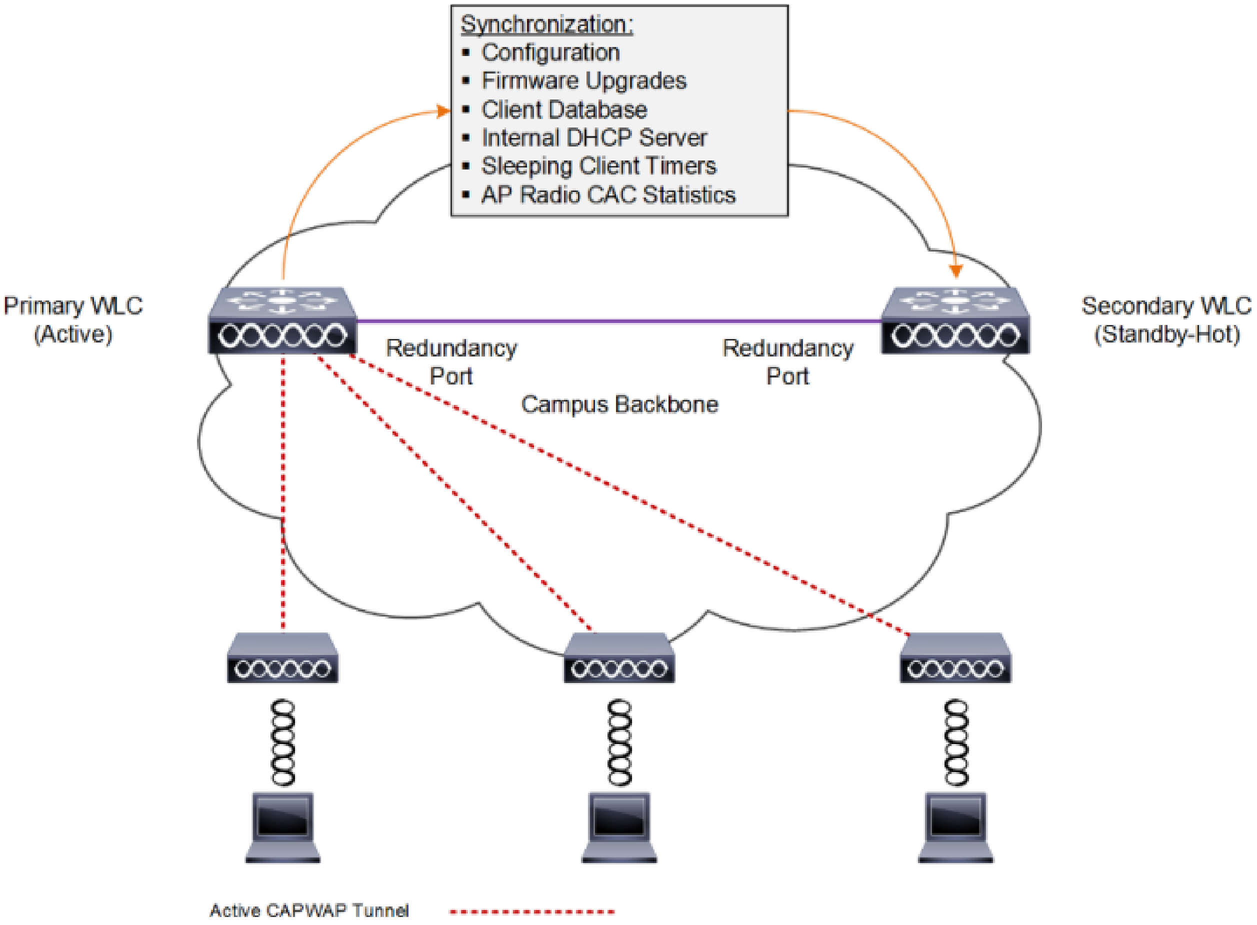
Both the N+1 and N+1 HA redundancy architectures discussed in the previous sections provide AP failover in the event that a primary WLC becomes unreachable. Both architectures impact wireless services while APs detect that their primary WLC is unreachable and failover to their secondary or tertiary WLC. To provide HA without impacting service, there needs to be support for seamless transition of both APs and clients between WLCs. The WLCs implement both AP stateful switchover (AP SSO) and client stateful switchover (Client SSO) to provide zero client service downtime and prevent SSID outages during a WLC failover.

HA stateful switchover (SSO) is the recommended HA deployment architecture for a CUWN. This design builds upon the N+1 HA architecture where two WLCs are deployed as a 1:1 primary / secondary pair. The current configuration as well as AP and client state information is automatically synchronized between the primary and secondary peers. For most deployments the primary WLC has the permanent AP licenses installed while the secondary WLC is a HA-SKU (see Figure 2-16).

During normal operation the primary WLC assumes an active role while the secondary WLC assumes a standby-hot role. After a switchover, the secondary WLC assumes the active role and the primary WLC assumes the standby-hot role. After subsequent switchovers, the roles are interchanged between the primary and secondary WLCs. The WLCs exchange UDP keep-alive packets through their redundancy management interfaces (RMI) to check peer and management gateway reachability.

Once HA-SSO is enabled all configuration is performed on the active WLC which is automatically synchronized to the standby-hot WLC. No configuration can be performed on the CLI or Web-UI on the standby-hot WLC. Firmware images are also distributed to the standby-hot WLC.

Figure 2-16 HA-SSO Wireless Controller Redundancy



Note For additional details please see the "High Availability (SSO) deployment guide" at: http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/HA_SSO_DG/High_Availability_DG.html.

The HA-SSO architecture consists of both AP and client SSO which combine to provide sub-second failure detection and failover without impacting wireless services to clients. AP SSO was initially introduced in release 7.3 while client SSO was introduced in release 7.5:

- AP SSO – Allows the APs to establish a CAPWAP tunnel with the active WLC and share a mirror copy of the AP database with the standby-hot WLC. The APs do not go into a CAPWAP discovery state during a failover. There is only one CAPWAP tunnel maintained at a time between the APs and the WLC that is in an active state. The overall goal for AP SSO is to reduce downtime in wireless networks due to failure conditions that may occur such as a WLC or network failover.
- Client SSO – To provide seamless failover without impacting service, there needs to be support for seamless transition of both clients and APs from the active WLC to the standby-hot WLC. With Client SSO, a client's information is synchronized to the standby-hot WLC when the client associates to the active WLC or the client's parameters change. All fully authenticated clients are synced to the standby-hot WLC and thus, client re-association is avoided during a switch over making the failover seamless for the APs as well as for the clients. This results in zero client service downtime and no SSID outages.

AP and client SSO is supported by the 5500 series, 7500 series and 8500 series WLCs as well as the Wireless Services Module 2. Each appliance based WLC supports a dedicated redundancy port while the WiSM2 implements a redundancy VLAN. The redundancy port is used to exchange keep-alive messages as well as synchronize configuration and state information. Redundancy ports are either be directly connected or indirectly connected through an intermediate layer 2 network. Table 2-4 provides a summary of HA SSO support for each model of WLC:

Table 2-4 HA-SSO Support by Controller Platform

Platform	Redundancy Port	AP SSO	Client SSO
Cisco 2504 Wireless Controller	No	No	No
Cisco 5508 Wireless Controller	Yes	Yes (7.3 and above)	Yes (7.5 and above)
Cisco 5520 Wireless Controller	Yes	Yes (8.1 and above)	Yes (8.1 and above)
Cisco Flex 7500 Wireless Controller	Yes	Yes (7.3 and above)	Yes (7.5 and above)
Cisco 8510 Wireless Controller	Yes	Yes (7.3 and above)	Yes (7.5 and above)
Cisco 8540 Wireless Controller	Yes	Yes (8.1 and above)	Yes (8.1 and above)
Cisco Wireless Services Module 2	Yes-VLAN	Yes	Yes
Virtual Wireless Controller (vWLC)	No	No	No

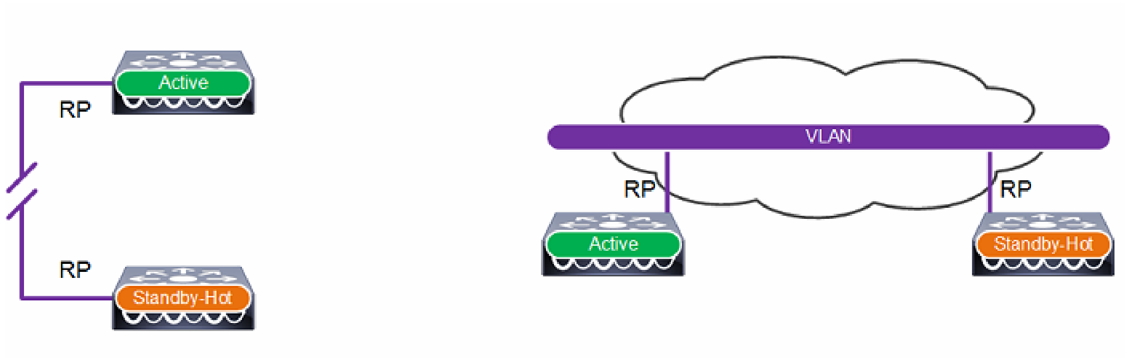
Note The implementation of AP and Client SSO is dependent on the software release operating on the primary and secondary WLCs and cannot be independently configured. For example if HA is enabled and both WLCs support 8.1, both AP SSO and Client SSO will be implemented.

Redundancy Port / VLAN Configurations

A redundancy port / VLAN is mandatory for HA-SSO deployments and are used to synchronize configuration / state as well as exchange keep-alive packets. A redundancy port / VLAN is also used for role negotiation. Appliance based WLCs such as the 5500 series, 7500 series and 8500 series controllers implement a dedicated Ethernet redundancy port while the WiSM2 implements a redundancy VLAN.

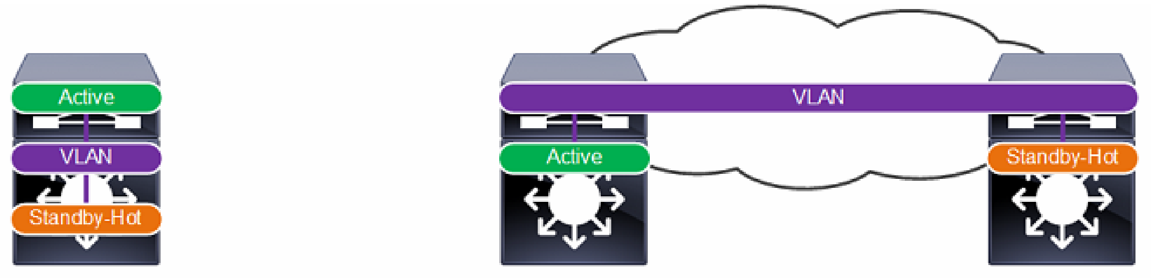
In release 7.5 and above, the redundancy ports for appliance based WLCs can be interconnected via a dedicated Ethernet cable or indirectly connected at layer 2 over intermediate switches using a dedicated non-routable VLAN. Direct connections with fiber over media converters is also supported. Figure 2-17 demonstrates the supported redundancy port connection options.

Figure 2-17 Redundancy Port Interconnections



For WiSM-2 based deployments, HA-SSO is supported for both single chassis and multiple chassis deployments. Multi chassis deployments are supported using VSS or by extending the redundancy VLAN. The redundancy VLAN must be dedicated and non-routable. Figure 2-18 demonstrates the chassis deployment options.

Figure 2-18 WiSM2 Redundancy VLAN



Considerations

When connecting redundancy ports or VLANs over an intermediate L2 network, the following considerations must be met:

- The round trip time (RTT) latency between the peers must be 400 milliseconds or less (80 milliseconds by default). The RTT is 80% of the keepalive timer which is configurable in the range of 100 (default) – 400 milliseconds. A higher RTT requires the keepalive timer to be increased.
- A minimum of 60 Mbps of bandwidth is required between the peers.
- A minimum 1,500 byte MTU path is required between the peers.

Topologies

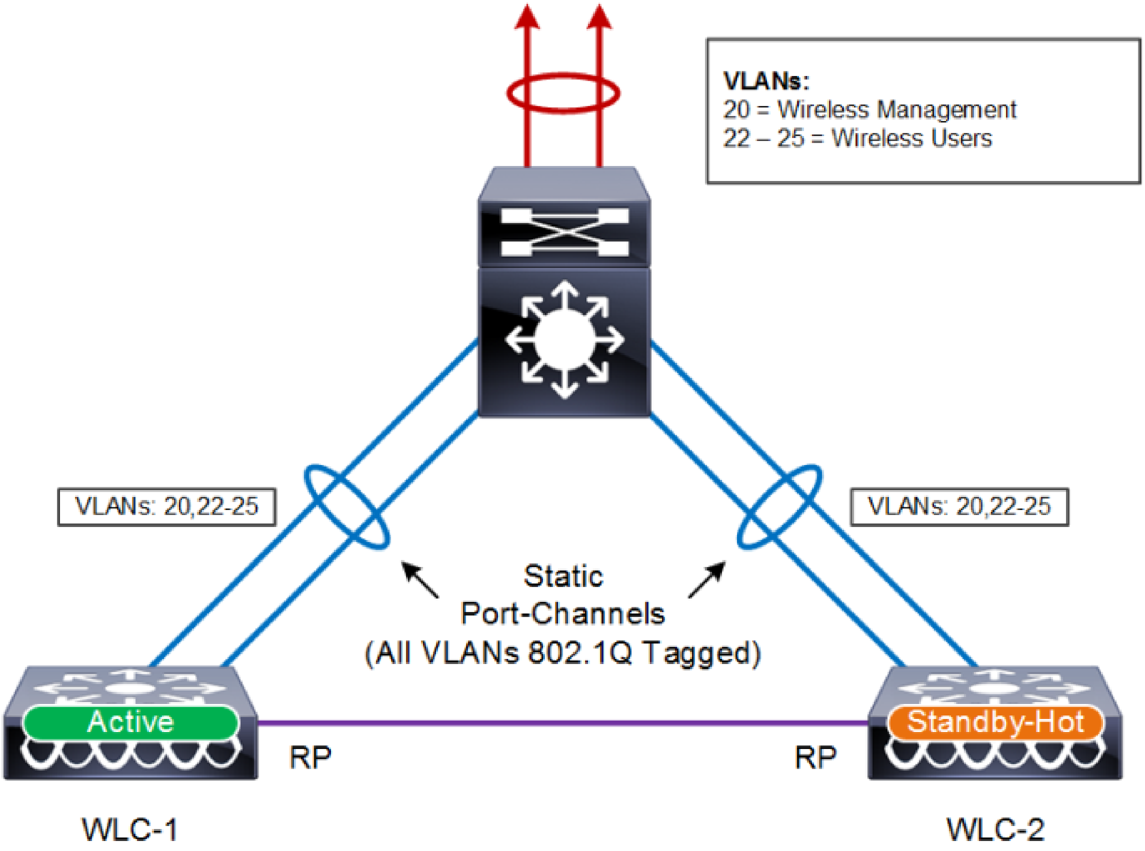
The following section provides an overview of the typical topologies used when deploying HA-SSO within a Cisco Unified Wireless Network (CUWN). For simplicity each example shows appliance based WLCs with their redundancy ports directly connected. Each topology also applies to WiSM2 deployments.

For each of the below designs, the Catalyst distribution switches provide a boundary between the wireless services block and core layers. This boundary provides two key functions for the LAN. On the Layer 2 side, the distribution layer creates a boundary for spanning tree protocol (STP), limiting propagation of Layer 2 faults. On the Layer 3 side, the distribution layer provides a logical point to summarize IP routing information when it enters the network. The summarization reduces IP route tables for easier troubleshooting and reduces protocol overhead for faster recovery from failures.

Standalone Distribution Switch

The topology shown in Figure 2-19 demonstrates a HA-SSO pair of WLCs that are connected to a standalone Catalyst switch within the wireless services block. Redundancy is provided by deploying multiple line cards or switches to form a resilient stack. This design provides minimum protection against network and hardware failures as a complete chassis or stack failure will result in the HA-SSO WLCs being isolated from the rest of the network.

Figure 2-19 HA-SSO with a Standalone Distribution Switch



Note The above architecture also applies to WiSM2 deployments. The equivalent WISM2 design consisting of a single Catalyst 6500 series chassis with two WiSM2 modules installed.

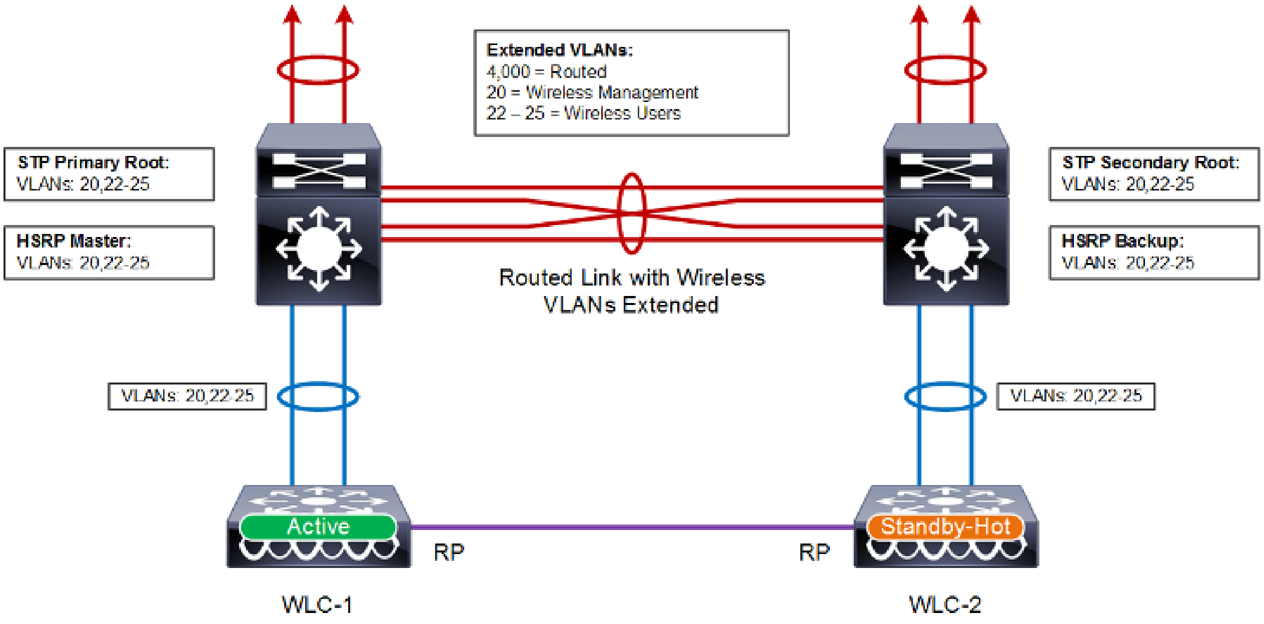
Multilayer Distribution Switches

The topology shown in Figure 2-20 demonstrates a HA-SSO pair of WLCs that are connected to a pair of Catalyst switches within the wireless services block implementing a multilayer design. As the Catalyst switches in this topology example are layer 3 connected, this results in a more complex design as the wireless management and wireless user VLANs must be extended between the Catalyst switches. This results in a looped multilayer architecture that requires a spanning tree protocol and a first-hop routing protocol:

- With this architecture you cannot implement routed ports or a routed port-channel between the Catalyst switches. Instead a link-local VLAN with switched virtual interfaces (SVIs) must be used. This allows the wireless VLANs to be extended between the Catalyst switches while maintaining a multilayer design.
- For loop prevention spanning tree protocol (STP) must be enabled for each of the wireless VLANs. The Catalyst switch connected to the primary WLC must be configured as the STP root bridge for each VLAN.
- First-hop router redundancy such as HSRP must be enabled and configured for each wireless VLAN. The distribution switch connected to the primary WLC must be configured as the HSRP master for each VLAN.

During normal operation the Catalyst switch connecting to the active WLC is the first-hop router for each of the wireless management and wireless user VLANs. This minimizes the traffic that crosses the link between the pair of Catalysts switches as it is both the STP root and the HSRP master. If the primary Catalyst switch fails, HA-SSO will failover to the standby-hot WLC. If the primary Catalyst switch loses connectivity to the core network, a HA-SSO failover will not occur as the primary WLC can still communicate with the standby-hot WLC through the port-channel established between the two Catalyst switches.

Figure 2-20 HA-SSO with Multilayer Distribution Switches

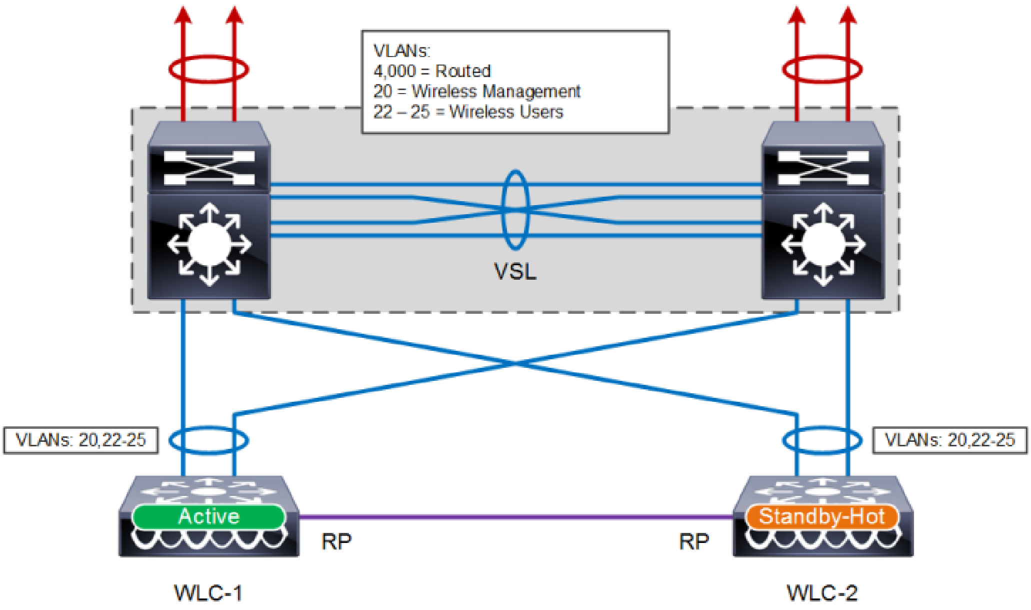


Note The above architecture also applies to WiSM2 deployments. The equivalent WISM2 design consisting of two Catalyst 6500 series chassis configured for multilayer operation each with a WiSM2 module installed.

VSS Distribution Switches

The topology shown in Figure 2-21 demonstrates a HA-SSO pair of WLCs that are connected to a VSS pair of distribution switches within the wireless services block and is the recommended design. This design minimizes the traffic that crosses the virtual switch link between the Catalyst switches in the VSS pair during normal operation, because both the active and standby-hot WLCs have ports connected to both switches. This design also avoids a switchover from the active WLC to the standby-hot WLC in the event of a switch failure within the VSS pair. However, in the event of a switch failure within the VSS pair, the number of ports connected to the active WLC would be reduced by half.

Figure 2-21 HA-SSO using VSS



Note The above architecture also applies to WiSM2 deployments. The equivalent WISM2 design consisting of two Catalyst 6500 series chassis in a VSS configuration each with a WiSM2 module installed.

Considerations

When implementing HA-SSO, the following considerations should be made:

- The Catalyst switches should be configured and deployed following Cisco recommended best practices as outlined in the published Cisco Validated Designs (CVDs) available at: http://www.cisco.com/c/en/us/solutions/enterprise/design-zone/index.html.
- HA-SSO failover times are dependent on the convergence times introduced by routing protocol, spanning tree protocol and first-hop router redundancy protocol.
- The wireless management, wireless user VLANs should be 802.1Q tagged between the Catalyst switches and the WLCs.
- It is recommended that the HA-SSO WLCs be connected to the Catalyst switches using link aggregation (LAG). The WLC ports should be distributed between ports on different line cards within a chassis or switches within a resilient stack. If VSS is deployed the WLC ports can be distributed between both Catalyst switches.

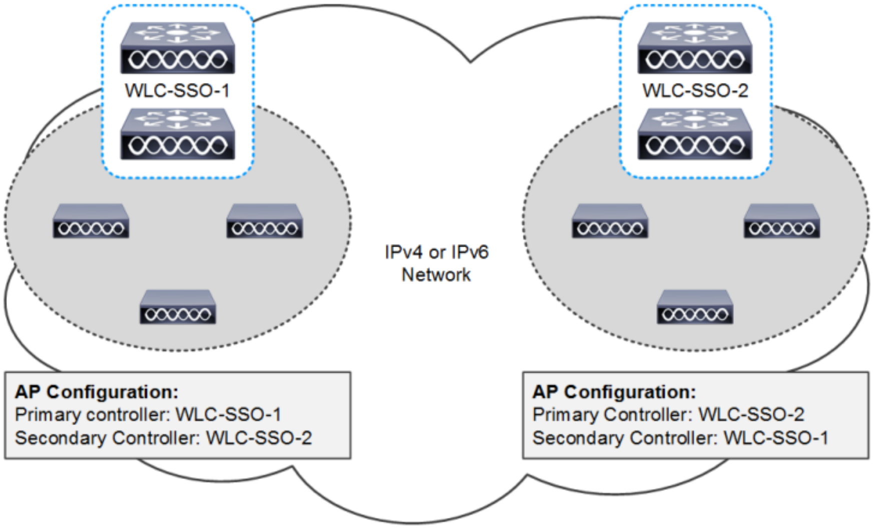
- The channel mode for the port-channel on the neighboring Catalyst switch or VSS connecting to the WLCs must be set to mode on (static). The WLC software release 8.1 does not support LACP or PaGP protocols.
- When connecting HA-SSO WLCs to multilayer distribution switches:
- The wireless management and user VLANs are 802.1Q tagged between the Catalyst distribution switches. This will result in a multilayer looped design.
- For loop prevention it is recommended that rapid spanning tree protocol be enabled for the wireless management and wireless user VLANs. The Catalyst switch is connected to the primary WLC during normal operation should be configured as the STP root bridge for each wireless VLAN.
- A first-hop routing protocol such as HSRP must be enabled for the wireless management and user VLANs. The Catalyst switch that is connected to the primary WLC during normal operation should be configured as the HSRP master for each wireless VLAN.
- Appliance based WLC redundancy ports can be directly connected or indirectly connected at layer 2. If indirectly connected it is recommended that you extend a dedicated non-routable 2 VLAN between each of the Catalyst switches.
- If the redundancy ports are extended over an intermediate L2 network, the latency, bandwidth and MTU requirements outlined in the previous section must be followed.

HA-SSO and N+1 Redundancy

For large Cisco Unified Wireless Network (CUWN) deployments both HA-SSO and N+1 redundancy can be combined to provide AP failover in the event that SSO-HA WLCs become unreachable (Figure 2-22). This is the recommended design for a large CUWN deployment where different HA-SSO pairs are assigned to service APs within a defined geography such as buildings or floors.

The configuration works exactly the same as an N+1 HA deployment where the APs are configured with primary, secondary and tertiary WLCs. The APs primary WLC is configured as their assigned HA-SSO WLC pair, while the secondary (and optionally the tertiary) WLC can be configured as a separate HA-SSO WLC pair or a standalone WLC. The APs will only failover to the secondary WLC if both the active and standby-hot WLCs in the primary HA-SSO pair become unreachable. Failover to the secondary or tertiary WLCs is stateless.

Figure 2-22 HA-SSO and N+1 Redundancy


WLC-SSO-1
WLC-SSO-2
IPv4 or IPv6
Network
AP Configuration:
Primary controller: WLC-SSO-1
Secondary Controller: WLC-SSO-2
AP Configuration:
Primary Controller: WLC-SSO-2
Secondary Controller: WLC-SSO-1

Fast Restart

The Fast restart enhancement aims to reduce network and service downtime by up to 73% when making changes to the following features:

- LAG Configuration Change
- Mobility Mode Change
- Web-Auth Certificate Change
- Clear Configuration

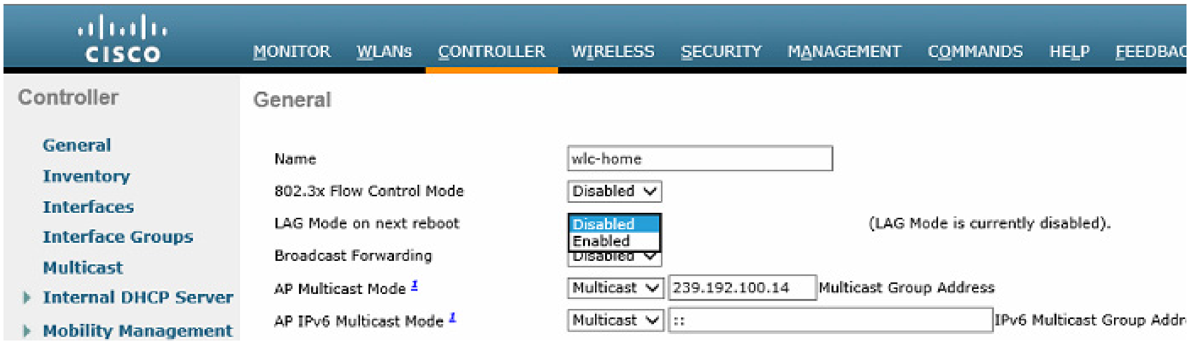
Without fast restart, the above changes required a full system restart. Fast restart feature is supported on the Cisco WLC 5520, 7510, 8510, 8540 and vWLC starting release 8.1. It can be invoked using the CLI by issuing the **Restart** command or by clicking Save and Restart within the Web-UI.

Link Aggregation (LAG)

Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. When enabled LAG bundles all of the WLCs Ethernet ports into a single 802.3ad port-channel providing additional bandwidth and fault-tolerance between the WLC and its neighboring switch. If any of the WLC ports or connections fail, traffic is automatically migrated to one of the other remaining Ethernet ports in the bundle. As long as at least one Ethernet port is functioning, the wireless system continues to operate, APs remain and clients are able to send and receive data.

LAG is a globally enabled on the WLC (Figure 2-23) and is supported by the Cisco WLC 2504, 5508, 5520 and 8540. When you enable LAG all Ethernet ports will participate in the bundle. The WLC requires an immediate full system reboot or fast restart to enable LAG.

Figure 2-23 LAG Mode



General

Name: wlc-home
802.3x Flow Control Mode: Disabled
LAG Mode on next reboot: Disabled / Enabled (LAG Mode is currently disabled).
Broadcast Forwarding: Disabled
AP Multicast Mode 1: Multicast 239.192.100.14 Multicast Group Address
AP IPv6 Multicast Mode 1: Multicast :: IPv6 Multicast Group Addr

Considerations

When implementing LAG, the following considerations should be made:

- A Cisco WLC does not send CDP advertisements on a LAG interface.
- All WLC Ethernet ports in the LAG must operate at the same speed. You cannot mix Gigabit and 10Gigabit ports.
- The channel mode for the port-channel on the neighboring Catalyst switch or VSS connecting to the WLCs must be set to mode on (static). The WLC software release 8.1 does not support LACP or PaGP protocols.
- You cannot separate the WLC Ethernet ports into separate LAG groups.
- Only one AP-manager interface is supported as all Ethernet ports are bundled into a single logical port.
- When you enable LAG, all dynamic AP-manager interfaces and untagged interfaces are deleted, and all WLANs are disabled and mapped to the management interface. The management, static AP-manager, and VLAN-tagged dynamic interfaces are assigned to the LAG port.
- When you enable LAG, the WLC sends packets out on the same port on which it received them. If a CAPWAP packet from an AP enters the controller on physical port 1, the WLC removes the CAPWAP wrapper, processes the packet, and forwards it to the network on physical port 1.

Mobility Groups, AP Groups, RF Groups

Within the Cisco Unified Wireless Network there are three important group concepts:

- Mobility groups
- AP groups
- RF groups

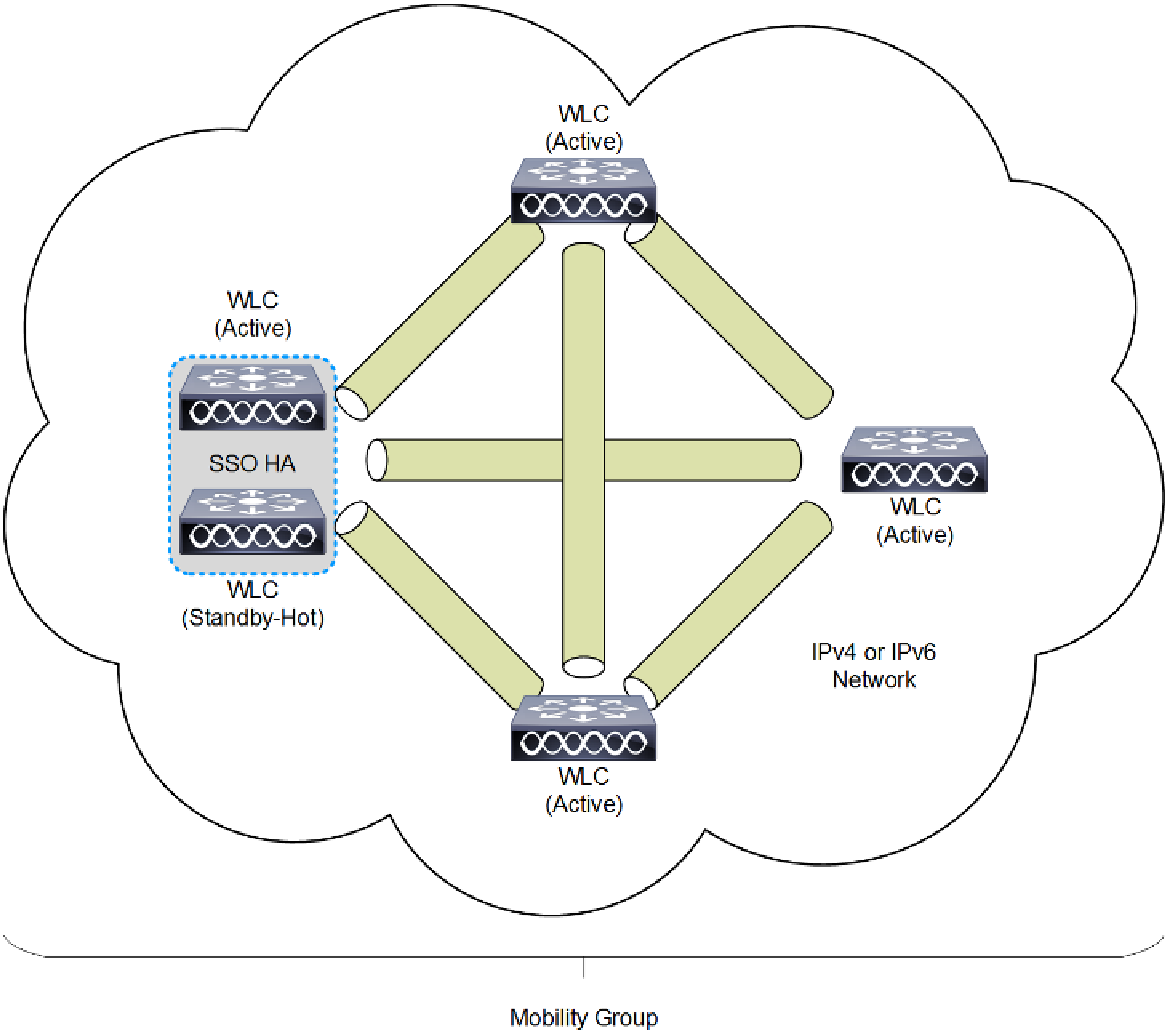
The following sections describe the purpose and application of these groups within the Cisco Unified Wireless Network.

Mobility Groups

A mobility group is a set of controllers, identified by the same mobility group name that defines the realm of seamless roaming for wireless clients. By creating a mobility group, you can enable multiple WLCs in a network to dynamically share essential client, AP and RF information as well as forward data traffic when inter-controller or inter-subnet roaming occurs. WLCs in the same mobility group can share the context and state of client devices as well as their list of access points so that they do not consider each other's access points as rogue devices. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

A mobility group forms a mesh of authenticated tunnels between member WLCs, thereby allowing any WLC to directly contact another WLC within the group, as shown in Figure 2-24.

Figure 2-24 WLC Mobility Group



In release 8.0 and above, mobility tunnels can be established between WLC peers using either Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6). The implementation of IPv4 or IPv6 tunnels is driven by the mobility configuration defined for each peer. Table 2-5 lists the protocol and ports implemented for each mobility tunnel version:

Table 2-5 Mobility Tunnel Protocols and Ports

Internet Protocol	IP Protocol	DST Port	Description
Version 4	17 (UDP)	16,666	IPv4 Mobility Tunnel Control Channel
	97 (EITHERIP)	-	IPv4 Mobility Tunnel Data Channel
Version 6	17 (UDP)	16,666	IPv6 Mobility Tunnel Control Channel
	17 (UDP)	16,667	IPv6 Mobility Tunnel Data Channel

Mobility Group Considerations

Creating a mobility group is simple and well documented. However, there are a few important considerations to keep in mind:

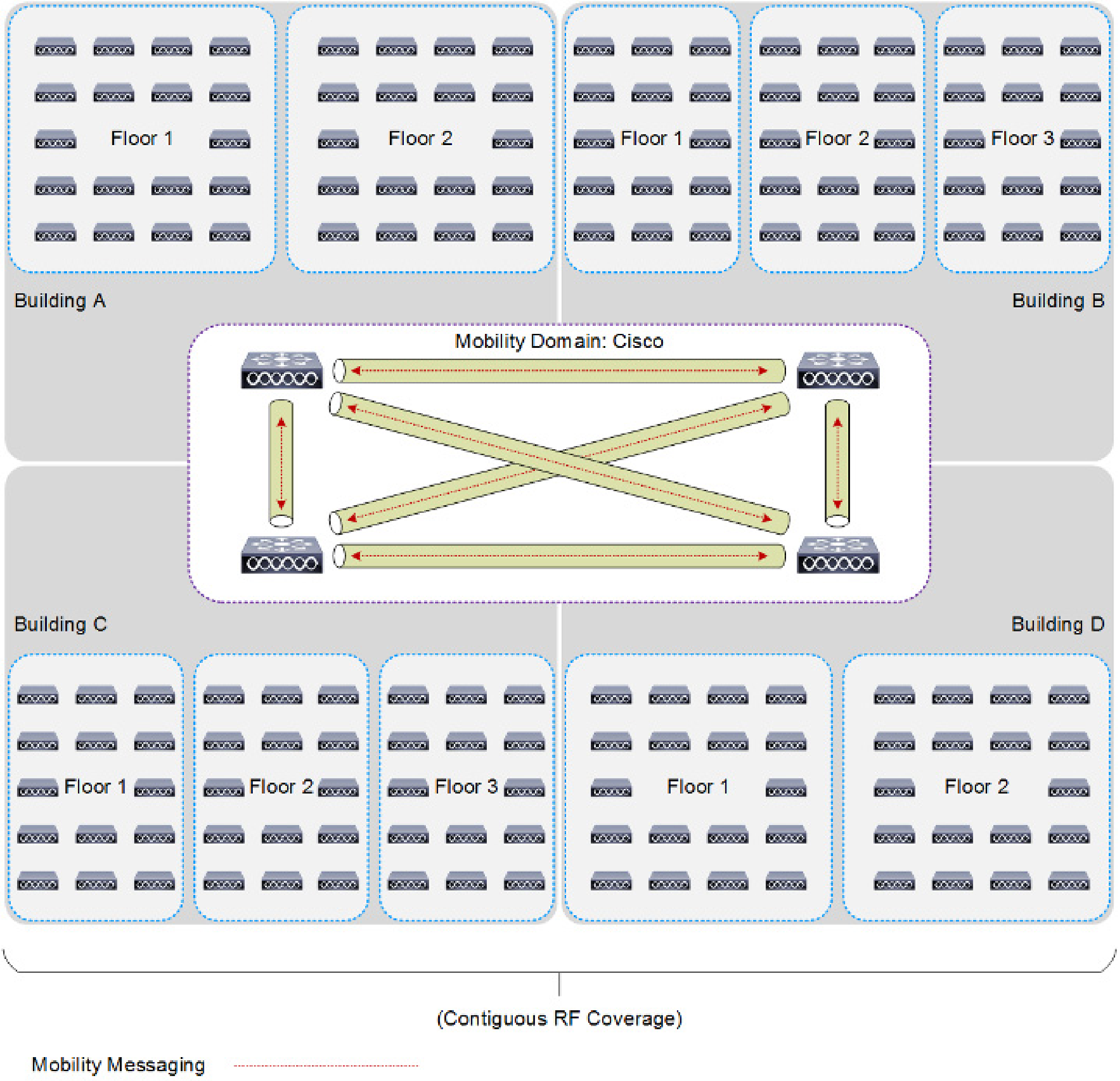
- Up to 24 x WLCs (any model) can be assigned to a single mobility group. A maximum of 144,000 APs are supported in a single mobility group (24 WLCs x 6,000 APs = 144,000 APs). An enterprise deployment can consist of more WLCs and APs, however they must be configured as members of a different mobility group.
- The WLCs do not have to be of the same model or type to be a member of a mobility group, however each member should be running the same software version.
- While mobility groups can function with software differences between members, Cisco strongly recommends you use a common software version to ensure feature and functional parity across the Cisco Unified Wireless Network deployment.
- If WLCs with switchover (SSO) are deployed, each WLC SSO pair is considered a single mobility peer.
- A mobility group requires all WLCs in the group to use the same virtual IP address.
- Each WLC must use the same Mobility Domain name and be defined as a peer in each other's Static Mobility Members list. The exception to this rule are when guest anchors are deployed where Cisco recommends deploying a separate Mobility Group for the guest anchors.
- For a wireless client to seamlessly roam between mobility group members (WLCs), a given WLAN SSID and security configuration must be consistent across all WLCs comprising the mobility group.
- As a Cisco best practice it is recommended that you enable the Multicast Mobility feature on all members of the mobility group. This feature requires a common Local Group Multicast IPv4 Address to be defined on each mobility group member.

Mobility Group Applications

Mobility groups are used to help facilitate seamless client roaming between APs that are joined to different WLCs. The primary purpose of a mobility group is to create a virtual WLAN domain (across multiple WLCs) in order to provide a comprehensive view of a wireless coverage area.

The use of mobility groups are beneficial only when a deployment comprises of overlapping coverage established by two or more APs that are connected to different WLCs. A mobility group provides no benefit when two APs, associated with different WLCs, are in different physical locations with no overlapping (contiguous) coverage between them. For example roaming between a campus and branch or between two or more branches.

Figure 2-25 Mobility Group Example



Mobility Group Exceptions

The Cisco Unified Wireless Network solution offers network administrators the ability to define static mobility tunnel (auto anchor) relationships between an anchor WLC and other WLCs in the network. This option, among other things, is used when deploying wireless guest access and BYOD services.

If the auto anchor feature is used, no more than 71 WLCs can be mapped to a designated anchor WLC. Foreign WLCs do not, by virtue of being connected to the auto anchor, establish mobility relationships between each other. The anchor WLC must have a static mobility group member entry defined for each foreign WLC where a static mobility tunnel is needed. The same is true for each foreign WLC where a static mobility tunnel is being configured; the anchor WLC must be defined as a static mobility group member in the foreign WLC.

A WLC can be member of only one mobility group for the purpose of supporting dynamic inter-controller client roaming. A WLC that is configured as an auto anchor does not have to be in the same mobility group as the foreign WLCs. It is possible for a WLC to be a member of one mobility group while at the same time, act as an auto anchor for a WLAN originating from foreign WLCs that are members of other mobility groups. For a discussion on mobility anchor configuration, see, Chapter 10, "**Cisco Unified Wireless Network Guest Access Services**."

AP Groups

An AP group is logical grouping of APs within a geographic area such as a building, floor or remote branch office that share common WLAN, RF, Hotspot 2.0 and location configurations. AP groups are useful in a Cisco Unified Wireless Network deployment as they allow administrators to assign specific configurations to different groups of APs. For example AP groups can be used to control which WLANs are advertised in different buildings in a campus, the interface or interface groups WLAN clients are assigned or the RRM and 802.11 radio parameters for radios in specific coverage areas to support high-density designs.

Supported AP group specific configurations include:

- CAPWAP Preferred Mode – Used to determine if the AP prefers IPv4 or IPv6 CAPWAP modes.
- NAS-ID – Used by the WLC for RADIUS authentication and accounting.
- WLAN – WLAN assignments, interface / interface group mappings and NAC state
- RF Profile Assignments – 802.11, RRM, high density and client load balancing configurations.
- Hotspot 2.0 – 802.11u venue configuration and languages.
- Location – HyperLocation configuration.

By default each AP is automatically assigned to a default AP group named "default-group" and WLANs IDs (1-16) map to this default group. WLANs with IDs greater than 16 require a custom AP group to be defined. When customized AP groups are defined on a WLC, the APs must be manually assigned to the AP group.

Note AP groups do not allow multicast roaming across group boundaries. For more information, see: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch5_QoS.html.

Table 2-6 Cisco Wireless Controller AP Group scaling (by platform)

Controller Platform	Max AP Groups	Max APs per AP Group
Cisco 2504 Wireless Controller	75	75
Cisco 5508 Wireless Controller	500	500
Cisco 5520 Wireless Controller	1,500	1,500
Cisco Flex 7500 Wireless Controller	6,000	6,000
Cisco 8510 Wireless Controller	6,000	6,000

Table 2-6 Cisco Wireless Controller AP Group scaling (by platform)

Controller Platform	Max AP Groups	Max APs per AP Group
Cisco 8540 Wireless Controller	6,000	6,000
Cisco Wireless Services Module 2	1,000	1,000
Cisco Virtual Wireless Controller	200	200

AP Group Considerations

Creating an AP group is simple and well documented. However, there are a few important considerations to keep in mind:

- If an AP does not belong to an AP group, it is assigned to the default AP group named "default-group" and will inherit any configurations applied to that group.
- As a Cisco best practice it is recommended that the customized AP group configurations on the primary, secondary and tertiary WLCs be consistent. If an AP joins a WLC with an undefined AP group name, the AP maintains its assigned AP group (NVRAM) but will inherit any configurations applied to the default-group. This can result in misconfigured APs and an undesirable user experience.
- Suppose that the interface mapping for a WLAN in the AP group table is the same as the WLAN interface. If the WLAN interface is changed, the interface mapping for the WLAN in the AP group table also changes to reflect the new WLAN interface.
- Suppose that the interface mapping for a WLAN in the AP group table is different from the one defined for the WLAN. If the WLAN interface is changed, then the interface mapping for the WLAN in the AP group table does not change to the new WLAN interface.
- If you clear the configuration on a controller, all of the AP groups (except the AP group named "default-group") will disappear.
- The default access point group can have up to 16 WLANs associated with it. The WLAN IDs for the default access point group must be less than or equal to 16. If a WLAN with an ID greater than 16 is created in the default access point group, the WLAN SSID will not be broadcasted. All WLAN IDs in the default access point group must have an ID that is less than or equal to 16. WLANs with IDs greater than 16 require a custom AP group to be defined.
- The OfficeExtend 600 Series access point supports a maximum of two WLANs and one remote LAN. If you have configured more than two WLANs and a remote LAN on the WLC, you must assign the Office Extend 600 Series APs to a customized AP group. The support for two WLANs and one remote LAN still applies to the default AP group. Additionally the WLAN/remote LAN ids must be lower than 8.
- All OfficeExtend access points should be in the same AP group, and that AP group should contain no more than 15 WLANs. A controller with OfficeExtend access points in an access point group publishes only up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID.
- Cisco recommends that you configure all FlexConnect APs (in the same branch / site) in the same AP group and FlexConnect group. This ensures that all the APs at a site inherit the correct WLAN-VLAN mappings.

AP Group Applications

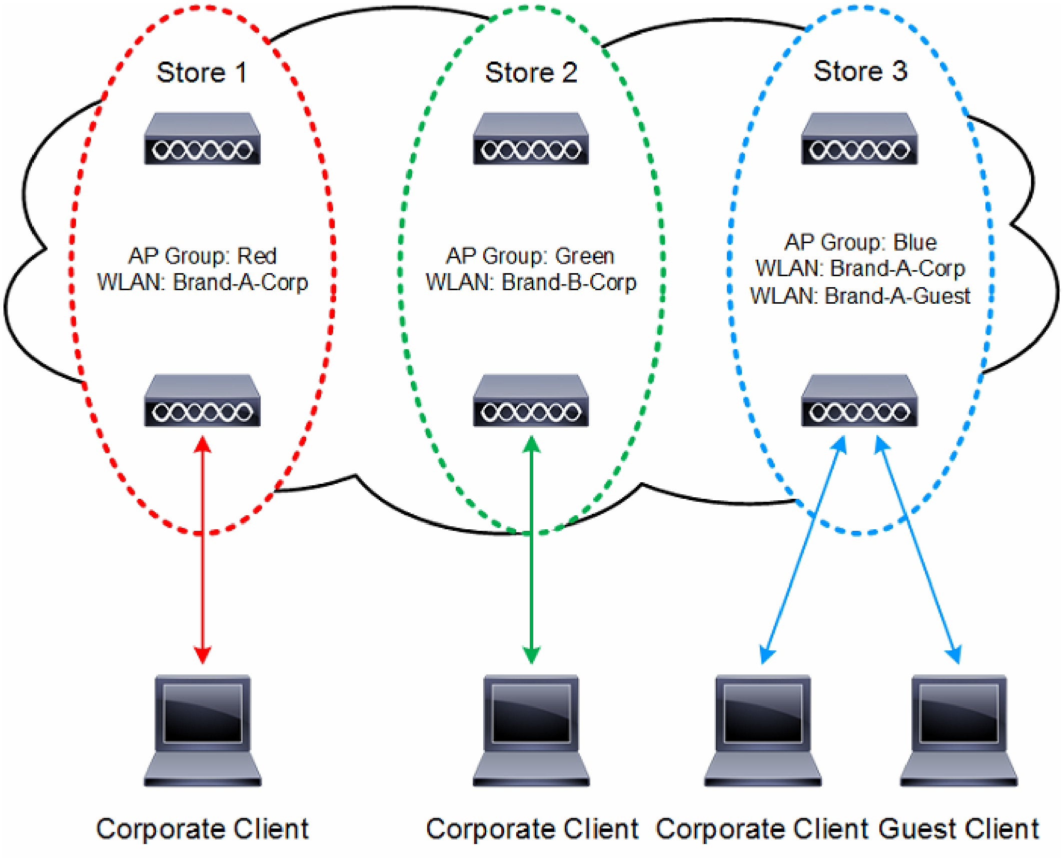
AP groups can be used to solve several business challenges within a Cisco Unified Wireless Network. This section provides some common use-cases where AP groups can solve these problems:

- Controlling which WLANs are advertised by APs within specific geographic locations. For example in a campus deployment separate AP groups can be employed to only advertise a guest WLAN in public areas vs. campus wide. For retail deployments AP groups can be employed to advertise unique SSIDs for different brands stores (mergers and acquisitions) or to provide guest Wi-Fi services to subsets of retail stores.

As shown in Figure 2-26 a WLC supporting remote FlexConnect APs has been configured with three separate AP groups to support remote retail stores of different brands and client support. Stores 1 and 3 are the same brand and both share a common corporate SSID, however a separate AP group is required for store 3 as this store it offers guest Wi-Fi to patrons which is not yet available in store 1.

Store 2 is a different brand that implements a different corporate SSID. A separate AP group is required to support store 2 as the client devices in the store have not yet been migrated to the standard corporate SSID.

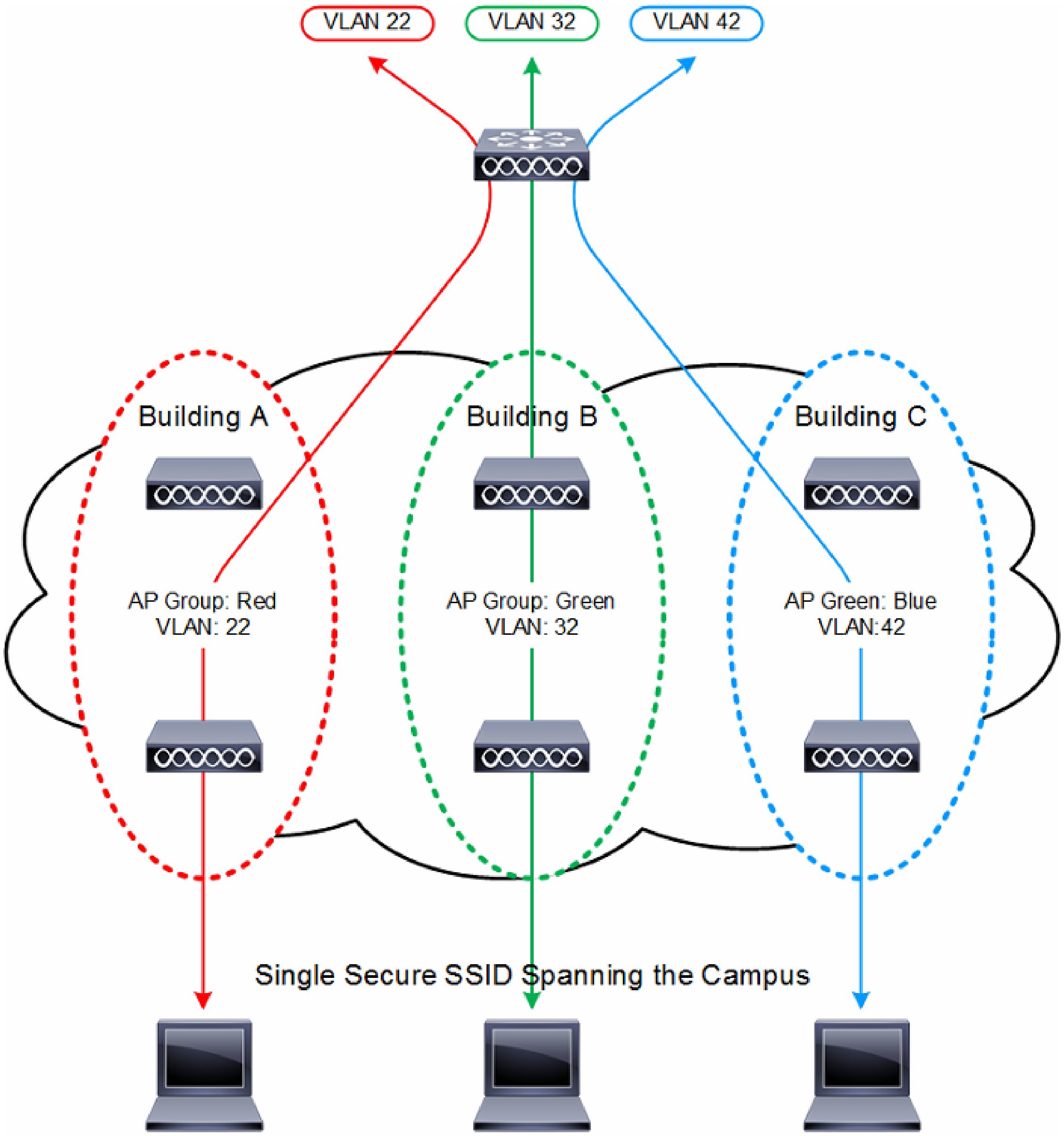
Figure 2-26 AP Groups for WLAN Assignments



- Reducing broadcast domain sizes by mapping WLAN clients to different interfaces or interface groups within a WLC. For example in a campus deployment, AP groups can be employed to map WLAN clients in separate buildings or floors to separate interfaces or interface groups on a single WLC.

As shown in Figure 2-27, a WLC has three dynamic interfaces configured, each with a site-specific VLAN (VLANs 22, 32 and 42). Each site-specific VLAN and associated APs are mapped to the same WLAN SSID using AP groups. A corporate user associating to the WLAN on an AP in the AP group corresponding to VLAN 22 is assigned an IP address on the VLAN 22 subnet. Likewise, a corporate user associating to the WLAN on an AP in the AP group corresponding to VLAN 32 is assigned an IP address on the VLAN 32 subnet and so on. Roaming between the site-specific VLANs is handled internally by the WLC as a Layer 3 roaming event and because of this the wireless LAN client maintains its original IP address.

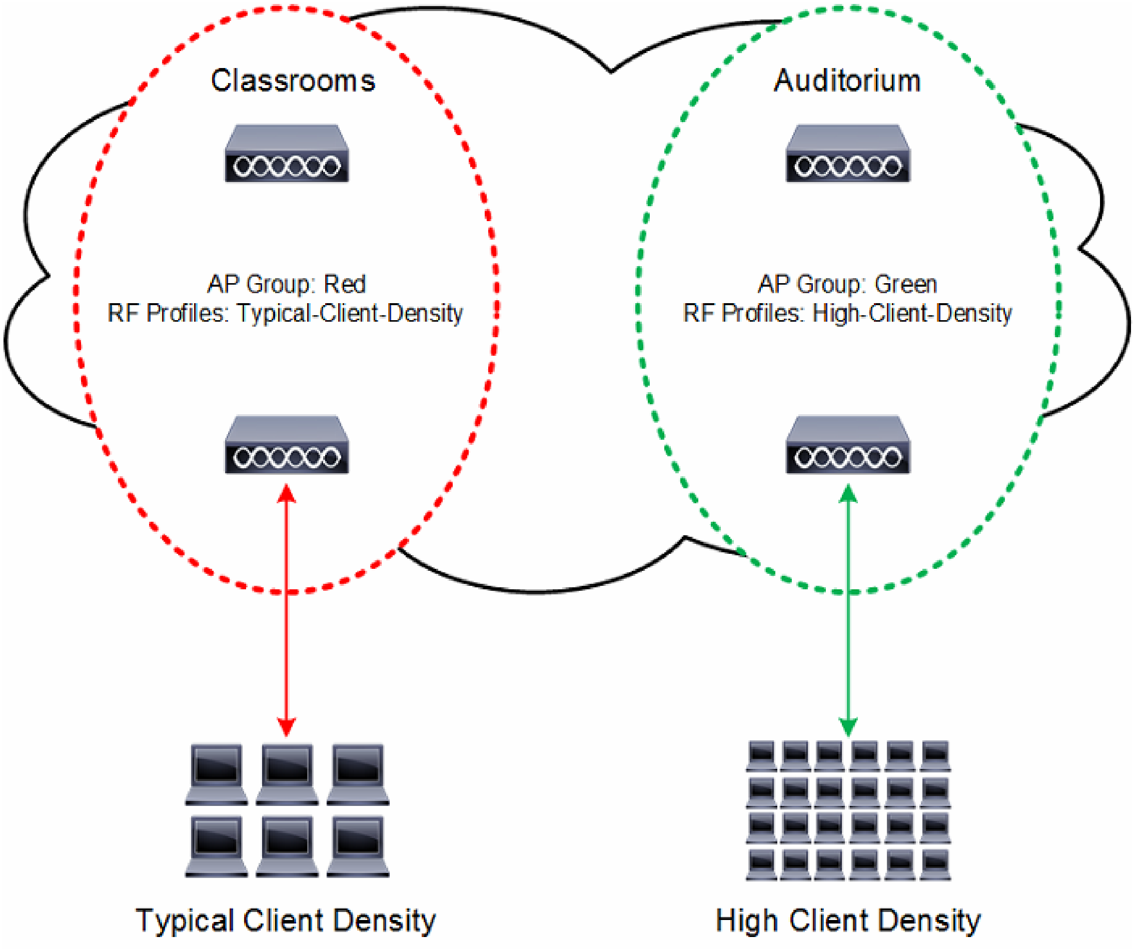
Figure 2-27 AP Groups for Interface / Interface Group Assignments



- Optimizing the RF environment within geographic locations to support different client densities. APs in coverage areas can be assigned different RF profiles optimized to support different client needs or densities.

As shown in Figure 2-28, a WLC has been configured with two AP groups to support different AP and client densities. One AP group is configured for APs and clients deployed in a typical density while the second AP group is configured to support APs and clients in a high density.

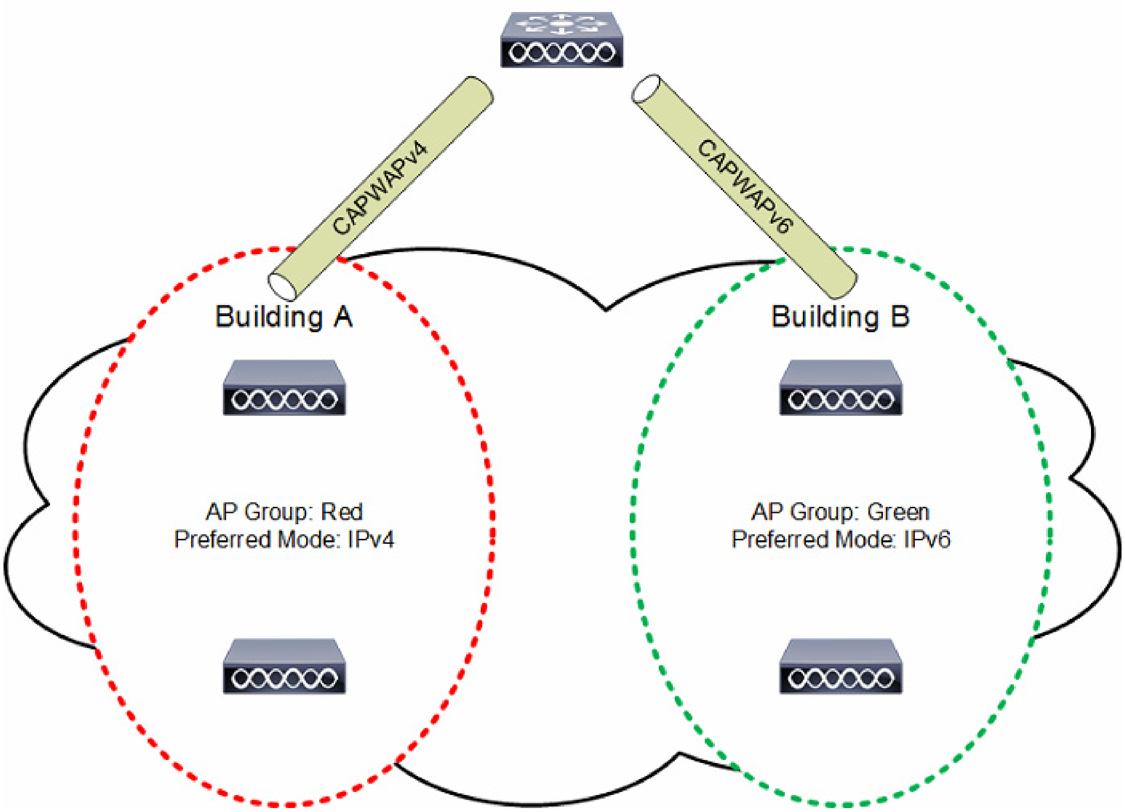
Figure 2-28 \AP Groups for RF Optimization & Client Densities



- Migrating APs from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6). AP groups can be employed to switch the APs CAPWAP preferred mode from IPv4 to IPv6 as individual buildings or sites are transitioned.

As shown in Figure 2-29, a WLC has been configured with two AP groups to aid in the transition from IPv4 to IPv6. Each AP group is configured with a specific CAPWAP preferred mode that determines the IP Protocol used by the APs when joining a WLC.

Figure 2-29 AP Groups for IPv6 Migrations



RF Groups

An RF group is a logical collection of Cisco WLCs that coordinate to perform RRM in a globally optimized manner to perform network calculations on a per-radio basis. An RF group exists for each 802.11 network type. Clustering Cisco WLCs into a single RF group enable the RRM algorithms to scale beyond the capabilities of a single Cisco WLC. Controller software can scale to support up to 20 WLCs and 6,000 APs in an RF group.

RF Groups and RRM is discussed in more detail in Chapter 3, WLAN RF Design Considerations” but can be summarized as follows:

- CAPWAP APs periodically send out neighbor messages over the air that includes the WLC IP address and a hashed message integrity check (MIC) derived from a timestamp and the BSSID of the AP.
- The hashing algorithm uses a shared secret (the RF Group Name) that is configured on the WLC and is pushed out to each AP. APs sharing the same secret are able to validate messages from each other using the MIC. When APs belonging to other WLCs hear validated neighbor messages at a signal strength of -80 dBm or stronger, their WLCs dynamically become members of the RF group.
- Members of an RF group elect an RF domain leader to maintain a master power and channel scheme for the RF group.
- The RF group leader analyzes real-time radio data collected by the system and calculates a master power and channel plan.

- The RRM algorithms attempt to:
    - Achieve a uniform (optimal) signal strength of -65 dBm across all APs
    - Avoid 802.11 co-channel interference and contention
    - Avoid non-802.11 interference.
- The RRM algorithms employ dampening calculations to minimize system-wide dynamic changes. The end result is dynamically calculated, near-optimal power and channel planning that is responsive to an ever changing RF environment.
- The RF group leader and members exchange RRM messages at a specified update interval, which is 600 seconds by default. Between update intervals the RF group leader sends keep alive messages to each of the RF group members and collects real-time RF data. Note that the maximum number of WLCs per RF group is 20.

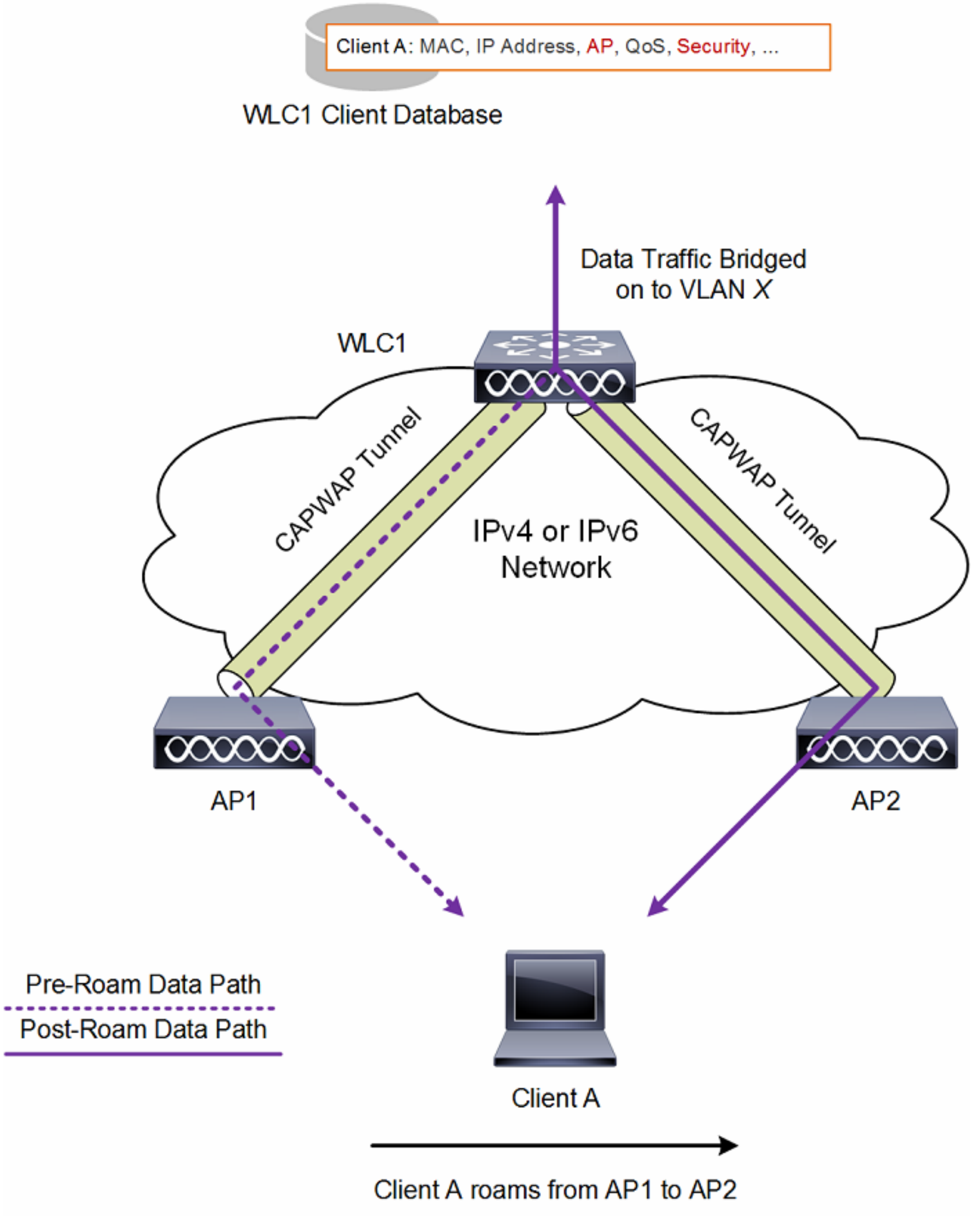
Note RF groups and mobility groups are similar in that they both define clusters of WLCs, but they are different in terms of their use. An RF group facilitates scalable, system-wide dynamic RF management while a mobility group facilitates scalable, system-wide mobility and WLC redundancy.

Roaming

Mobility, or roaming, is the ability of a WLAN client to maintain its association seamlessly from one AP to another securely and with as little latency as possible. This section explains how mobility works when WLCs are included in a Cisco Unified Wireless Network.

When a WLAN client associates and authenticates to an AP, the WLC places an entry for that client in its client database. This entry includes the client MAC and IP addresses, security context and associations, quality of service (QoS) contexts, the WLAN, SSID and the associated AP. The WLC uses this information to forward frames and manage traffic to and from the wireless client. Figure 2-30 shows a wireless client that roams from one AP to another when both APs are joined to the same controller.

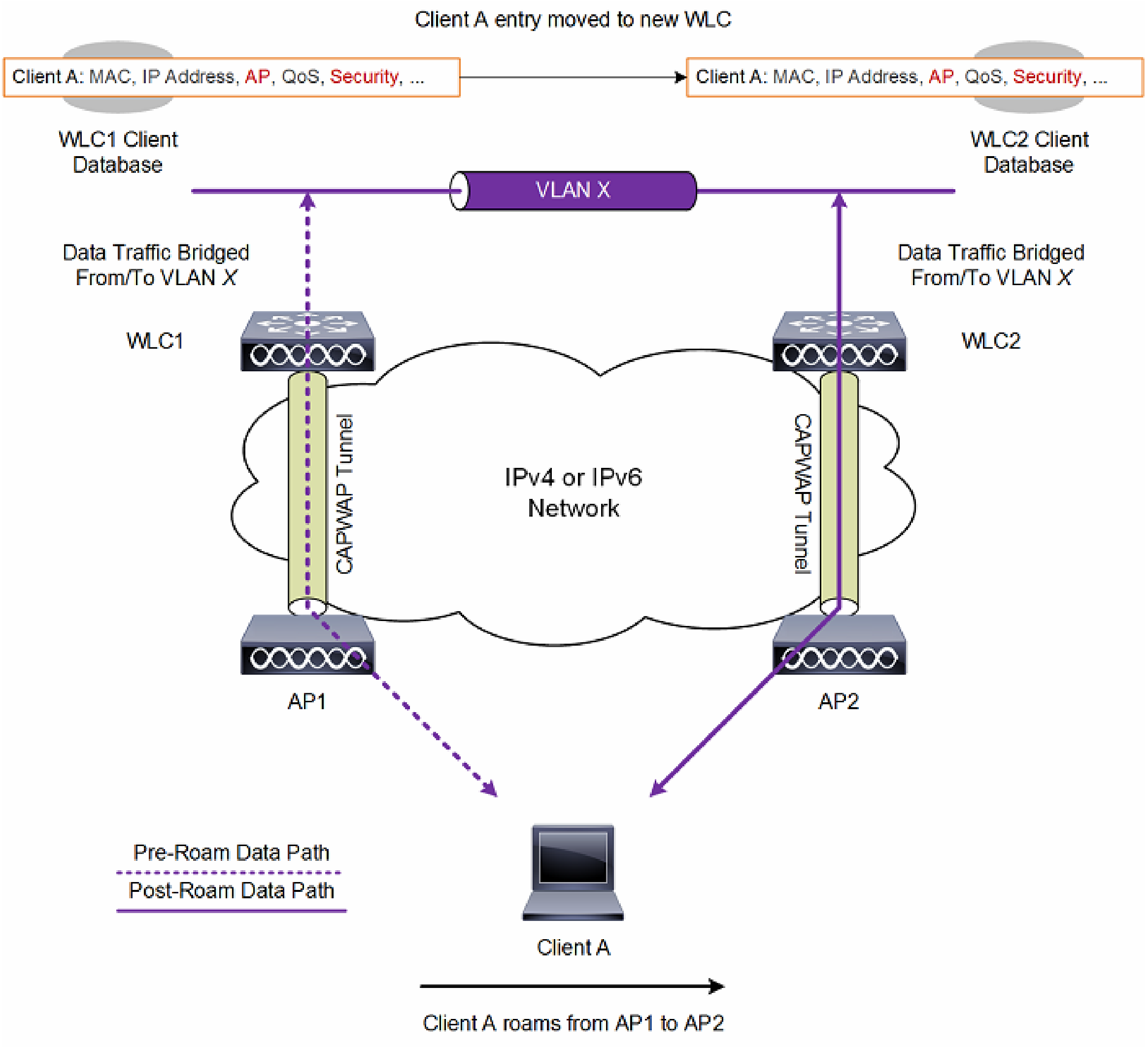
Figure 2-30 Intra-Controller Roaming



When the WLAN client moves its association from one AP to another, the WLC simply updates the client database with the newly associated AP. If necessary, new security context and associations are established as well.

The process becomes more complicated, however, when a client roams from an AP joined to one WLC to an AP joined to a different WLC. It also varies based on whether the WLCs are operating on the same VLAN. Figure 2-31 shows inter-controller roaming, which occurs when the WLCs interfaces or interface groups are support the same VLAN.

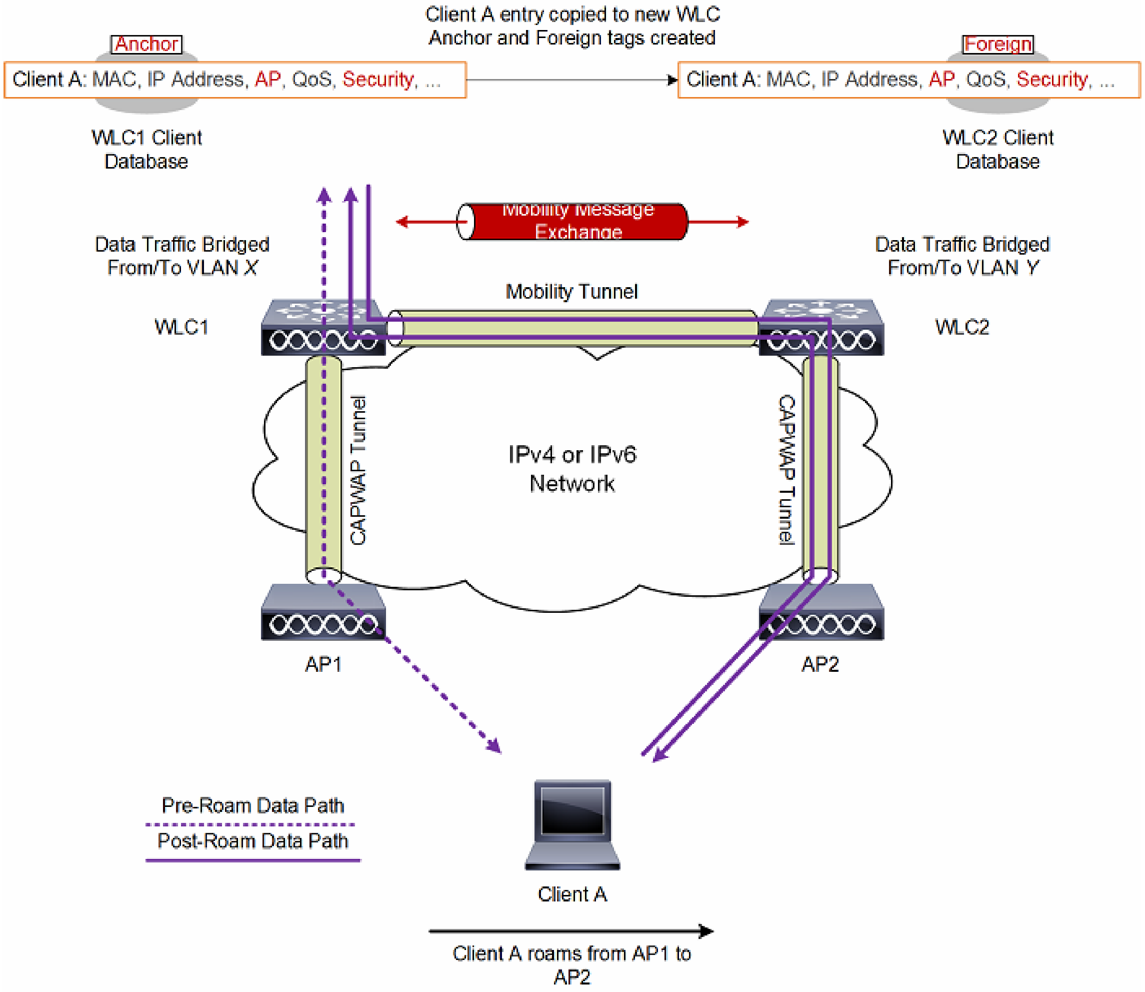
Figure 2-31 Inter-Controller Roaming


Client A entry moved to new WLC
Client A: MAC, IP Address, AP, QoS, Security, ...
Client A: MAC, IP Address, AP, QoS, Security, ...
WLC1 Client Database
WLC2 Client Database
VLAN X
Data Traffic Bridged From/To VLAN X
Data Traffic Bridged From/To VLAN X
WLC1
WLC2
CAPWAP Tunnel
IPv4 or IPv6 Network
CAPWAP Tunnel
AP1
AP2
Pre-Roam Data Path
Post-Roam Data Path
Client A
Client A roams from AP1 to AP2

When the client associates to an AP joined to a new controller, the new WLC exchanges mobility messages with the original WLC, and the client database entry is moved to the new WLC. New security context and associations are established if necessary, and the client database entry is updated for the new AP. This process remains transparent to the user.

Figure 2-32 shows inter-subnet roaming, which occurs when the WLCs interfaces are on different VLANs.

Figure 2-32 Inter-Subnet Roaming


Client A entry copied to new WLC
Anchor and Foreign tags created
Anchor
Client A: MAC, IP Address, AP, QoS, Security, ...
Foreign
Client A: MAC, IP Address, AP, QoS, Security, ...
WLC1 Client Database
WLC2 Client Database
Mobility Message Exchange
Data Traffic Bridged From/To VLAN X
Data Traffic Bridged From/To VLAN Y
Mobility Tunnel
WLC1
WLC2
CAPWAP Tunnel
IPv4 or IPv6 Network
CAPWAP Tunnel
AP1
AP2
Pre-Roam Data Path
Post-Roam Data Path
Client A
Client A roams from AP1 to AP2

Inter-subnet roaming is similar to inter-controller roaming in that the WLCs exchange mobility messages on the client roam. However, instead of moving the client database entry to the new WLC, the original controller marks the client with an Anchor entry in its own client database. The database entry is copied to the new controller client database and marked with a Foreign entry in the new WLC. The roam remains transparent to the wireless client, and the client maintains its VLAN membership and original IP address.

In inter-subnet roaming, WLANs on both anchor and foreign WLCs need to have the same network access privileges and no source-based routing or source-based firewalls in place. Otherwise, the clients may experience connectivity issues after the handoff.

Note If a client roams in web authentication state, the client is considered as a new client on another controller instead of considering it as a mobile client.

IPv6 Client Mobility

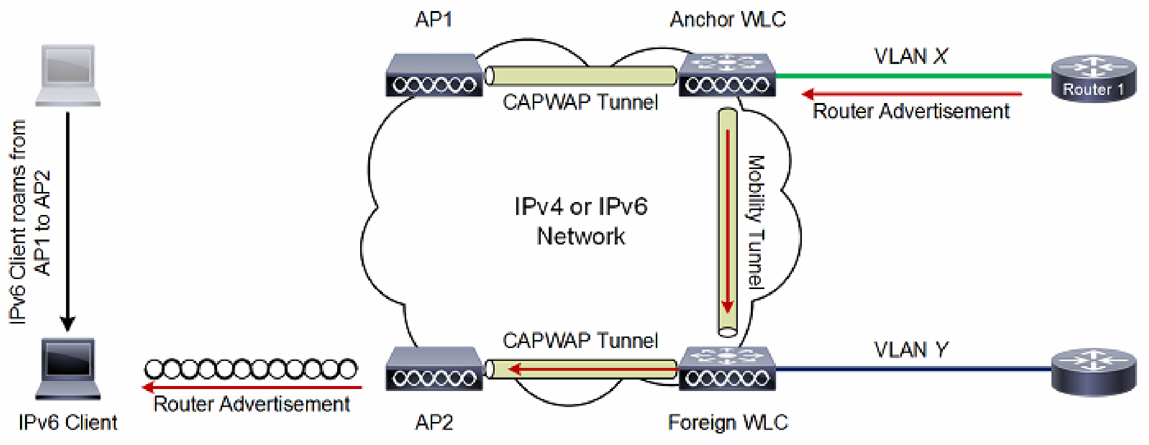
In order to accommodate roaming for IPv6 clients across WLCs, the ICMPv6 messages such as Neighbor Solicitations (NS), Neighbor Advertisements (NA), Router Advertisements (RA), and Router Solicitations (RS) must be dealt with to ensure that an IPv6 client remains on the same Layer 3 network. The configuration for IPv6 mobility is the same as for IPv4 mobility and requires no separate software on the client side to achieve seamless roaming. The only required configuration is the WLCs must be part of the same mobility group.

The process of IPv6 client mobility across WLCs is as follows:

- If both WLCs have access to the same VLAN the client was originally on, the roam is simply a Layer 2 roaming event where the client record is copied to the new WLC and no traffic is tunneled back to the anchor WLC.
- If the second WLC does not have access to the original VLAN the client was on, a Layer 3 roaming event will occur. All traffic from the client must be tunneled using a mobility tunnel to the anchor controller. In a mixed WLC deployment with release 7.x and 8.x, the mobility tunnels will be IPv4 based using EitherIP. In a pure 8.0 deployment, the mobility tunnels can be IPv4 or IPv6 based and will use EtherIP (IPv4) or CAPWAP (IPv6).
    - To ensure that the client retains its original IPv6 address, the RA's from the original VLAN are sent by the anchor WLC to the foreign WLC where they are delivered to the client using L2 unicast from the AP.
    - When the roamed client renews its address via DHCPv6 or generates a new address via SLAAC, the RS, NA, and NS packets continue to be tunneled to the original VLAN so that the client receives an IPv6 address that is applicable to its assigned VLAN.

Figure 2-33 shows inter-subnet roaming for IPv6 clients, which occurs when the WLCs interfaces are on different VLANs. The process is identical to inter-subnet roaming shown in Figure 2-32 where the roamed client's traffic is tunneled to the anchor WLC. All ICMPv6 RS, NA and NS packets are tunneled to the anchor WLC so that the IPv6 client can maintain its original VLAN and IPv6 address providing a seamless roaming experience.

Figure 2-33 IPv6 Inter-Subnet Roaming



Fast Secure Roaming

Before discussing the various fast roaming methods supported by a Cisco Unified Wireless Network (CUWN), it is important to understand how clients are authenticated and validated when connecting to a WPA2 WLAN using PSK or 802.1X key management. This information is important to provide additional context when understanding how fast secure roaming is implemented for each method.

Even though WPA/WPA2-PSK and WPA/WPA2-EAP methods authenticate and validate the WLAN clients in different ways, both use the same rules for the key management process. Whether the key management of a WPA2 WLAN is PSK or 802.1X, the process known as the 4-way handshake begins the key negotiation between the WLC/AP and the client with a Master Session Key (MSK) being used as the original key material once the client is validated with the specific authentication method used.

Here is a summary of the process:

- An MSK is derived from the EAP authentication phase when WPA/WPA2 with 802.1X key management is used, or from the pre-shared key when WPA/WPA2 with PSK is used.
- From the MSK, the client and WLC/AP derive the Pairwise Master Key (PMK).
- Once these two Master Keys have been derived, the client and the WLC/AP initiate the 4-Way handshake with the Master Keys as the seeds to negotiate the actual encryption keys:
    - Pairwise Transient Key (PTK) – The PTK is derived from the PMK and used in order to encrypt unicast frames with the client.
    - Group Transient Key (GTK) – The Group Transient Key (GTK) is derived from the GMK, and is used in order to encrypt multicast/broadcast on this specific SSID/AP.

Fast secure roaming aims to reduce the amount of time it takes a client to roam between APs in a CUWN. Fast roaming is achieved by implementing clever key management and distribution techniques that can avoid subsequent EAP authentications and/or the 4-way handshakes during a roam. Avoiding these phases reduces the amount of time it takes a client to reassociate to a new AP limiting the perceptible delay for time sensitive applications such as Voice over IP (VoIP).

The following section provides a brief overview of each of the supported fast secure roaming method available in the 8.0 release.

Note For more detailed information on each of the fast secure roaming methods described in this section (including packet captures and debugs), see the Cisco troubleshooting technote titled “802.11 WLAN Roaming and Fast-Secure roaming” at: http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html.

Cisco Centralized Key Management

Cisco Centralized Key Management (CCKM) is the first fast secure roaming method developed by Cisco for enterprise WLANs, as the solution to mitigate roaming delays when 802.1X/EAP security is enabled on a WLAN. As this is a Cisco proprietary protocol, it is only supported by Cisco and third-party clients that are Cisco Compatible Extension (CCX) compatible.

CCKM can be implemented with all of the different encryption methods available for WLANs including WEP, TKIP, and AES. It is also supports multiple EAP methods (dependent upon the CCX version supported by the client devices).

With CCKM, the initial association to the WLAN is similar to WPA/WPA2, where an MSK (also known here as the Network Session Key) is mutually derived from a successful authentication with a RADIUS server. This master key is sent from the server to the WLC after a successful authentication, and is cached as the basis for derivation of all subsequent keys for the lifetime of the client session. The WLC and client derive the seed information that is used for fast secure roaming based on CCKM, performing a 4-way handshake (similar to WPA/WPA2), in order to derive the unicast (PTK) and multicast/broadcast (GTK) encryption keys.

When a CCKM client roams to a new AP, it sends a single Reassociation Request frame to the CAPWAP AP (including an MIC and a sequentially incrementing Random Number), and provides enough information (including the new BSSID MAC address) in order to derive the new PTK. With this Reassociation Request, the WLC and new AP also have enough information in order to derive the new PTK, so they simply respond with a Reassociation Response, avoiding both the EAP authentication and 4-way handshake.

Summary:

- Is supported by Cisco and third-party clients that are CCX compatible.
- Supports different encryption and EAP methods (depending on CCX version).
- Fast roaming is performed by avoiding the 802.1X/EAP authentications and 4-way handshakes.
- Supported for both Centralized and FlexConnect deployments (locally or centrally switched):
  - Centralized – Works across APs and WLCs in the same Mobility group
  - FlexConnect – Works across APs in the same FlexConnect group
- FlexConnect WLANs can be configured for local or centralized authentication using central or local switching.
- FlexConnect APs are supported in connected or standalone modes – however there are restrictions as to how the MSK is shared in standalone mode.

Pairwise Master Key Caching

Pairwise Master Key (PMK) caching or Sticky Key Caching (SKC) is the first fast secure roaming method suggested by the IEEE 802.11 standard within the 802.11i security amendment. PMK caching allows the client to associate with an AP and upon a successful 802.1X/EAP authentication and 4-way handshake store the PMK in a cache. Should the client roam away from the AP and back again, the client can avoid the 802.1X/EAP authentication.

PMK caching is supported on WPA2 WLANs using 802.1X or PSK key management and requires both WLAN infrastructure and client support:

- The initial association to any AP is just like a regular first-time authentication to the WLAN, where a successful 802.1X or PSK authentication and the 4-way handshake must occur before the client is able to send data frames.
- If the wireless client roams to a new AP (where it has never previously associated), the client must perform a full 802.1X or PSK authentication and 4-way handshake again.

If the wireless client roams back to an AP (where it has previously associated), the client sends a Reassociation Request frame that lists multiple PMKIDs, which informs the AP of the PMKs cached from all of the APs where the client has previously authenticated. As the client is roaming back to an AP that also has a PMK cached for this client, it does not need to reauthenticate to derive a new PMK. The client simply goes through the WPA2 4-way handshake in order to derive the new transient encryption keys. The roam back has to occur within a limited time window configurable on the client (default 720 minutes in Windows).

In a CUWN centralized deployment, the cached PMKs for each CAPWAP AP are managed and maintained by the WLC. As separate PMKs are generated for each client per AP, scaling is limited. As such PMK caching is not recommended for large scale enterprise deployments and is not widely adopted.

Summary:

- Is referred to as Sticky Key Caching (SKC) in Cisco documentation.
- Is only supported for WPA2 WLANs using 802.1X or PSK key management.
- Due to the inefficient key management has severe scaling limitations which makes it unsuitable for large scale enterprise deployments. A WLC can only cache PMK entries for up to eight APs per client. Old cache entries are removed to store newly created entries if a client roams between more than 8 APs.
- Fast roaming is performed by avoiding 802.1X or PSK authentication during a roam. A fast roam is only provided if:
  - The client roams to an AP it has previously associated with.
  - The AP/WLC has the PMK cache entries for the client. In other words the cache entries have not been removed due to successive roams.
- Does not function across WLCs in a mobility domain. WLCs do not exchange PMKs with mobility peers.
- Not supported for FlexConnect deployments.

Proactive Key Caching

Proactive Key Caching (PKC) or pre-authentication is the second fast secure roaming method suggested by the IEEE 802.11 standard within the 802.11i security amendment. PKC was intended to be deployed with autonomous APs but has been adapted to work more efficiently in a CUWN (explained in more detail later).

PKC as it was intended to be implemented, allows a WPA2 802.1X client to carry out an 802.1X/EAP authentication with neighboring APs prior to roaming. The WPA2 client can perform the 802.1X authentication while connected to its current AP. Pre-authentication is achieved by the current AP relaying the EAPOL packets to neighboring APs which in turn query the RADIUS server and cache the PMK. The main challenge with pre-authentication is that there was no detection mechanism to determine how the neighboring APs were selected. As a result an initial client association could result in as many RADIUS authentications and PMKs as there were APs in the system.

A CUWN provides a more intelligent and efficient implementation by centrally caching and managing the clients PMKs. For this to function the APs must be under common administrative control, with a centralized device that caches and distributes the PMKs to all of the APs in the WLAN system. For a CUWN, the WLC performs this task for all the CAPWAP APs under its control and uses mobility messaging to exchange PMKs between other WLCs within its Mobility group. The clients cached PMK is used for the lifetime of the client’s session.

This fast secure roaming method avoids 80.1X/EAP authentication when roaming because it reutilizes the original PMK cached by the client and the WLCs. The client only has to perform a WPA2 4-way handshake in order to derive new encryption keys.

- Each time the wireless client connects to a specific AP, a PMKID is hashed based on: the client MAC address, the AP MAC address (BSSID of the WLAN), and the PMK derived with that AP. As PKC caches the same original PMK for all of the APs and the specific client, when a client roams to another AP, the only value that changes in order to hash the new PMKID is the new APs MAC address.
- When the client initiates roaming to a new AP and sends the Reassociation Request frame, it adds the PMKID on the WPA2 RSN Information Element if it wants to inform the AP that a cached PMK is used for fast secure roaming. As it already knows the MAC address of the BSSID (AP) for where it roams, then the client simply hashes the new PMKID that is used on this Reassociation Request. When the AP receives this request from the client, it also hashes the PMKID with the values that it already has (the cached PMK, the client MAC address, and its own AP MAC address), and responds with the successful Reassociation Response that confirms the PMKIDs matched. The cached PMK can be used as the seed that starts a WPA2 4-way handshake in order to derive the new encryption keys thus avoiding the EAP authentication phase.

Summary:

- Is referred to as Proactive Key Caching (PKC) in Cisco documentation but is not the same implementation as what has been defined as part of the 802.11i amendment.
- Is enabled by default for WPA2 WLANs using 802.1X key management.
- Fast roaming is performed by avoiding 802.1X/EAP authentications during a roam.
- Supported for centralized deployments.
- Provides scaling making it suitable for large scale enterprise deployments.
- Functions across WLCs in a mobility domain.
- Not supported for FlexConnect deployments.

Opportunistic Key Caching

Opportunistic Key Caching (OKC) and Proactive Key Caching (PKC) are used interchangeably by WLAN vendors but are not the same thing. The main difference between the two methods is that OKC is not defined by IEEE 802.11 and is therefore not a standard. OKC also operates differently PKC in how the PMKs are managed and distributed between the APs.

As previously discussed the main limitation of PKC (pre-authentication) was there was no mechanism in place to determine which neighboring APs pre-authenticated the client. A WPA2 client connection would result in as many RADIUS authentications and PMKs as there were APs in the system.

Vendors attempted to solve these inefficiencies with OKC by distributing the clients initial PMK to all the APs in a defined mobility zone. When a client connects it performs an 802.1X/EAP authentication and 4-way handshake and the derived PMK is distributed to all the APs in the zone the client is connected to. In affect the client is pre-authenticated on neighboring APs without each of the neighboring APs having to perform a RADIUS authentication. Fast roaming is performed when a client roams to another AP in the mobility zone by avoiding the 802.1X/EAP exchange.

The main disadvantage to OKC is in how the PMKs are distributed to the APs in the mobility zone. Unless the AP management / control protocol is secured using a mechanism such as Datagram Transport Layer Security (DTLS), the PMKs are distributed insecurely.

In a CUWN, OKC is supported by default on WPA2 WLANs using 802.1X key management for FlexConnect deployments. In a FlexConnect deployment the mobility zone that defines the APs the PMKs are distributed to is the FlexConnect group. When client successfully authentications, the WLC distributes the PMK to all the APs in the FlexConnect group. As Cisco's implementation of CAPWAP is secured using DTLS, the PMK key distribution is secure.

As the PMK distribution is managed by the WLC it requires all of the FlexConnect APs to be in connected mode. If the FlexConnect APs at a site transition into standalone mode, fast secure roaming can only be provided for existing clients.

Summary:

- Opportunistic Key Caching (OKC) is used interchangeably with Proactive Key Caching (PKC), however they are not the same thing.
- Is not defined as an IEEE 802.11 standard.
- Is enabled by default for WPA2 WLANs using 802.1X key management for FlexConnect deployments.
- Fast roaming is performed by avoiding 802.1X/EAP authentications during a roam.
- Supported for FlexConnect only (locally or centrally switched).
- FlexConnect APs must be in connected mode when the PMK is initially derived.
- Functions across APs in the same FlexConnect group that are associated to the same WLC.

Fast Secure Roaming with 802.11r

802.11r (officially named Fast BSS Transition by the 802.11 standard, and known as FT), is the first fast secure roaming method officially ratified by the IEEE as the solution to perform fast transitions between APs. The 802.11r amendment was officially ratified in 2008 and clearly defines the key hierarchy that is used to handle and cache keys on a WLAN.

This technique is more complex to explain than the other methods, as it introduces new concepts and multiple layers of PMKs that are cached on different devices (each device with a different role), and provides even more options for fast secure roaming. Therefore, a brief summary is provided about this method and the way it is implemented with each option available.

- Handshake messaging (PMKID, ANonce, and SNonce exchange, for example) happens in 802.11 Authentication frames or in Action frames instead of Reassociation frames. Unlike PMKID caching methods, the separate 4-way handshake phase, which is carried after the (re)association message exchange, is avoided. The key handshake with the new AP begins before the client fully roams/reassociates with this new AP.
- It provides two methods for the fast roaming handshake: over the AIR, and over the Distribution System (DS).
- 802.11r has more layers of key hierarchy.
- As this protocol avoids the 4-way handshake for the key management when a client roams (generates new encryption keys PTK and GTK without the need of this handshake), it can also be applied for WPA2 setups with a PSK, and not only when 802.1X/EAP is used for the authentication. This accelerates the roaming even more for these setups, where no EAP or 4-way handshake exchanges occur.

With 802.11r, the wireless client performs just one initial authentication against the WLAN infrastructure when a connection is established to the first AP, and performs fast secure roaming while roaming between APs within the same FT mobility domain. APs that use the same SSID (known as an Extended Service Set or ESS) handle the same FT keys. The way the APs handle the FT mobility domain keys is identical to PKC/OKC. For a CUWN, the WLC performs this task for all the CAPWAP APs under its control and uses mobility messaging in order to exchange FT keys between other WLC peers within its Mobility group.

Here is a summary of the key hierarchy:

- An MSK is still derived on the client supplicant and RADIUS server from the initial 802.1X/EAP authentication phase (transferred from the RADIUS server to the WLC once the authentication is successful). This MSK is used as the seed for the FT key hierarchy. When you use WPA2-PSK instead of an EAP authentication method, the PSK is the MSK.
- A Pairwise Master Key R0 (PMK-R0) is derived from the MSK, which is the first-level key of the FT key hierarchy. The key holders for this PMK-R0 are the WLC and the client.
- A second-level key, called a Pairwise Master Key R1 (PMK-R1), is derived from the PMK-R0, and the key holders are the client and the APs managed by the WLC that holds the PMK-R0.
- The third and final level key of the FT key hierarchy is the PTK, which is the final key used in order to encrypt the 802.11 unicast data frames (similar to the other methods that use WPA/TKIP or WPA2/AES). This PTK is derived on FT from the PMK-R1, and the key holders are the client and the APs managed by the WLC.

802.11r is supported by default for both Centralized and FlexConnect deployments (centralized or local switching). To be supported by FlexConnect the WLAN authentication must be centralized. 802.11r is not supported on FlexConnect APs using local authentication or FlexConnect APs operating in standalone mode. FlexConnect APs within a given 802.11r roaming domain should belong to the same FlexConnect group.

Summary:

1. Only supported on WPA2 WLANs using PSK or 802.1X key management.
2. Fast roaming is performed by avoiding 802.1X/EAP authentications and 4-way handshakes during a roam.
3. Supported for both Centralized and FlexConnect (centralized or locally switched) deployments:
    a. Centralized – Works across WLCs in the same Mobility group.
    b. FlexConnect – Works across APs in the same FlexConnect group.
4. FlexConnect requires WLANs to be configured for centralized authentication, local authentication is not supported. Fast secure roaming is not supported on FlexConnect APs operating in standalone mode.

Note For Additional details on IEEE 802.11r and other 802.11 amendments, please see 802.11r Fast Transition Roaming

Considerations

The following provides some considerations that need to be made when selecting a fast secure roaming method for WLANs:

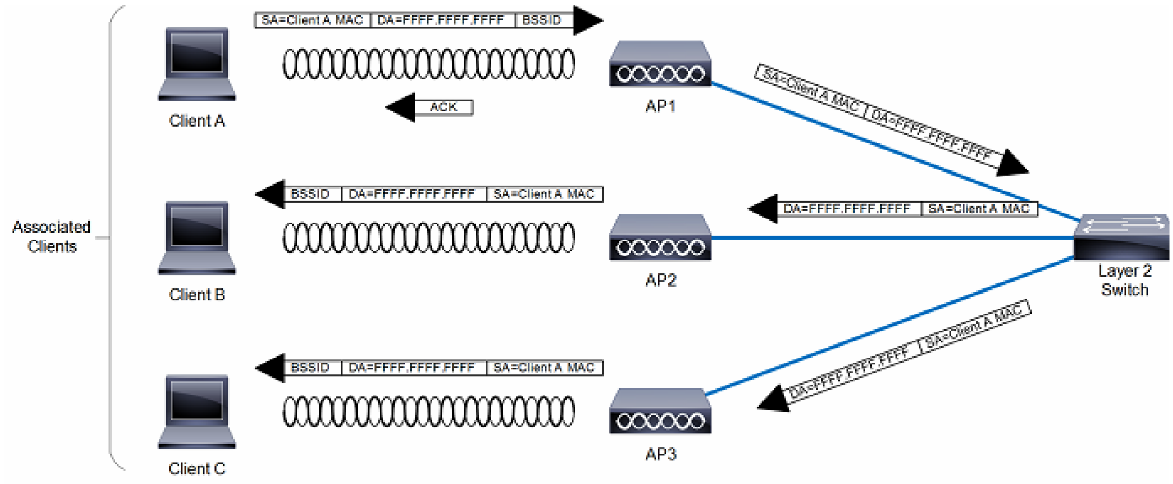
- It is very important to understand that fast secure roaming methods are developed in order to accelerate the roaming process when clients move between APs on WPA2 WLANs with security enabled. When no WLAN security is in place, there is no 802.1X/EAP authentication or 4-way handshake that can be avoided to accelerate the roam.
- 802.11r is the only fast secure roaming method that supports WPA2-PSK. 802.11r accelerates WPA2-PSK roaming events avoiding the 4-way handshake.

- None of the fast secure roaming methods will work in FlexConnect deployments when WLANs are configured for local authentication. If local authentication is enabled, the clients will perform a full authentication during a roam.
- All of the fast secure roaming methods have their advantages and disadvantages, but in the end, you must verify that the wireless client stations support the specific method that you want to implement. You must select the best method that is supported by the wireless clients that connect to the specific WLAN/SSID. For example, in some deployments you might create a WLAN with CCKM for Cisco wireless IP Phones (which support WPA2/AES with CCKM, but not 802.11r), and then another WLAN with WPA2/AES via 802.11r/FT for wireless clients that support 802.11r (or use OKC/PKC, if this is what is supported).
- If the 802.1X clients do not support any of the fast secure roaming methods available, those clients will always experience delays when roaming between APs. The 802.1X clients will need to perform a full 802.1X/EAP authentication and 4-way handshake during a roaming event. This can cause disruptions to applications and services.
- All fast secure roaming methods (except PMKID/SKC) are supported between APs managed by different WLCs (inter-controller roaming), as long as the WLCs are members of the same Mobility group.

Broadcast and Multicast on the WLC

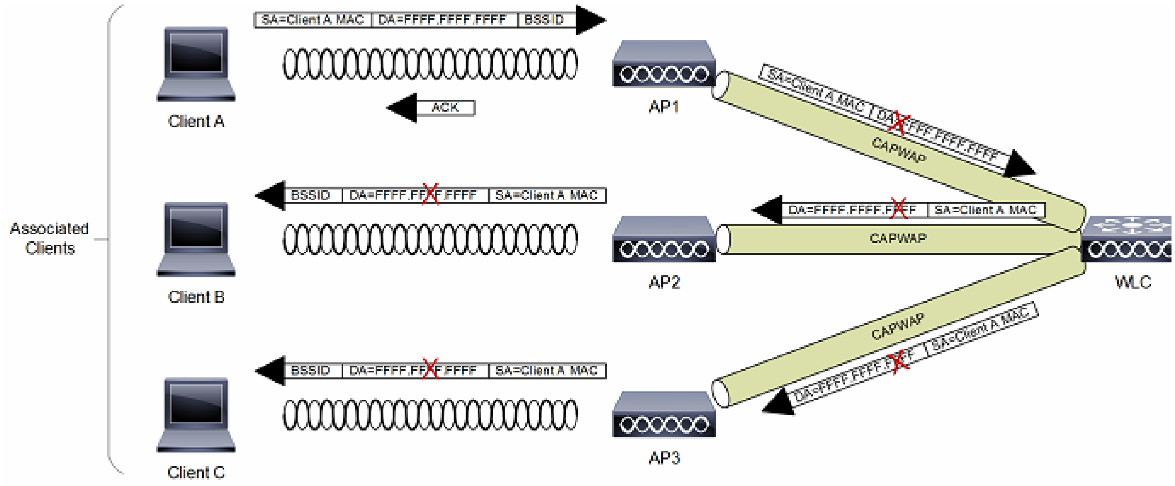
The section discusses the handling of broadcast and multicast traffic by a WLC and its impact on design. Figure 2-34 depicts basic 802.11 broadcast/multicast behavior. In this example, when Client 1 sends an 802.11 broadcast frame it is unicasted to the AP. The AP then sends the frame as a broadcast out both of its wireless and wired interfaces. If there are other APs on the same wired VLAN as the AP, they also forward the wired broadcast packet out their wireless interface.

Figure 2-34 802.11 Broadcast / Multicast Behavior


SA=Client A MAC | DA=FFFF.FFFF.FFFF | BSSID
ACK
Client A
AP1
SA=Client A MAC | DA=FFFF.FFFF.FFFF
Associated Clients
BSSID | DA=FFFF.FFFF.FFFF | SA=Client A MAC
DA=FFFF.FFFF.FFFF | SA=Client A MAC
Client B
AP2
Layer 2 Switch
BSSID | DA=FFFF.FFFF.FFFF | SA=Client A MAC
DA=FFFF.FFFF.FFFF | SA=Client A MAC
Client C
AP3

The WLC CAPWAP split MAC method treats broadcast traffic differently, as shown in Figure 2-35. In this case, when a broadcast packet is sent by a client, the AP/WLC does not forward it back out the WLAN, and only a subset of all possible broadcast messages are forwarded out a given WLAN's wired interface at the WLC.

Figure 2-35 Default WLC Broadcast Behavior


SA=Client A MAC | DA=FFFF.FFFF.FFFF | BSSID
ACK
Client A
AP1
SA=Client A MAC | DA=FFFF.FFFF.FFFF
CAPWAP
Associated Clients
BSSID | DA=FFFF.FFFF.FFFF | SA=Client A MAC
DA=FFFF.FFFF.FFFF | SA=Client A MAC
CAPWAP
Client B
AP2
WLC
CAPWAP
BSSID | DA=FFFF.FFFF.FFFF | SA=Client A MAC
DA=FFFF.FFFF.FFFF | SA=Client A MAC
Client C
AP3

Note The protocols forwarded under which situations is discussed in the following section.

WLC Broadcast and Multicast Details

Broadcast and multicast traffic often require special treatment within a WLAN network because of the additional load placed on the WLAN as a result of this traffic having to be sent at the lowest common data rate. This is done to ensure that all associated wireless devices are able to receive the broadcast / multicast information.

The default behavior of the WLC is to block broadcast and multicast traffic from being sent out the WLAN to other wireless client devices. The WLC can do this without impacting client operation because most IP clients do not send broadcast / multicast type traffic for any reason other than to obtain network information (DHCP).

DHCP

The WLC acts as a DHCP relay agent for associated WLAN clients. The WLC unicasts client DHCP requests to a locally configured or upstream DHCP server except during Layer 3 client roaming (discussed in more detail below). DHCP server definitions are configured for each dynamic interface, which in turn is associated with one or more WLANs. DHCP relay requests are forwarded by way of the dynamic interfaces using the source IP address of a given dynamic interface. Because the WLC knows which DHCP server to use for a given interface/WLAN, there is no need to broadcast client DHCP requests out its wired and wireless interfaces.

This method accomplishes the following:

- It eliminates the need for DHCP requests to be broadcasted beyond the WLC.
- The WLC becomes part of the DHCP process, thereby allowing it to learn the MAC/IP address relationships of connected WLAN clients, which in turn allows the WLC to enforce DHCP policies and mitigate against IP spoofing or denial-of-service (DoS) attacks.

VideoStream

The VideoStream feature makes the IP multicast stream delivery reliable over the air, by converting the broadcast frame over the air to a unicast frame. Each VideoStream client acknowledges receiving a video IP multicast stream. VideoStream is supported on all Cisco APs.

The following are the recommended guidelines for configuring VideoStream on the controller:

- The AP1100 and AP1200 do not support the reliable multicast feature.
- Ensure that the multicast feature is enabled. As a best practice Cisco recommends configuring IP multicast on the controller with multicast-multicast mode.
- Check for the IP address on the client device. The device should have an IP address from the respective VLAN.
- Verify that the AP has joined the controllers.
- Ensure that the clients are able to associate to the configured WLAN at 802.11a/n/ac speed.

Other Broadcast and Multicast Traffic

As mentioned earlier, the WLC (by default) does not forward broadcasts or multicasts toward the wireless users. If multicast forwarding is explicitly enabled, as described in **Chapter 6, "Chapter 6, "Cisco Unified Wireless Multicast Design""**, steps should be taken to minimize the multicast traffic generated on those interfaces that the WLC connects to.

All normal precautions should be taken to limit the multicast address groups explicitly supported by a WLAN. When multicast is enabled, it is global in nature, meaning it is enabled for every WLAN configured regardless if multicast is needed by that WLAN or not. The Cisco Unified Wireless Network solution is not able to distinguish between data link layer and network layer multicast traffic, nor is the WLC capable of filtering specific multicast traffic. Therefore, the following additional steps should be considered:

- Disable CDP on interfaces connecting to WLCs.
- Port filter incoming CDP and HSRP traffic on VLANs connecting to the WLCs.
- Keep in mind that multicast is enabled for all WLANs on the WLC, including the guest WLAN; therefore multicast security including link layer multicast security must be considered.

Design Considerations

For a Cisco Unified Wireless Network deployment, the primary design considerations are WLC location and AP/WLC connectivity. This section will briefly discuss these topics for centralized (local-mode) AP deployments and make general recommendations where appropriate. Recommendations and design considerations for FlexConnect AP deployments are not covered in this section and are instead discussed in Chapter 7, “FlexConnect”.

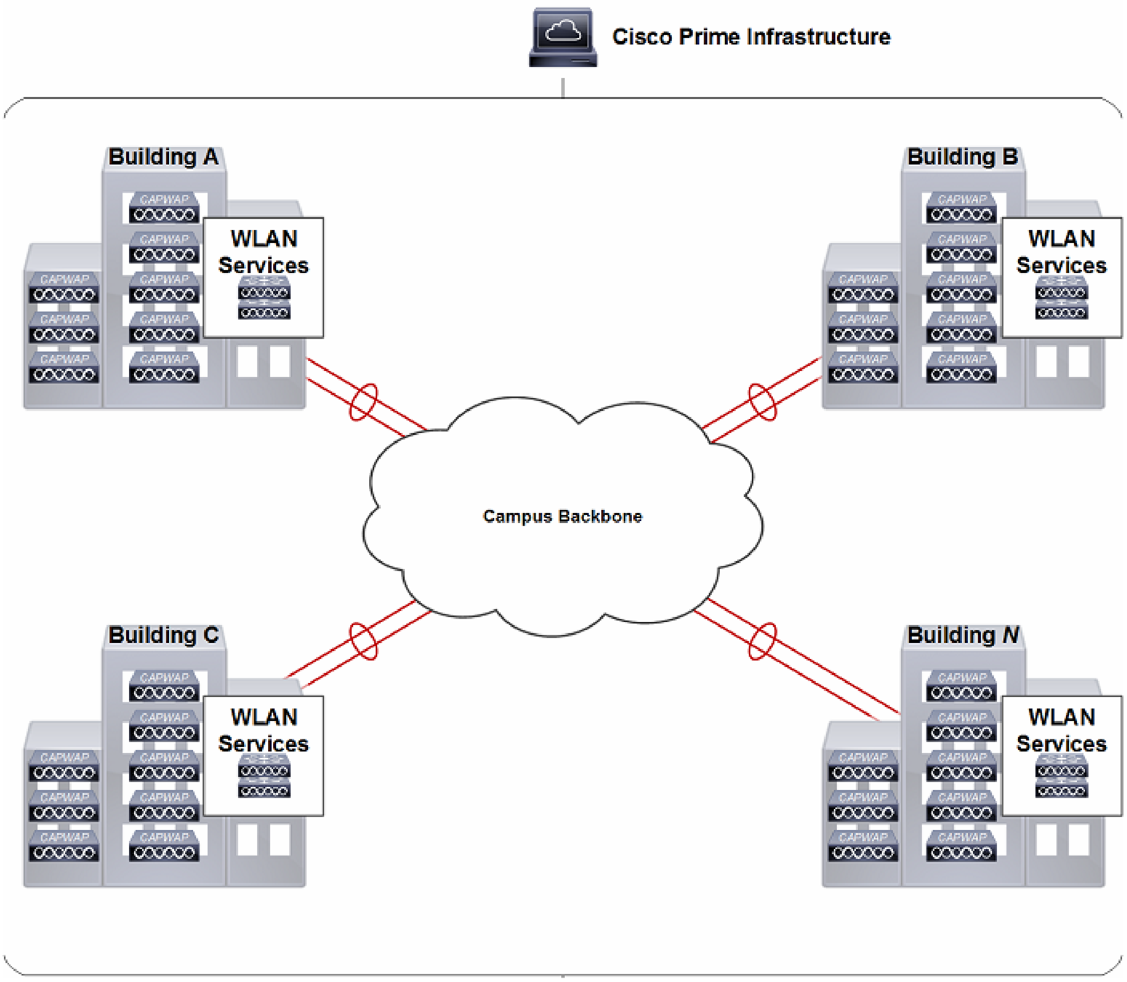
WLC Location

A Cisco Unified Wireless Network allows the WLCs to be centrally located or distributed within a campus depending on the size and type of the deployment. The different deployment types and considerations are described in the following sections.

Distributed WLC Deployment

Figure 2-36 illustrates a distributed WLC deployment. In this model the WLCs are located throughout the campus network, typically on a per building basis, to manage the APs that are resident in the given building. The WLCs are connected to the campus network by way of the distribution layer switches within each building. In this scenario the CAPWAP tunnels between the APs and the WLC stay within each building.

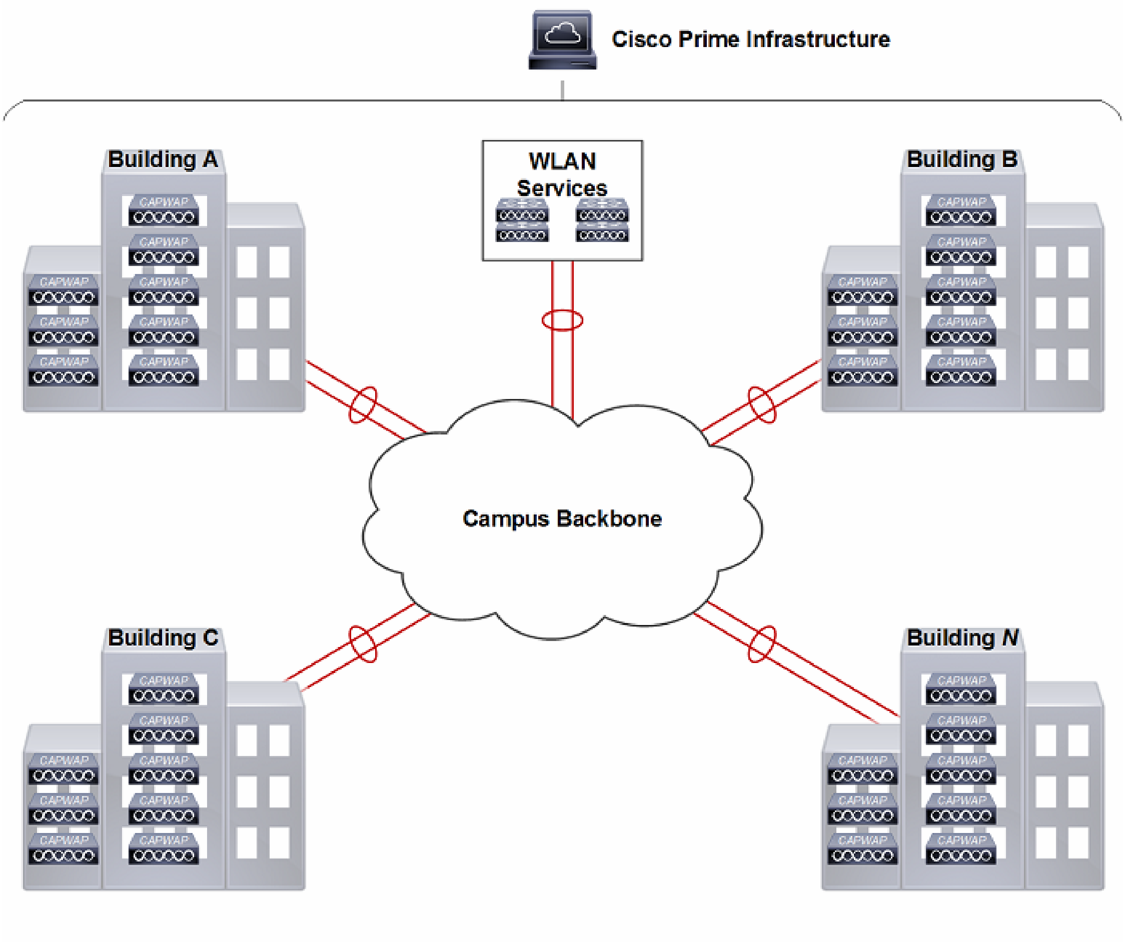
Figure 2-36 FWLCs in Distributed Deployment



Centralized WLC Deployment

Figure 2-37 illustrates a centralized WLC deployment. In this model, WLCs are placed at a centralized location in the campus network. This deployment model requires the CAPWAP tunnels to traverse the campus backbone network. Note in the illustration that the centralized WLCs are not shown in a specific building. The centralized pool of WLCs are connected by way of a dedicated switch block to the campus core, which is typically located in the same building as the data center. The WLCs should not be connected directly to the data center switching block because network and security requirements within data center are generally different than that of the WLC pool.

Figure 2-37 Centralized WLCs in a Campus



Reference Architectures

Cisco's recommendation for the WLC placement is dependent on the size and scale of the Cisco Unified Wireless Network deployment. The following section provides reference architectures with recommended WLC placement and redundancy configuration for small, medium, large and very large campus networks each based on Cisco's hierarchical design principles. A reference architecture for a remote branch office deployment using local-mode APs is also provided at the end this section.

Note Additional details for Cisco validated designs and best practices can be viewed at: http://www.cisco.com/c/en/us/solutions/enterprise/design-zone/index.html

Small Campus

Figure 2-38 shows the recommended WLC placement for a CUWN deployment for a small campus network implementing a distribution layer operating as a collapsed core. The distribution layer provides connectivity to the WLCs, WAN and Internet edge. Depending on the size of the LAN, the WLCs may connect directly to distribution layer or be connected by means of a dedicated switch block (as shown). The small campus in this example is a single building with multiple access layer switches.

Figure 2-38 Small Campus Reference Design

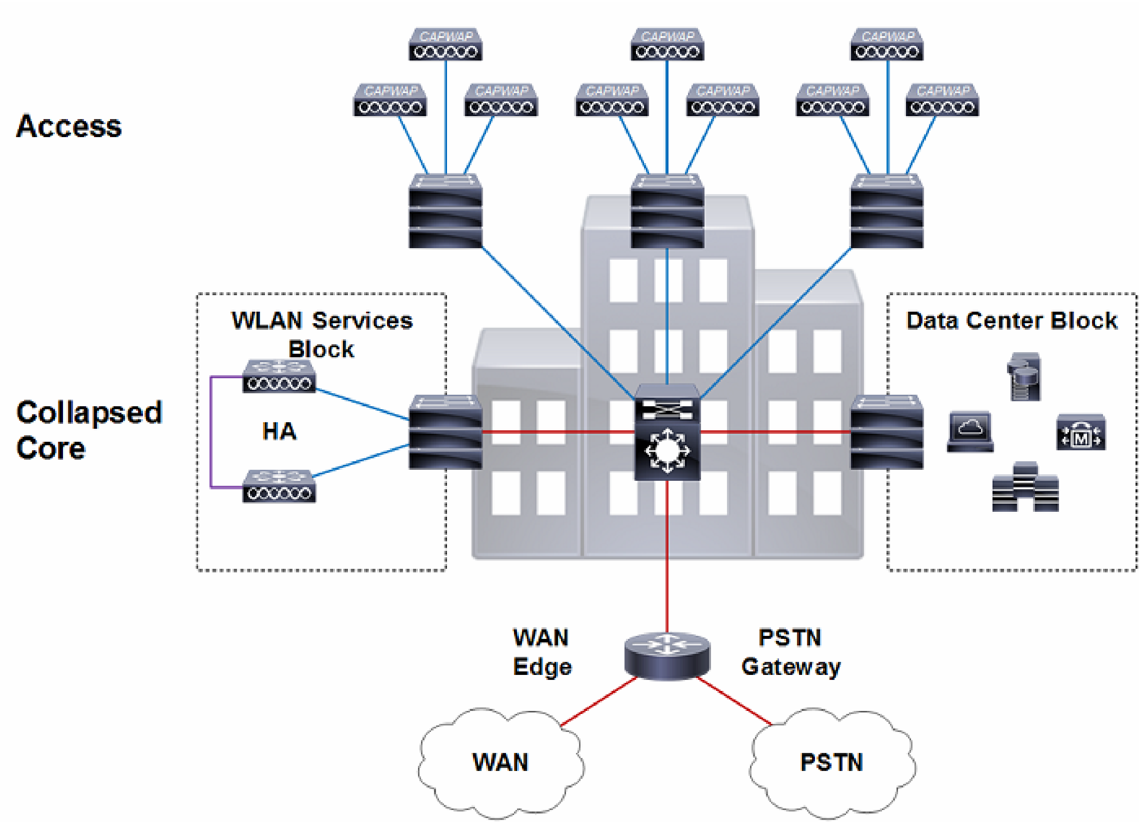
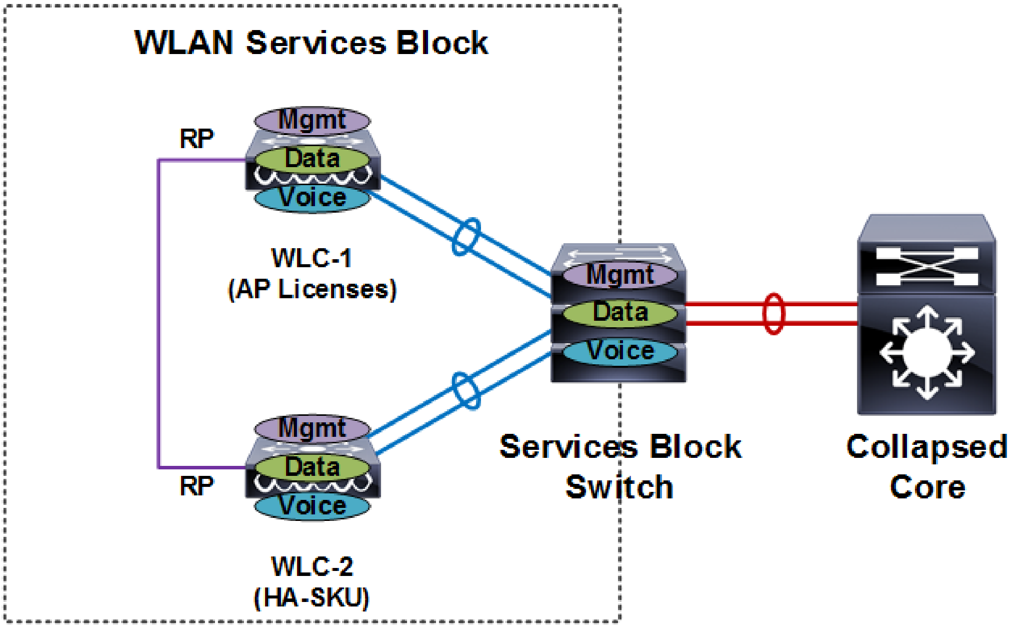


Figure 2-39 shows additional details for the wireless services block for a small campus network deployment. In this example a pair of WLCs are connected to a dedicated services switch block (Catalyst chassis or resilient stack) that connects to the distribution layer. The services switch block can be dedicated to services or connect both the data center and services blocks. The switch block is connected to the distribution layer using layer 3 links implementing EIGRP or OSPF for route aggregation. The WLCs in this example are considered to be centralized.

The WLCs connect to the services switch block using static port-channels configured for 802.1Q VLAN tagging. The wireless management, data and voice VLANs are all 802.1Q tagged between the WLCs and the services switch block. The services switch block provides first-hop unicast and multicast routing for each of the wireless VLANs.

Figure 2-39 Small Campus / Wireless Services Block Detail



For a small campus deployment Cisco recommends a pair of Cisco 5508 or Cisco 5520 WLCs configured for HA-SSO. The WLC model you select will depend on the specific throughput that is required for the site. The redundancy ports for both WLCs are directly connected as both WLCs reside in the same physical data center. The APs are configured to use the HA-SSO pair as their primary WLC. All configuration is automatically synchronized between the active and standby-hot WLC.

Medium Campus

Figure 2-40 shows the recommended WLC placement for a CUWN deployment for a medium campus network implementing a dedicated distribution layer. The benefits for deploying a dedicated distribution layer for larger networks is well documented and understood. The WLCs in this architecture connect directly to the core layer by means of a dedicated switch block. The medium campus in this example is a single building with multiple floors each with multiple access layer switches.

Figure 2-40 Campus WLC Deployment Details

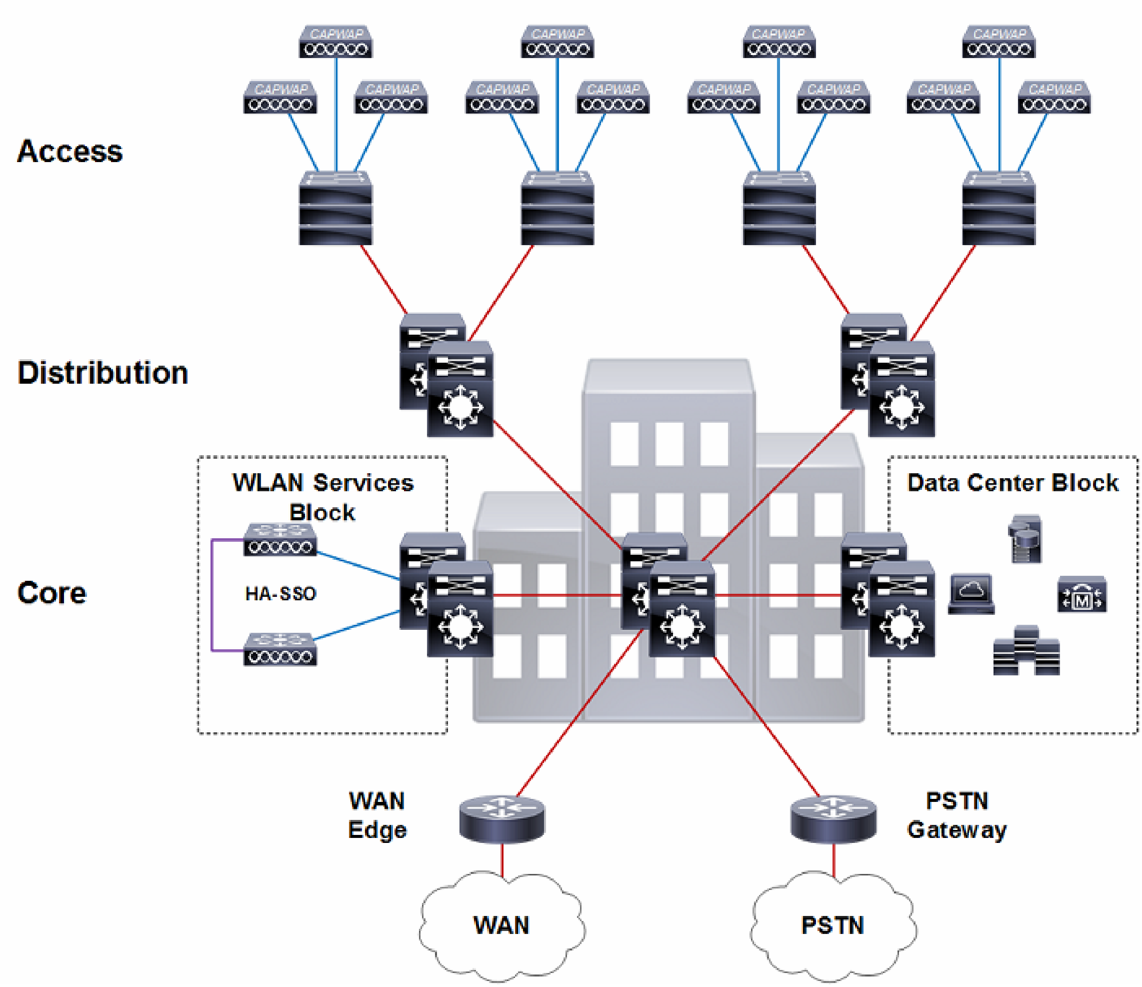
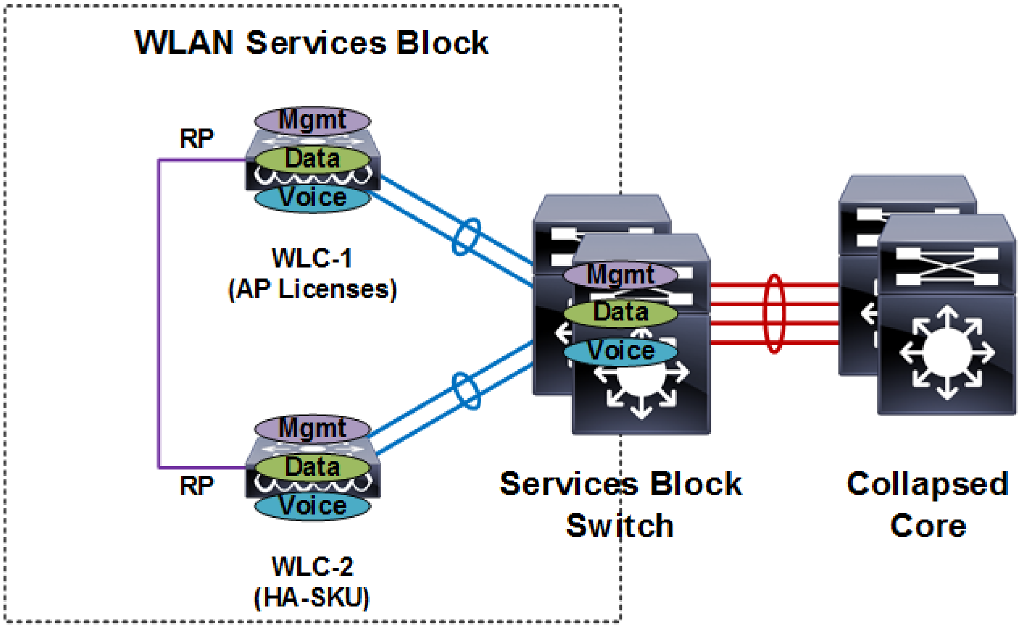


Figure 2-41 shows additional details for the wireless services block for a medium campus deployment. In this example a pair of WLCs are connected to a dedicated services switch block that connects to the core layer. The services switch block is a pair of Catalyst switches configured for multilayer or VSS. The services switch block is connected to the core layer using layer 3 links implementing EIGRP or OSPF for route aggregation. The WLCs in this example are considered to be centralized.

The WLCs connect to the services switch block using static port-channels configured for 802.1Q VLAN tagging. The wireless management, data and voice VLANs are all 802.1Q tagged between the WLCs and the services switch block. The services switch block provides first-hop unicast and multicast routing for each of the wireless VLANs.

Figure 2-41 Medium Campus / Wireless Services Block Detail



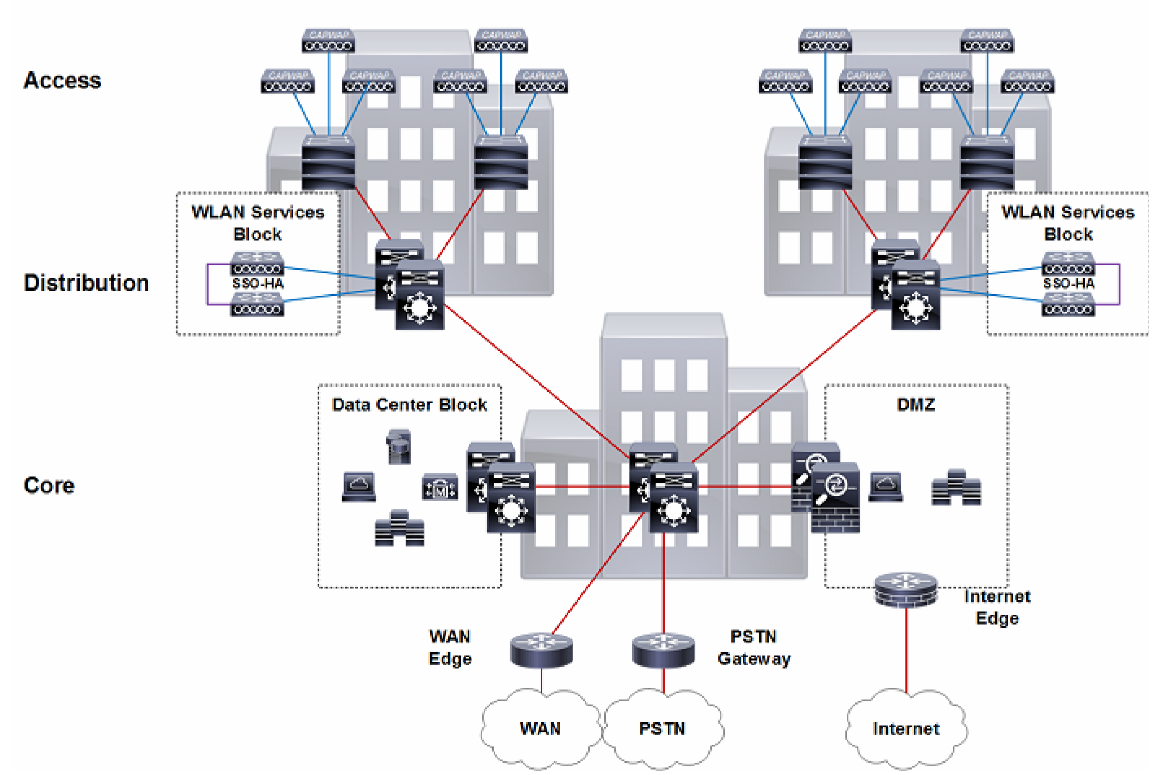
For a medium campus deployment Cisco recommends a pair of Cisco 5508 or Cisco 5520 WLCs configured for HA-SSO. The WLC model you select will depend on the specific throughput that is required for the site. The redundancy ports for both WLCs are directly connected as both WLCs reside in the same physical data center. The APs are configured to use the HA-SSO pair as their primary WLC. All configuration is automatically synchronized between the active and standby-hot WLC.

Large Campus

Figure 2-42 shows the recommended WLC placement for a CUWN deployment for a large campus network consisting of multiple buildings connected to a campus core. The WLCs in this architecture are distributed between the buildings where each pair of WLCs manages the APs within their given building. The WLCs in this architecture connect directly to the distribution layer within each building.

As multiple pairs of WLCs are distributed throughout the campus, each WLC is assigned as a member of the same Mobility group to provide seamless mobility to clients as they roam throughout the campus. The WLCs in each building are assigned different wireless management and user VLANs that terminate at the distribution layer within each given building. Mobility tunnels are used to forward roam user’s traffic between the foreign and anchor WLCs through the campus core.

Figure 2-42 Large Campus Reference Design



Distributing the WLCs between the buildings provides several scaling advantages as the number of wireless clients supported by a CUWN increases. As more devices are added to the wireless network, the number of layer 2 and layer 3 table entries that are processed and maintained by the service block switches increases exponentially. This results in a higher CPU load on the service block switches.

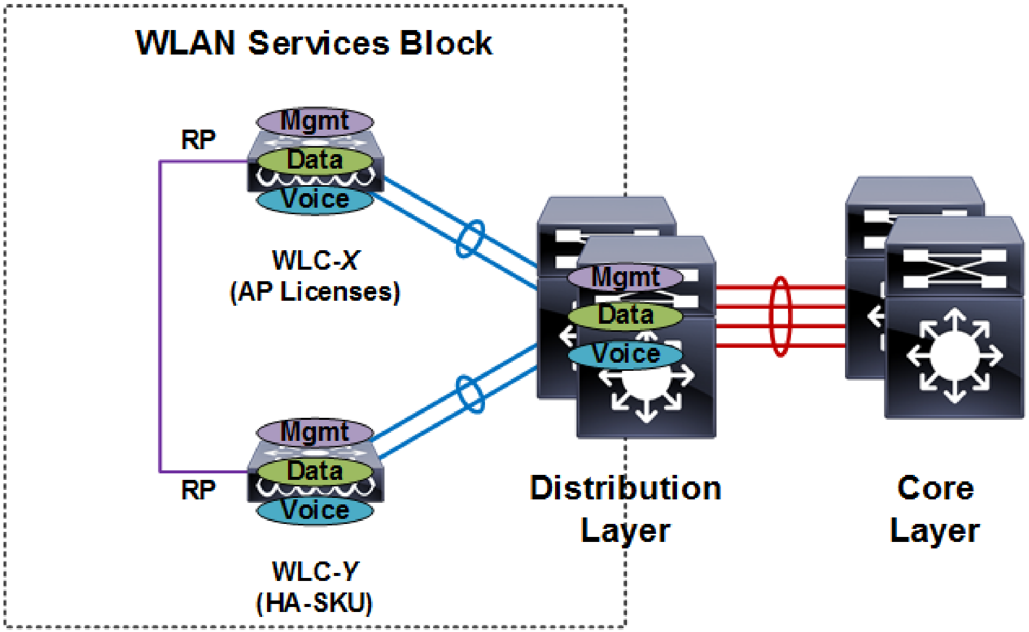
Why is this consideration important? The current generation of WLCs can scale to support up to 6,000 APs and 64,000 clients. In a pure IPv4 environment, this can result in a 128,000 entries being processed and maintained by the service block switches. As most wireless clients also support a dual-stack, the number of entries that are processed and maintained increase further.

As a best practice Cisco recommends distributing the WLCs for large campus deployments supporting 25,000 or more wireless clients. Distributing the WLCs spreads the MAC, ARP and ND processing and table maintenance between the distribution layer switches reducing CPU load. This architecture also allows for faster convergence during a distribution layer failure as only a subset of the entries need to be re-learned by the affected distribution layer. If the campus deployment supports fewer than 25,000 clients, a centralized WLC architecture can be employed where the WLCs are connected to the core by means of a dedicated switch block (see medium campus).

Figure 2-43 shows additional details for the wireless services block for a large campus deployment. In this example each pair of WLCs are connected to the distribution layer switches within each building. The distribution layer switches are Catalyst switches configured as multilayer or VSS that connect to the core layer using layer 3 links. EIGRP or OSPF is used for route aggregation.

The WLCs connect to the distribution switches using static port-channels configured for 802.1Q VLAN tagging. The wireless management, data and voice VLANs are all 802.1Q tagged between the WLCs and the distribution switches. The distribution switches provides first-hop unicast and multicast routing for each wireless VLAN.

Figure 2-43 Large Campus / Wireless Services Block Detail



For large campus deployments Cisco recommends a pair of Cisco 5520 or 8540 WLCs within each distribution layer configured for HA-SSO. The WLC model that you select for each building will depend on the number of APs and the throughput required for each building. The redundancy ports for both WLCs can be directly connected or extended over a dedicated layer 2 VLAN depending on the physical location of the distribution layer switches.

The APs within each building are configured to use their local HA-SSO pair as their primary WLC. Additional redundancy is provided using N+1 redundancy by configuring a different buildings HA-SSO pair as the secondary WLC. The necessary WLANs, AP groups and RF groups are defined on both the primary and secondary HA-SSO pairs.

Note The configuration requirements of the distribution layer switches different depending on if they are configured as multilayer or VSS. A detailed overview of the requirements for each implementation is provided in the High Availability, page 2-42 section of this chapter.

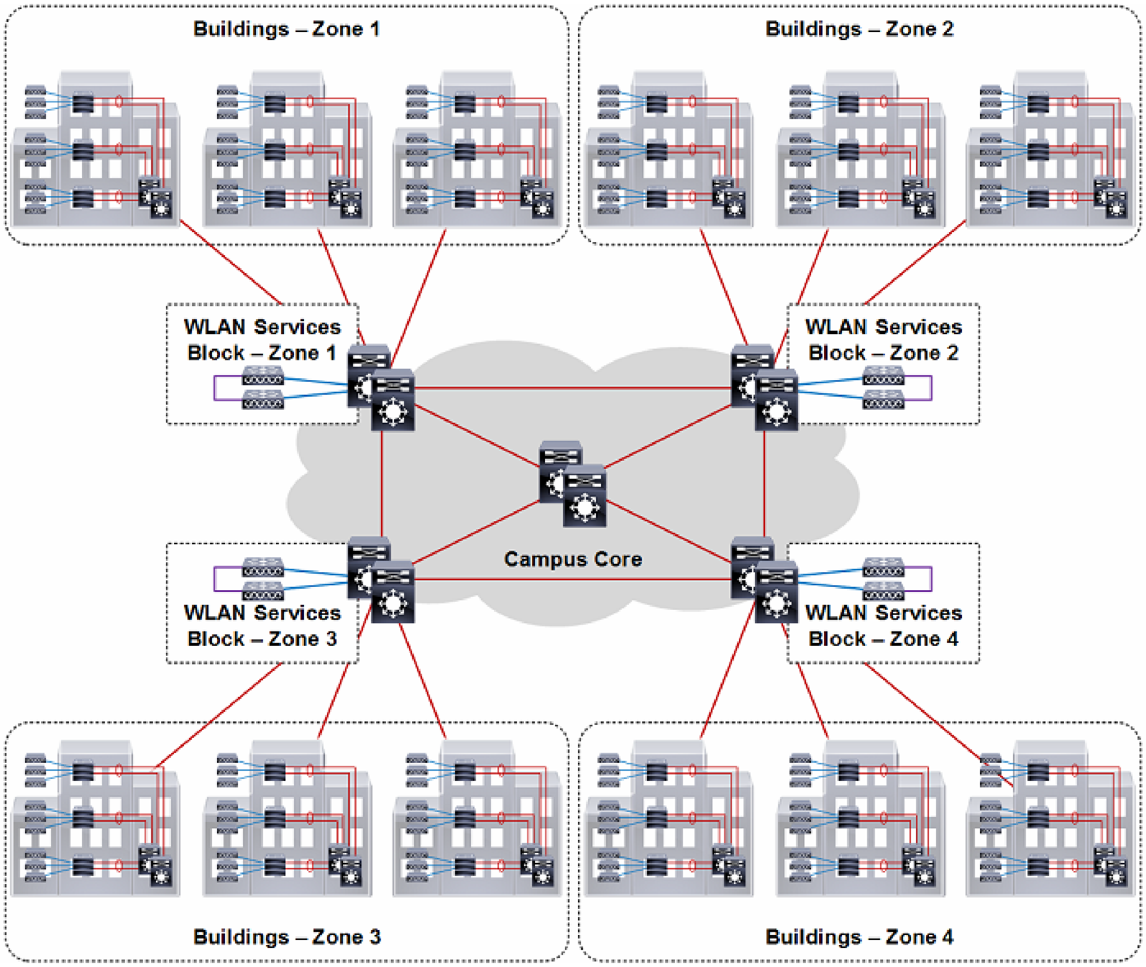
Very Large Campus

Figure 2-44shows the recommended WLC placement for a CUWN deployment for a very large campus network supporting hundreds of buildings that connect to a distributed core layer. Each distributed core switch acting as a distribution layer within the campus core. Large buildings in the campus implement their own distribution and access layers while smaller buildings implement only an access layer.

The WLCs in this architecture are distributed between the core layer switches where each pair of WLCs manages the APs for groups of buildings. Each wireless services block can support up to 6,000 APs, 25,000 and 40Gbps of throughput. The WLCs in each wireless services block are assigned different wireless management and user VLANs that terminate at the distributed / core layer servicing each group of buildings. The number of required wireless services blocks being determined by the number of wireless devices that need to be supported.

The example campus network shown in Figure 2-44 implements four separate wireless services blocks, each block supporting groups of buildings placed into a specific zone. This CUWN design comfortably scaling to support up to 24,000 APs and 100,000 clients.

Figure 2-44 Very Large Campus Reference Design


Buildings – Zone 1
Buildings – Zone 2
WLAN Services Block – Zone 1
WLAN Services Block – Zone 2
Campus Core
WLAN Services Block – Zone 3
WLAN Services Block – Zone 4
Buildings – Zone 3
Buildings – Zone 4

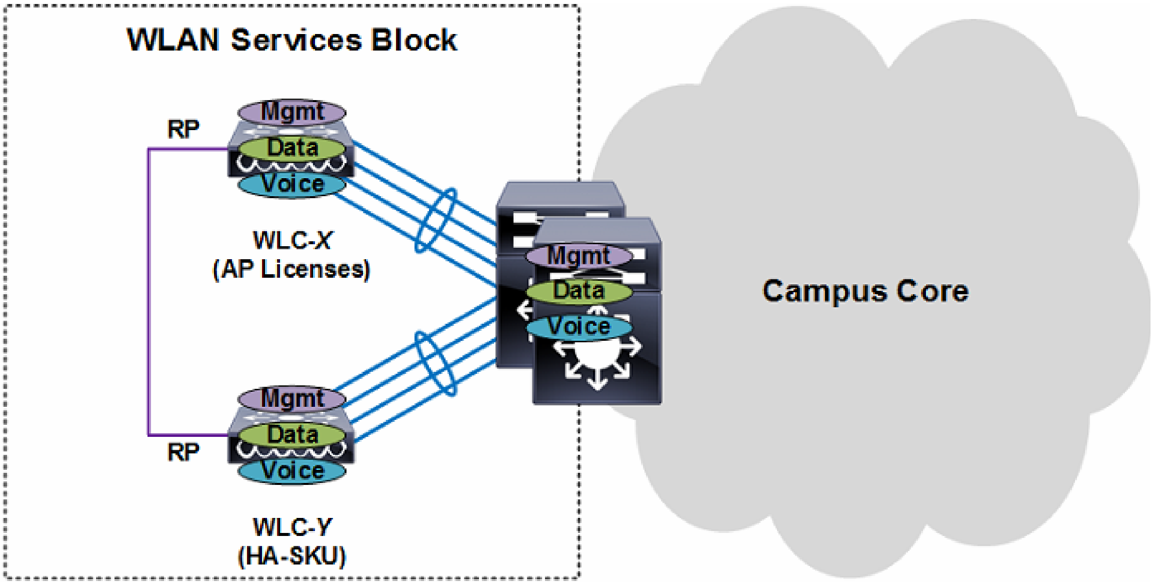
The Mobility group design for a very large campus is also an important consideration and is dependent on the wireless coverage provided between the buildings and zones. Ideally the buildings placed into each zone representing a wireless coverage area.

- If continuous wireless coverage is provided within each zone and between zones, a single Mobility group can be defined. Each pair of WLCs configured as members of the same Mobility group. Wireless clients will be able to seamlessly roam throughout the campus while maintaining their original network membership.
- If continuous wireless coverage is only provided within each zone, separate Mobility groups must be deployed. Each pair of WLCs configured with a separate Mobility group. Wireless clients will be able to maintain their network membership within the zone and be assigned to a new network when they connect to an AP in a separate zone.
- If continuous wireless coverage is provided between some of the zones, the WLCs servicing those zones maybe assigned to the same Mobility group. Wireless clients will be able to maintain their network membership within those zones and be assigned to a new network when they connect to an AP in a separate zone.

Figure 2-45 shows additional details for the wireless services block for a very large campus deployment. In this example each pair of WLCs are connected to the distribution / core layer switches servicing each group of buildings. The distribution / core layer switches are Catalyst switches configured as multilayer or VSS that are interconnected using layer 3 links. EIGRP, OSPF or BGP is used for route aggregation.

The WLCs connect to the distributed core switches using static port-channels configured for 802.1Q VLAN tagging. The wireless management, data and voice VLANs are all 802.1Q tagged between the WLCs and the distributed / core switches. The distribution / core switches provides first-hop unicast and multicast routing for each wireless VLAN.

Figure 2-45 Very Large Campus / Wireless Services Block Detail



For very large campus deployments Cisco recommends a pair of Cisco 8540 WLCs within each distribution layer configured for HA-SSO. The redundancy ports for both WLCs can be directly connected or extended over a dedicated layer 2 VLAN depending on the physical location of the distribution layer switches.

The APs within each zone are configured to use their designated HA-SSO pair as their primary WLC. Additional redundancy is provided using N+1 redundancy by configuring a different zones HA-SSO pair as the secondary WLC. The necessary WLANs, AP groups and RF groups are defined on both the primary and secondary HA-SSO pairs.

Note The configuration requirements of the distribution layer switches different depending on if they are configured as multilayer or VSS. A detailed overview of the requirements for each implementation is provided in the High Availability, page 2-42 section of this chapter.

Branch

A Cisco Unified Wireless Network provides two architectures to support remote branch offices connected over a wide area network (WAN). For branch sites network administrators can implement APs operating in local or FlexConnect modes. Both CUWN architectures operate differently and solve different business needs. This section provides details for local mode AP deployments only. Additional details and recommendations for FlexConnect AP deployments is discussed in Chapter 7, “FlexConnect”.

A branch site implementing local mode APs follows the small campus architecture where a WLC is placed directly within a branch. All CAPWAP tunnels stay within the branch. If multiple branch sites with local mode APs are deployed, it is considered a distributed architecture as WLCs are deployed in one or more branches connected by means of a WAN.

Figure 2-46 shows the recommended WLC placement for a CUWN deployment for a small branch network implementing a distribution layer operating as a collapsed core. The distribution layer provides connectivity to the WLCs, WAN and Internet edge. Depending on the size of the branch, the WLCs may connect directly to distribution layer (as shown) or be connected by means of a dedicated switch block. The branch network in this example is a single building with one distribution layer two access layer switches.

Figure 2-46 Small Branch Reference Design

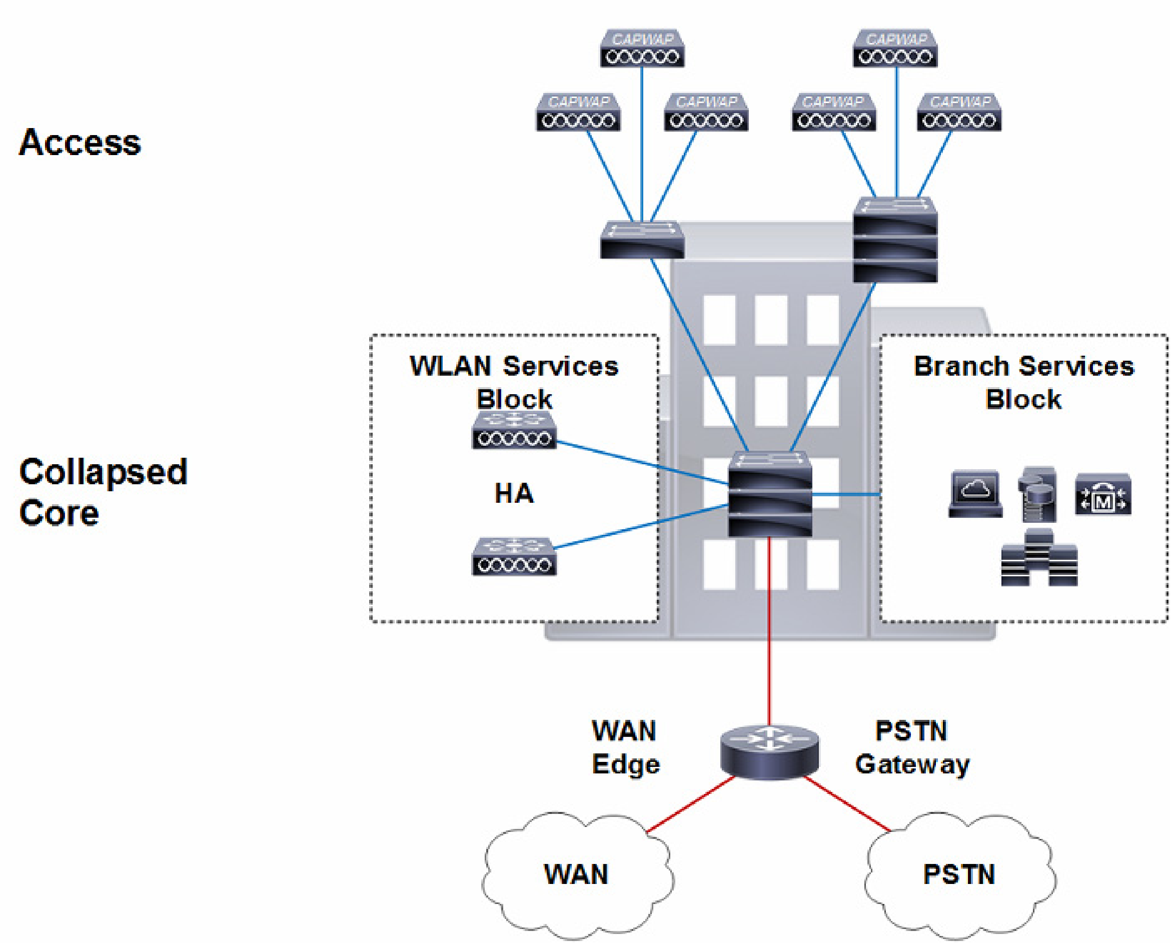
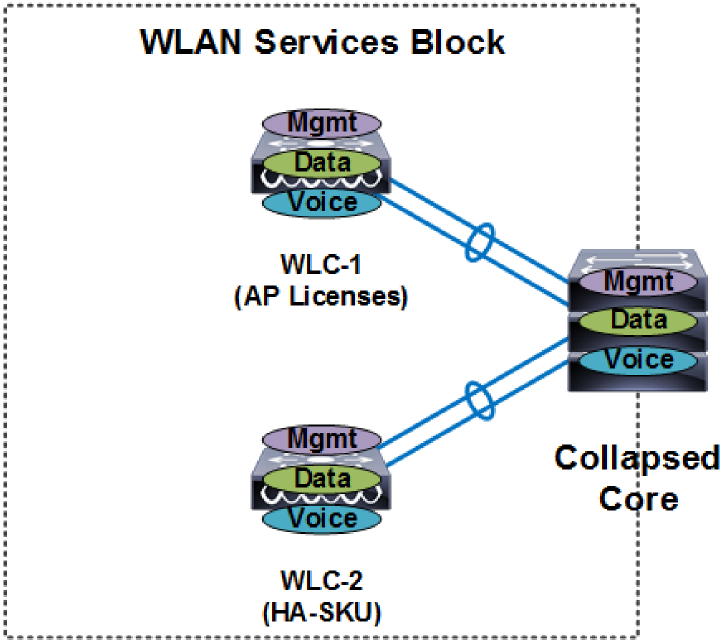


Figure 2-47 shows additional details for the wireless services block for a branch network deployment. In this example a pair of WLCs are connected directly to the distribution layer using static port-channels configured for 802.1Q VLAN tagging. The wireless management, data and voice VLANs are all 802.1Q tagged between the WLCs and the distribution layer. The distribution layer provides first-hop unicast and multicast routing for each of the wireless VLANs.

Figure 2-47 Small Branch / Wireless Services Block Detail



For a branch office deployment Cisco recommends a pair of Cisco 2504 WLCs configured for N+1 HA. The Cisco 2504 WLC is designed specifically for branch office deployments and can scale to support up to 75 APs. Both WLCs are configured are assigned to the same Mobility group and are configured to support the same interfaces / interface groups, WLANs, AP groups and RF groups. The APs are configured to use the permanently licensed WLC as their primary WLC and the HA-SKU WLC as their secondary WLC.

Note Cisco does not support deploying local mode APs using a centralized WLC over a wide area network. If remote APs need to be supported over a WAN, Cisco recommends implementing the FlexConnect architecture.

Traffic Load and Wired Network Performance

When deploying a Cisco Unified Wireless Network solution, topics of discussion often include:

- CAPWAP traffic impact/load across the wired backbone.
- Minimum performance requirements to support a unified wireless deployment.
- Relative benefits of a distributed versus centralized WLC deployment in the context of traffic load on the network.

In examining the impact of the CAPWAP traffic in relation to overall network traffic volume, there are three main points to consider:

- Volume of CAPWAP control traffic
- Overhead introduced by tunneling
- Traffic engineering

Volume of CAPWAP Control Traffic

The volume of traffic associated with CAPWAP control can vary depending on the actual state of the network. For example, traffic volume is usually higher during a software upgrade or WLC reboot situations. Traffic studies have found that the average load CAPWAP control traffic places on the network is approximately 0.35 Kbps. In most campuses, this would be considered negligible and would be of no consequence when considering a centralized deployment model over a distributed one.

Overhead Introduced by Tunneling

A CAPWAP tunnel adds 44 bytes to a typical IP packet to and from a WLAN client. Given that average packets sizes found on typical enterprises are approximately 300 bytes, this represents an overhead of approximately 15 percent. In most campuses, this overhead would be considered negligible and again would be of no consequence when considering a centralized deployment model over a distributed one.

Traffic Engineering

Any WLAN traffic that is tunneled to a centralized WLC is then routed from the location of the WLC to its end destination in the network. Depending on the distance of the tunnel and location of the WLC, WLAN client traffic might not otherwise follow an optimal path to a given destination. In the case of a traditional access topology or distributed WLC deployment, client traffic enters the network at the edge and is optimally routed from that point based on destination address.

The longer tunnels and potentially inefficient traffic flows associated with a centralized deployment model can be partially mitigated by positioning the WLCs in that part of the network where most of the client traffic is destined (for example, a data center). Given the fact that most enterprise client traffic goes to servers in the data center and the enterprise backbone network is of low latency, any overhead associated with inefficient traffic flow would be negligible and would be of no consequence when considering a centralized deployment model over a distributed one.

For most enterprises, the introduction of a WLAN does not result in the introduction of new applications, at least not immediately. Therefore, the addition of a Cisco Unified Wireless Network alone is not likely to have a significant impact on the volume of campus backbone traffic.

AP Connectivity

APs should be on different subnets from the end users (802.11 clients). This is consistent with general best-practice guidelines that specify that infrastructure management interfaces should be on a separate subnet from end users. Additionally, Cisco recommends that Catalyst Integrated Security Features (CISF) be enabled on the CAPWAP AP switch ports to provide additional protection to the WLAN infrastructure. (FlexConnect AP connectivity is discussed in **Chapter 7, “FlexConnect”**).

DHCP is generally the recommended method for AP address assignment, because it provides a simple mechanism for providing current WLC address information for ease of deployment. A static IP address can be assigned to APs, but requires more planning and individual configuration. Only APs with console ports permit static IP address configuration.

In order to effectively offer WLAN QoS within the Cisco Unified Wireless Network, QoS should also be enabled throughout the wired network that provides connectivity between CAPWAP APs and the WLCs.

Operation and Maintenance

This section focuses on general deployment considerations and recommendations for easy operation and maintenance of a Cisco Unified Wireless Network deployment.

WLC Discovery

The different WLC discovery mechanisms for APs (discussed earlier) make initial deployment of CAPWAP APs very simple. Options include:

- Staging (priming) CAPWAP APs in advance using a WLC in a controlled environment
- Deploying them right out of the box by using one of the auto discovery mechanisms (DHCP or DNS)

Although auto discovery is highly useful, a network administrator will generally want to be able to control which WLC an AP will join once it is connected to the network for the first time. Subsequently, an administrator will want to define which WLC will be the primary for a given AP during normal operation in addition to configuring secondary and tertiary WLCs for backup purposes.

AP Distribution

In a typical initial WLAN deployment, the APs automatically distribute themselves across the available WLCs based on the load of each WLC. Although this process makes for an easy deployment, there are a number of operational reasons not to use the auto distribution method.

APs in the same physical location should be joined to the same WLC. This makes it easier for general management, operations and maintenance, allowing staff to control the impact that various operational tasks will have on a given location, and to be able to quickly associate WLAN issues with specific WLCs, whether it be roaming within a WLC, or roaming between WLCs.

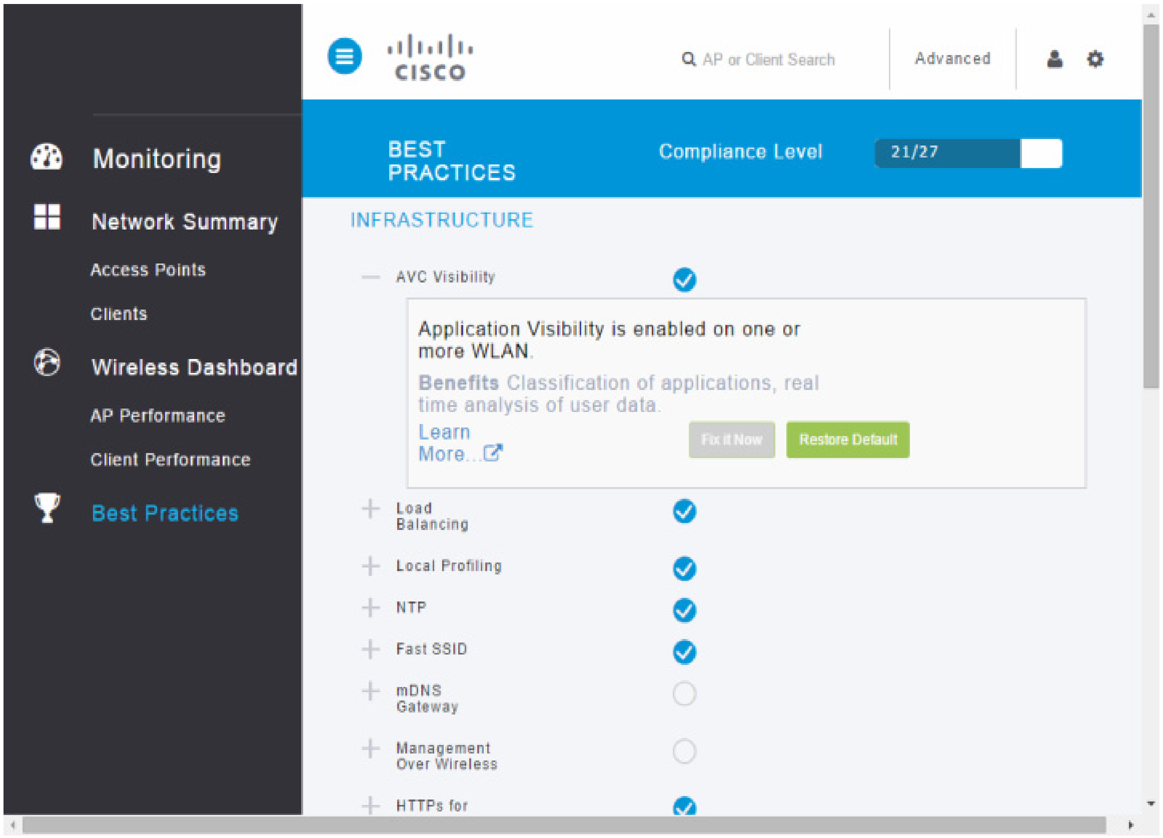
The elements used to control AP distribution across multiple WLCs are:

- Primary, secondary, and tertiary WLC names – Each AP can be configured with a primary, secondary, and tertiary WLC name, which in turn determines the first three WLCs in the mobility group that the AP will prefer to join regardless of the load variations across WLCs in the mobility group.
- Master WLC – When an AP joins a WLC for the first time in a mobility group, it is not yet configured with a preferred primary, secondary, and tertiary WLC; therefore, it will be eligible to partner with any WLC (within the mobility group) depending upon the perceived WLC load. If a WLC is configured as a master WLC, all APs without primary, secondary, and tertiary WLC definitions will join with the master WLC. This allows operations staff to easily find newly joined APs and control when they go into production by defining the primary, secondary, and tertiary WLCs name parameters.

Best Practices

For convenience of network deployment engineers, starting with CUWN software release 8.1, a best practices checklist is available within the dashboard for WLAN controllers (Figure 2-48). The checklist is used to fine tune WLC configuration to match the best practices as suggested by Cisco. The checklist compares the local configuration on the WLC with recommended best practices and highlights all of the features that differ. The check also provides a simple configuration panel to turn on the best practices. Use of best practices is highly recommended for all CUWN deployments.

Figure 2-48 Best Practices Dashboard



Compliance Level 21/27

Application Visibility is enabled on one or more WLAN.

Benefits Classification of applications, real time analysis of user data.

Learn More...

The dashboard checks the adherence for each recommended feature and provides feedback about the compliance of each one. A best practice score is displayed based on the number of recommended features that are enabled. Each recommended features is categorized as either Infrastructure, Security or RF Management and the majority can be enabled directly within the dashboard using a single mouse click. Additional information about a specific feature as well as the benefits are also provided in the dashboard.

The dashboard checks the adherence for each recommended feature and provides feedback about the compliance of each one. A best practice score is displayed based on the number of recommended features that are enabled. Each recommended features is categorized as either Infrastructure, Security or RF Management and the majority can be enabled directly within the dashboard using a single mouse click. Additional information about a specific feature as well as the benefits are also provided in the dashboard.

Table 2-7 Release 8.1 Best Practices

Infrastructure	Security	RF Management
• Application Visibility and Control • Load Balancing • Local Profiling • NTP • Fast SSID • mDNS Snooping • Management over Wireless • Secure Web Access • Aironet IE • Multicast Forwarding • Controller High Availability	• 802.1X on WLAN • Rogue Policies • Rogue Threshold • SSH / Telnet Access • Client Exclusion • Legacy IDS • Local Management Password Policies • CPU ACLs	• SSID Limit • Client Bandselect • 40MHz Channel Width • Auto Dynamic Channel Assignment • Automatic Transmit Power Control • Automatic Coverage Hole Detection • CleanAir • Event Driven Radio Resource Management

Note A full list of each of the current best practices provided in the dashboard is available at: http://www.cisco.com/c/en/us/td/docs/wireless/controller/best-practices/base/b_bp_wlc.html

CHAPTER 3

WLAN RF Design Considerations

This chapter describes the basic information necessary to understand radio frequency (RF) considerations in planning for various wireless local area network (WLAN) environments. The topics of this chapter includes:

- Regulatory domains and RF considerations
- IEEE 802.11 standards
- RF spectrum implementations of 802.11b/g/n (2.4-GHz) and 802.11a/n/ac (5-GHz)
- Planning for RF deployment
- Radio resource management (RRM) algorithms and configuration
- RF Profiles and fine tuning

RF Basics

In the United States there are three main bands (frequency ranges) allocated for unlicensed industrial, scientific, and medical (ISM) usage.

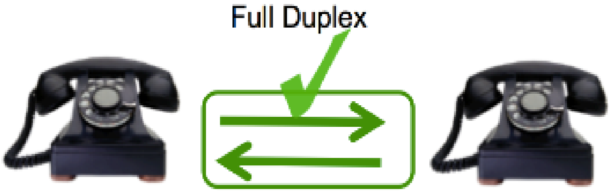
The ISM bands are designated as the:

- 900 MHz band: 902 to 928 MHz
- 2.4 GHz band (IEEE 802.11b/g/n): 2.4 to 2.4835 GHz
- 5 GHz band (IEEE 802.11a/n/ac):
- 5.150 to 5.250 GHz (UNII-1)
  - 5.250 to 5.350 GHz (UNII-2)
  - 5.450 to 5.710 GHz (UNII-2e)
  - 5.725 to 5.875 GHz (UNII-3)

The 900 MHz band is not used for Wi-Fi. Each of the remaining bands has different characteristics and for Wi-Fi the pro's and con's depend on what your coverage and capacity goals are, and what is already occupying the spectrum in your location. See deployment considerations later in this chapter for more detail.

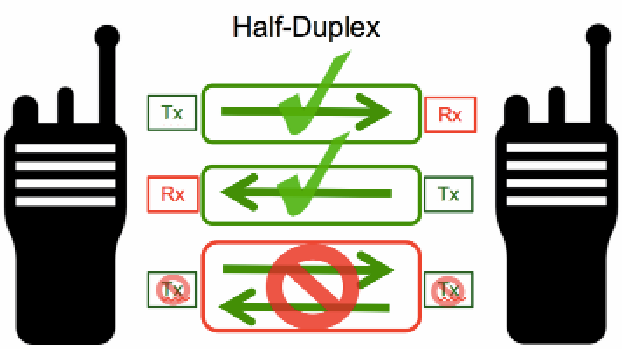
It is important to understand how Wi-Fi differs from modern day LAN implementations. A modern day wired LAN is most often a full duplex, switched infrastructure. This means that traffic is sent and received simultaneously and switched between active ports, so a client can both transmit and receive concurrently. A telephone conversation is full duplex – see Figure 3-1.

Figure 3-1 Example of Full Duplex Conversation



Wi-Fi on the other hand is half duplex (Fig. 2), meaning we can either Transmit (Tx) to or Receive (Rx) from a client/AP on the medium, the clients and the network take turns accessing the medium – it is a shared broadcast and collision domain. Wi-Fi is contention based – meaning there are rules for stations trying to access the medium and collisions (due to two or more stations simultaneously accessing the medium) are worked out fairly so everyone gets a chance.

Figure 3-2 Example of a Half-Duplex Conversation



Separation of physical groups of clients is performed using different frequency assignments – or channels. For an access point operating on a given channel, there is a finite amount of airtime available and every client connecting to an access point shares the airtime that the AP's channel has to offer. The more clients that are actively using an AP, the less airtime each client will get individually. Supporting a higher data rate for one or more clients (more efficient use of airtime) will increase available airtime for all clients, and result in higher potential bandwidth to the individual user.

All clients on a given channel share a common collision domain that extends to other AP's operating on the same channel regardless of whose network they ultimately belong to. This means that other clients and access points using the same channel and can hear one another, share the available airtime. Each additional AP added to a channel brings with it management overhead on the air. The effect of this additional management traffic further reduces the total amount of airtime available for each user and constrains performance.

Bandwidth = Airtime x Data Rate.

If you require more bandwidth than can be served from a single access point (i.e. you have many users in a small area) then multiple AP's will be required. When implemented on non overlapping channels, each AP provides an isolated chunk of airtime over its coverage area. AP's that are on the same channel must be kept out of range of one another. This is what Cisco's RRM manages for you –the power and the channel selection to coordinate multiple AP's and neighbors for optimal performance. (*See* Radio Resource Management - RRM below in this document.)

Channel assignment and reuse for the network is a big factor in determining the airtime efficiency and ultimately the bandwidth that can be delivered to the clients. When two AP's can hear one another on the same channel the result can be co-channel interference unless the overlapping BSS is managed carefully. Whether co-channel interference is the result of your own AP's, or your AP and a neighbor doesn't matter– either way the AP's must share the channel. In order to produce a good physical design, four things must be considered:

- AP placement
- AP operating band (2.4 GHz or 5 GHz)
- AP channels selected
- AP power levels assigned

The goal in a good design is to produce even wireless coverage (similar conditions end to end) with minimal co-channel interference maximizing the available potential bandwidth for the client devices.

Cisco's RRM, Radio Resource Management, calculates and assigns the best channels and power combinations using measured, over the air metrics. Over The Air observations include Wi-Fi networks operating within the infrastructure as well as existing external users Wi-Fi and non-Wi-Fi of the spectrum. RRM will mitigate co-channel assignments and balance power, but if there are no open channels available, or the AP's are simply too close together the only choice remaining is sharing the channel with an existing user. This happens in congested environments and two different networks may have to share the same bandwidth. If one or the other is not busy – the other may use all of the bandwidth. If both become busy, they will share the bandwidth 50/50 due to 802.11's contention mechanisms ("listen before talk") that are designed to ensure fair access.

Regulatory Domains

Devices that operate in unlicensed bands do not require a formal licensing process by the end user. However equipment designed and built for operating 802.11 in the ISM bands is obligated to follow the government regulations for the region it is to be used in. "Unlicensed, does not mean "without rules". Cisco Wireless equipment is designed and certified to operate and meet the regulatory requirements for specific regions. Regulatory designations are either included in the part numbers for pre provisioned AP's built for a specific region or more recently a Universal AP (UAP) which is provisioned on site (*See* Universal AP Regulatory Domain Deployment Guide).

The end user bears responsibility for correct implementation and ensuring that the correct equipment is used for the specified region. Your Cisco sales team can guide you in selection. For provisioning a universal AP – at least one AP must be provisioned using the smart-phone application to ensure the GPS location of the AP. This ensures that the AP is physically located in the region being activated for. Once provisioning of the first UAP is completed, other UAP's may be provisioned off the initial UAP with enable radio interfaces.

The regulatory agencies in different regions of the world monitor the unlicensed bands according to their individual criteria. WLAN devices must comply with the specifications of the relevant governing regulatory body. Although the regulatory requirements do not affect the interoperability of IEEE 802.11b/g/n- and 802.11a/n/ac-compliant products, the regulatory agencies do set certain criteria in the product implementation. For example, the RF emission requirements for WLAN are designed to minimize the amount of interference any radio (not just Wi-Fi) can generate or receive from any other radio in the same proximity. It is the responsibility of the WLAN vendor to obtain product certification from the relevant regulatory body. And it is the responsibility of the installer to ensure that the resulting installation does not exceed those requirements. We recommend and certify the use of antenna's and radio combinations that meet regulatory requirements.

Besides following the requirements of the regulatory agencies, Cisco ensures interoperability with other vendors through various Wi-Fi Alliance (WFA) certification programs (www.wi-fi.org).

Operating Frequencies

The 2.4-GHz band regulations of 802.11b/g/n have been relatively constant, given the length of time they have been in operation. The FCC (U.S) allows for 11 channels, ETSI (and most other parts of the world) allow for up to 13 channels, and Japan allows up to 14 channels but requires a special license and operating modes to operate in channel 14.

Countries that adhere to the 5.0-GHz band regulations of 802.11a/n/ac are more diverse in the channels they allow and their rules for operation. In general, with the advancement of 802.11ac most are now considering opening more spectrum for 5 GHz Wi-Fi – and all have more non overlapping channels in 5 GHz than is available anywhere in 2.4 GHz.

These frequency bands and their associated protocols can and do change as the technology evolves and regulatory rules change. All Cisco AP’s regulatory certifications and allowed frequencies and channels are documented in their individual data. These documents are located under Access Points in Cisco Reference Guides.

2.4 GHz - 802.11b/g/n

The 2.4 GHz band as it is commonly referred to consists of frequencies between 2400 MHz and 2483 MHz for a total of 83 MHz of usable spectrum in most of the world.

There are currently 3 protocol specifications permitted for 802.11 Wi-Fi operations in the 2.4 GHz band. 802.11b, 802.11g and 802.11n are standards created by the IEEE and agreed to by individual regulatory authorities around the world. Many other non Wi-Fi technologies also use the 2.4 GHz band for operation; Microwave Ovens, Baby Monitors, Gaming consoles, Bluetooth devices and cordless phones to name just a few. These other non Wi-Fi devices represent interference to Wi-Fi signals as they can and do interfere with Wi-Fi operations in the 2.4 GHz band. Consumer Wi-Fi devices also heavily use the 2.4 GHz band. Many older (but still in widespread use) consumer access points (or wireless routers as they are sometimes called) are single band devices that only operate with a 2.4 GHz radio. The aggregate of all the various users accessing the 2.4 GHz band combined with a limited amount of spectrum leads to this bands growing reputation for congestion.

Does this mean that you wont be able to successfully deploy Wi-Fi in 2.4 GHz? No. It simply means that the 2.4 GHz band will fill up faster and support less users than the 5 GHz band will. Congestion in the band is a local phenomenon and your location may be fine. A site survey will show you what you have to work with in your application.

802.11b

The 802.11b protocol was ratified as an amendment to the 802.11 standards in 1999. It added support for data rates of 5.5 and 11 Mbps and enjoys broad user acceptance and vendor support. 802.11b has been deployed by thousands of organizations, as it was the first standardized specification for modern Wi-Fi communications. It is the least efficient of all the protocols available today, which means that you will exhaust available airtime quite rapidly using this protocol and with less airtime; you can support less users. 802.11b is based on a single transmitter/receiver design and suffers from multipath frequency phenomena that affects reliability and makes design more difficult. What remains of true 802.11b clients can generally be found in application specific appliances such as bar code scanners or printers generally in Logistics, Retail or Health Care verticals. Modern day radios that are able to support 802.11b are generally all implemented on radios designed for 802.11n and improve the reliability (MRC Receivers), but not the efficiency of the 802.11b standard.

802.11g

The 802.11g protocol, which was ratified as an amendment to the 802.11 IEEE standards in 2003, operates in the same spectrum as and is backwardly compatible with the 802.11b specification. The 802.11g standard uses a completely different modulation technique (OFDM) and supports data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. While backwardly compatible, this compatibility comes at a cost to airtime and additional management overhead required for 802.11b which reduces the overall gains that could be realized with 802.11g when operating in an 11g only client environment. Performance in a mixed 802.11b 802.11g environment will cost as much as 50% of a cells potential capacity. Initial 802.11g radios like 802.11b designs also had a single receiver and transmitter and where subject to a lot of the same reliability issues in implementation.

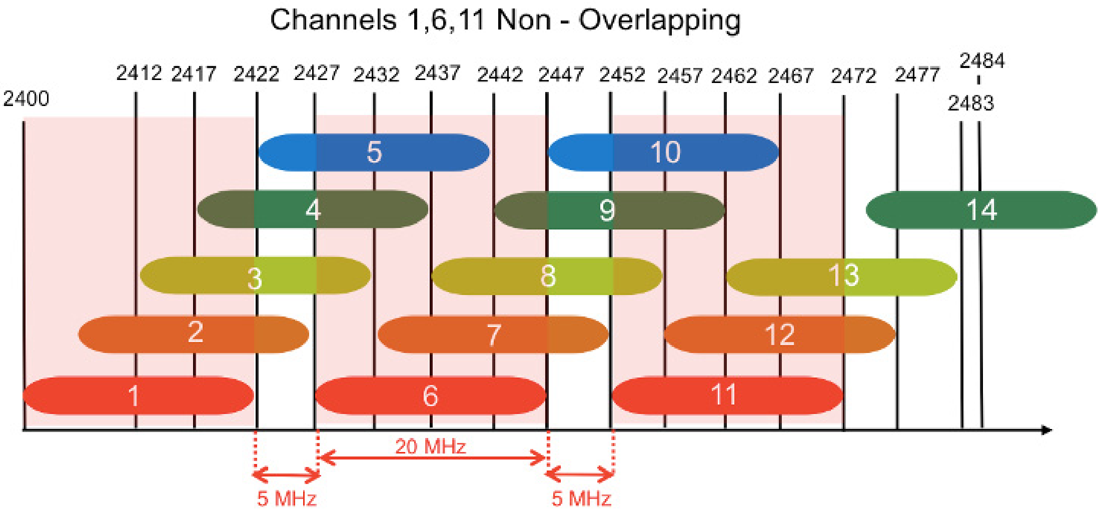
802.11n

The 802.11n protocol, which was ratified as an amendment to the 802.11 standards in 2009 allows for usage in either 2.4 or 5 GHz bands and introduces MIMO (multiple input, multiple output) using multiple radios allows for encoding multiple Spatial Stream's simultaneously (i.e) up to 4 times the data in the same amount of airtime theoretically, 3 spatial Streams is the practical limit. The 2.4 GHz band supports data rates up to 216 Mbps (assuming 20 MHz channel and 3 spatial stream transmitter). 802.11n also specifies a wider channel operation at 40 MHz commonly referred to as a bonded channel as it requires two 20 MHz channels to make a single 40 MHz channel. We do not support bonding of channels in 2.4 GHz because of interference issues associated with only having 3 non-overlapping channels available (Figure 3-3). The number of devices, which support 3 spatial streams, is limited to higher end laptops and tablets as well as access points. Two spatial stream devices are more plentiful but still limited to Laptops and tablets, with only a few of the newest smartphones now support multiple spatial streams. In all cases, 802.11n products introduced a technology for receivers called MRC (Maximal Ratio Combining) a technique which relied on multiple receivers/antenna's to mitigate the reliability issues associated with early 802.11b and 802.11g/a receivers and improved the overall reliability and performance of Wi-Fi. Therefore, modern 802.11n based radios improve on reliability when operating under the 802.11g standard.

2.4 GHz Wi-Fi Channel Planning

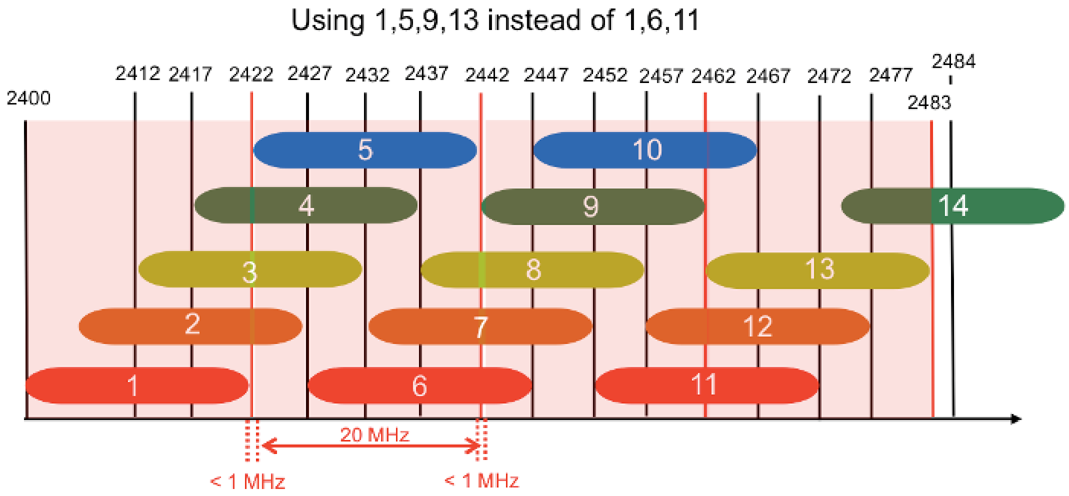
Channel plans for the 2.4 GHz band identify 14 Overlapping channels, but only 3 of these are Channels 1,6,11 are highlighted below, note that all other channels overlap or share boundaries and in the US only 1,6,11 are available for non-interfering channel operation.

Figure 3-3 2.4 GHz Channels, Showing 1,6,11 Selected



Note In some regulatory domains, it has been suggested that a 4 channel plan will work. This continues to come up time and again however without going into a lot of detail about what happens outside of the channel boundaries – there is simply not enough space between channels left for this to work practically in anything but the least dense environments. Also consider that the majority of the world agrees on 1,6,11 and most radios will default to this channel plan – in such a case if you have selected 1,5,9,13 any radio using the standard channels will interfere with at least one – in most cases 2 of your channels – We do not recommend it for these reasons.

Figure 3-4 2.4 GHz Channels Showing 1/5/9/13 Selected



Valid strategies for reducing the congestion in 2.4 GHz include reduction in self interference by:

1. Disabling the 802.11b data rates – this will reduce the area of coverage/interference and eliminate the least efficient protocols from the air
2. Choosing a relatively high minimum mandatory data rates – this also reduces effective coverage/interference and data rates of 12-18 Mbps are used in high density deployments

3. No more than 3-4 SSID's (WLAN's) on any one AP, as each AP must broadcast each configured WLAN – this can dramatically reduce the management overhead associated with the physical channel
4. Eliminate known non Wi-Fi interference sources, CleanAir can help you identify, evaluate and locate these.

For interference coming from neighboring Wi-Fi networks that are not part of your solutions. All involve additional hardware and complexity in design. If you have a valid need for critical operations in 2.4 GHz it is recommended that you employ someone who has experience with this level of design.

5 GHz - 802.11a/n/ac

Operating in the unlicensed portion of the 5 GHz radio band, 802.11a/n/ac radios are immune to interference from ALL devices that operate in the 2.4 GHz band, including non Wi-Fi interference from consumer devices. The 5 GHz band available for Wi-Fi use can differ significantly around the world from 100 to 300 MHz, but in all cases there is more bandwidth available than in 2.4 GHz spectrums.

Because the 802.11a/n/ac standards operate in a different frequency range, 2.4 and 5 GHz band devices can operate in the same physical environment without interfering with each other. Most Cisco AP's support both 2.4 and 5 GHz dual band operation. There are three protocol specifications ratified for use in 5 GHz Wi-Fi, 802.11a, 802.11n and 802.11ac. The range of frequencies/channels is broken into different frequency segments in 5 GHz – and the range of frequencies has increased over time. In the United States we have:

- 5.150 to 5.250 GHz (UNII-1 - 4 Channels 36-48)
- 5.250 to 5.350 GHz (UNII-2 - 4 Channels 52-64)
- 5.450 to 5.710 GHz (UNII-2e - 12 Channels 100-144)
- 5.725 to 5.875 GHz (UNII-3 - 5 Channels 140-165)

All three protocols are backwardly compatible using identical mechanisms and work quite well together with no noticeable penalties for mixed operation apparent due to a common encoding technology. The primary differences are airtime efficiency.

Channel assignments in 5 GHz bands are much more straightforward in that all assignments are NON Overlapping channels with a minimum of 5 MHz separation maintained between channels.

802.11a

802.11a protocol, which was ratified as an amendment to the 802.11 standards in 1999 and is identical in most respects to the 802.11g standard except the band in which it operates and no need for backward compatibility for 802.11b. 802.11a supports speeds of 6, 9, 18, 24, 36, 48 and 54 Mbps. This is largely considered a legacy protocol in 2015 and you likely will not find many native 802.11a devices left in the wild. You may still see the 802.11a protocol in the air – but it is much more likely that this protocol is being used on a device that is natively at least an 802.11n device.

802.11n

802.11n protocol, which was ratified as an amendment to the 802.11 standards in 2009 allowed for operation in 2.4 GHz as well as 5 GHz. It also included several enhancements that allowed for wider channel operation (up to 40 MHz up from 20 MHz) with two times the channel width, one can expect twice the capacity or speed. This protocol introduced a new concept in radio design – MIMO – or Multiple Input, Multiple Output. Using multiple spatial streams allows simultaneous encoding of separate streams of data within the same signal and increased the density of data that could be sent at one time providing an order of magnitude increase in capacity and speed. The data rates for 802.11n needed to accommodate a varying number of spatial streams (dictated by individual radio design) as well as the encoding method used. The new data rate structure adopted MCS (Modulation and Coding Scheme) as a substitute for the then standard Data Rate.

Table 3-1 802.11n MCS 1-23 Data Rates

MCS Index	Spatial Streams	Modulation Type	Coding rate	Data Rate (Mbit/s)			
				20 MHz Channel		40 MHz Channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.5	7.2	13.5	15
1	1	QPSK	1/2	13	14.4	27	30
2	1	QPSK	3/4	19.5	21.7	40.5	45
3	1	16-QAM	1/2	26	28.9	54	60
4	1	16-QAM	3/4	39	43.3	81	90
5	1	64-QAM	2/3	52	57.8	108	120
6	1	64-QAM	3/4	58.5	65	121.5	135
7	1	64-QAM	5/6	65	72.2	135	150
8	2	BPSK	1/2	13	14.4	27	30
9	2	QPSK	1/2	26	28.9	54	60
10	2	QPSK	3/4	39	43.3	81	90
11	2	16-QAM	1/2	52	57.8	108	120
12	2	16-QAM	3/4	78	86.7	162	180
13	2	64-QAM	2/3	104	115.6	216	240
14	2	64-QAM	3/4	117	130	243	270
15	2	64-QAM	5/6	130	144.4	270	300
16	3	BPSK	1/2	19.5	21.7	40.5	45
17	3	QPSK	1/2	39	43.3	81	90
18	3	QPSK	3/4	58.5	65	121.5	135
19	3	16-QAM	1/2	78	86.7	162	180
20	3	16-QAM	3/4	117	130	243	270
21	3	64-QAM	2/3	156	173.3	324	360
22	3	64-QAM	3/4	175.5	195	364.5	405
23	3	64-QAM	5/6	195	216.7	405	450

MIMO or the use of Multiple Spatial Streams requires separate transmitters and receivers in order to operate – 1 for each Spatial Stream being coded. More radios require more power and antennas, for this reason the exact number of spatial streams that a given radio supports is often a design decision related to available power and real estate on a given device. In practical terms the more power and space a device has, the more spatial streams it can support. Hence AP's with wired power sources mostly support multiple spatial streams, as do many laptops and tablets. Smartphones with limited battery and space generally support a single spatial stream (there are exceptions, but not many). You will also find a range of capabilities related to cost and performance. The transmitter is the real power drain –SISO or Single input – Single Output) do support multiple receivers improving (and MRC – a dramatically improved receiver technology) even if they do not support multiple transmitters (and the ability to do multiple spatial streams). Notation for 802.11n radios is typically seen as 3x3:2 or 2x3:2 or 1x2:1 where as (#TX)x(#RX) and :# spatial streams supported.

802.11ac

802.11ac protocol which was ratified as an amendment to the 802.11 standards in 2013

Note There is only one 802.11ac standard, but there are two different timeliness for bringing 11ac to market commonly referred to by the market as Wave 1 and Wave 2.

802.11ac built upon many of the lessons learned in 802.11n and permitted up to 8 spatial streams using up to a 160 MHz channel. The first Wave 1 products to market supported up to 80 MHz channels with three spatial streams. All devices Wi-Fi certified for 802.11ac W1 must operate at 20, 40 and 80 MHz channel width. In the 802.11n specification 40 MHz operation was vendor optional and allowed for a mismatch of client capabilities to network design. Not all 802.11n devices can take advantage of a 40 MHz channel plan and see no gain for the reduced number of channels.

As of this writing, Wave 2 products are just starting to hit the market and implement up to 4 spatial streams and a 160 MHz channel width, this is formed by bonding 2x80 MHz channels together as a single channel (consuming a total of 4x20 MHz channel assignments). Again, 4 spatial streams means 4 transmitters and receivers (and antennas) – so there is a real estate issue right away with 8 Tx/Rx chains for a single band radio.

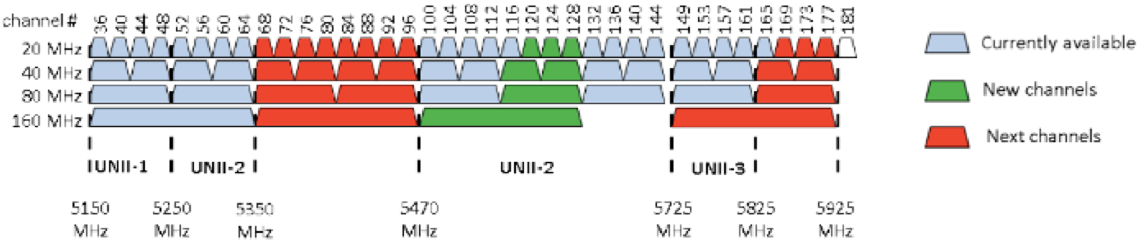
Note Just like 802.11n which supported up to 4 Spatial Streams, the practical limit was 3 Streams as gains from a fourth are miniscule. 8 Spatial Streams for 802.11ac is unlikely on a single 5 GHz radio. Pay attention as some manufacturers are marketing 4 ss on 2.4 and 4 ss on 5 GHz as 8 spatial streams – not quite the same thing. For More on Spatial Streams *see* Fundamentals of Spatial Streams with Rob Lloyd for an excellent short discussion.

The other major contribution to Wi-Fi coming with Wave 2 is MU-MIMO – That is Multi User MIMO. With 802.11ac MU-MIMO it will be possible to serve multiple clients on separate spatial streams simultaneously. For an in depth view of 802.11ac *see*: 802.11ac: The Fifth Generation of Wi-Fi Technical White Paper

US 5 GHz channel Plans

The creation of protocols that can consume ever larger channels (20/40/80/160 MHz) involves lot of pressure on the existing channels today. Due to regulatory restrictions, it is not always possible to bond channels in two separate frequency ranges (even though the 80+80 mode in 11ac enables this) – and today we have gaps between the channels defined, so there are real limits. In the US, more spectrum has already been granted (the return of channels 120, 124, 128) and facilitated the use of two 160 MHz channel possibilities. Additional spectrum has been requested to bridge gaps in ranges and is in currently under consideration to allow for more. World Wide, other regulatory agencies are taking note – as pressure is increasing every where. US Channel and band assignments for 20, 40, 80 and 160 MHz channels are depicted below with future requested allocations noted.

Figure 3-5 Current US 5 GHz 802.11 Wi-Fi channel plan



The data rate increases for 802.11ac come in three forms, either more spatial streams (1-8), wider channels (20/40/20/160 MHz) or expansion of encoding rates. 802.11n was limited to 2 channel widths, and 4 spatial streams (only 3 of which are practical) – so MCS 1-23 was used to define the speeds – with 0-7 defining the data rate for 1 spatial stream, and 8-15, 16-23 repeating those rates on first 2, then 3 spatial streams. We have 8 spatial streams now – so something needed to be done. I wish it were simpler – but MCS 0-9 now define the modulation and coding rate only. Multipliers are used to calculate the impact of additional spatial streams, and or additional channel widths. The table below shows up to 2 spatial streams and all channel widths. It's not easier – but it is easier in the long run given the challenge. Note the multiplier rules below the table.

Table 3-2 802.11ac MCS Data Rates

MCS Index	Modulation Type	Coding Rate	Spatial Streams	20 MHz	40 MHz	80 MHz	160 MHz
0	BPSK	1/2	1	7.2	15.12	32.4	64.8
0	BPSK	1/2	1	14.4	30.24	64.8	129.6
1	QPSK	1/2	1	14.4	30.24	64.8	129.6
1	QPSK	1/2	1	28.8	60.48	129.6	259.2
2	QPSK	3/4	1	21.7	45.57	97.65	195.3
2	QPSK	3/4	1	43.4	91.14	195.3	390.6
3	16-QAM	1/2	1	28.9	60.69	130.05	260.1
3	16-QAM	1/2	1	57.8	121.38	260.1	520.2
4	16-QAM	3/4	2	43.3	90.93	194.85	389.7
4	16-QAM	3/4	2	86.6	181.86	389.7	779.4
5	64-QAM	2/3	2	57.8	121.38	260.1	520.2
5	64-QAM	2/3	2	115.6	242.76	520.2	1040.4
6	64-QAM	3/4	2	65	136.5	292.5	585
6	64-QAM	3/4	2	130	273	585	1170
7	64-QAM	5/6	2	72.2	151.62	324.9	649.8
7	64-QAM	5/6	2	144.4	303.24	649.8	1299.6
8	256-Qam	3/4	3	86.7	182.07	390.15	780.3
8	256-Qam	3/4	3	173.4	364.14	780.3	1560.6

Table 3-2 802.11ac MCS Data Rates (continued)

MCS Index	Modulation Type	Coding Rate	Spatial Streams	20 MHz	40 MHz	80 MHz	160 MHz
9	256-Qam	5/6	3	96.3	202.23	433.35	866.7
9	256-Qam	5/6	3	192.6	404.46	866.7	1733.4

1. MCS9 20 MHz not legal per specification for SS1, 2, 4, 5, 7, 8
2. Each spatial stream adds %100 (i.e.) MCS0 1ss data rate = 7.2 x2 for 2 ss, x3 for 3 ss
3. Channel width multipliers = 20 MHz speed x 2.1 for 40 , 4.5 for 80, 9 for 160, i.e. MCS0 20 MHz, 1ss = 7.2 Mbps x 2.1 for 40 MHz = 15.2

802.11ac is a quantum leap in efficiency for Wi-Fi. As for device support, more spatial streams means more power and antennas. Radio designs continue to improve and we are already seeing more multi spatial stream implementations in smaller devices. Today, a lot of the clients are limited at 1-2 spatial streams (ss), but all 802.11ac clients must support up to 80 MHz channel operation for certification. A 160 MHz channel is a tight squeeze in current spectrum allocations in the US – and ranges to impossible in some regulatory domains. For reference – a 3ss Wave1 client operating in 80 MHz today can achieve a data rate of 1.3 Gbps, We will be going faster too in the future.

Understanding the IEEE 802.11 Standards

IEEE 802.11 is the working group within the Institute for Electrical and Electronics Engineers (IEEE) responsible for wireless LAN standards at the physical and link layer (Layers 1 and 2) of the OSI model, as compared to the Internet Engineering Task Force (IETF), which works on network layer (Layer 3) protocols. Within the 802.11 working group are a number of task groups that are responsible for elements of the 802.11 WLAN standard. Table 3-3 below summarizes some of the task group initiatives.

For more information on these working groups *see*: http://www.ieee802.org/11/

Table 3-3 IEEE Task Group Activities

Task Group	Project
MAC	Develop one common MAC for WLANs in conjunction with a physical layer entity (PHY) task group.
PHY	Develop three WLAN PHYs—Infrared, 2.4 GHz FHSS, 2.4 GHz DSSS.
a	Develop PHY for 5 GHz UNII band.
b	Develop higher rate PHY in 2.4 GHz band.
c	Cover bridge operation with 802.11 MACs (spanning tree).
d	Define physical layer requirements for 802.11 operation in other regulatory domains (countries).
e	Enhance 802.11 MAC for QoS. (see Chapter 5)
f	Develop recommended practices for Inter Access Point Protocol (IAPP) for multi-vendor use.
g	Develop higher speed PHY extension to 802.11b (54 Mbps).

Table 3-3 IEEE Task Group Activities (continued)

Task Group	Project
h	Enhance 802.11 MAC and 802.11a/n/ac PHY-Dynamic Frequency selection (DFS), Transmit Power control (TPC).
i	Enhance 802.11 MAC security and authentication mechanisms.
j	Enhance the 802.11 standard and amendments to add channel selection for 4.9 GHz and 5 GHz in Japan.
k	To facilitate roaming, an 11k capable client associated with an AP requests a list of suitable neighbor APs. The 802.11k capable AP responds with a list of neighbor APs on the same WLAN along with their current Wi-Fi channel numbers.
m	Perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.
n	Focus on high throughput extensions (>100 Mbps at MAC SAP) in 2.4 GHz and/or 5 GHz bands.
o	Provide Fast Handoffs in Voice over WLAN (goal is around 50 ms)
p	Focus on vehicular communications protocol aimed at vehicles, such as toll collection, vehicle safety services, and commerce transactions using cars.
r	802.11r introduces a new concept of roaming where the initial handshake with the new AP is done even before the client leaves the current AP. This is called Fast Transition (FT)
s	Define a MAC and PHY for meshed networks that improves coverage with no single point of failure.
t	Provide a set of performance metrics, measurement methodologies, and test conditions to enable manufacturers, test labs, service providers, and users to measure the performance of 802.11 WLAN devices and networks at the component and application level.
u	Provide functionality and interface between an IEEE 802.11 access network (Hotspot) and any external network.
v	Provide extensions to the 802.11 MAC/PHY to provide network management for stations (STAs).
w	Provide mechanisms that enable data integrity, data origin authenticity, replay protection, and data confidentiality for selected IEEE 802.11 management frames including but not limited to: action management frames, de-authentication and disassociation frames.
ac	This amendment specifies enhancements to the 802.11 MAC and PHY to support very high throughput (500-1000 Mbps) in the 5 GHz bands.

Deployment Considerations

Should I design for 2.4 or 5 GHz?

Wi-Fi is a relatively mature technology today. While there are still places where Wi-Fi is not present, it is hard to find any place where there are people and places, that doesn't have some signal coverage today. A good way to look at this is: the more independent neighbors you have – the more Wi-Fi interference you either already have – or possibly will. This is often at its worst in multi-dwelling facilities where many disparate company offices share a single building and spectrum.

This is of critical importance, since Wi-Fi passes through walls and floors and must operate and accept all interference from other Wi-Fi and non Wi-Fi devices alike. What this means is that to the degree that your network devices can hear other networks – they will share the available airtime with those other networks. If you and your neighbor are both heavy users, in the areas that your networks overlap you will both get less bandwidth than the connection speeds would suggest. For both networks waiting on the other to access the channel will cost time (and less time on the air leads to less throughput).

Using 2.4 GHz in a congested metropolitan city, multi dwelling facility, or shopping mall will enjoy variable success at best and frequently can be unusable at worst. Best Practices recommends three non-overlapping channels in most of the world. In a densely deployed environment with multiple different network owners– someone is always trying the other 8-10 channels in hope that this will buy some advantage in an over filled spectrum. Most often, it does not; in fact choosing channels that overlap others makes it worse for everyone.

When two AP’s are on the same channel, the contention mechanisms of each allow for fair access to the channel between them. An AP on a different but overlapping channel can’t demodulate the 802.11 packets on the overlapped frequencies and it appears only as noise. Without the 802.11 mac layer, no coordination is possible between the two AP’s. Errors, and collisions increase for both AP’s cell’s increasing utilization and wasting precious airtime. If you live in a region where a 4 channel plan is possible (1, 5, 9, 13) keep in mind that many client drivers will not enable channels 12 and 14 by default. Also most consumer and many AP systems default to using channels 1, 6, 11. Under these conditions channel 6 will interfere with both channel 5 and 9, and channel 11 interferes with 9 and 13 and vice versa. If your neighbors are using 1, 6, 11 – you should too – it will perform better.

If an application is critical to business operations, plan on using 5 GHz. Once upon a time – this was more difficult to do as 5 GHz devices were less prevalent. This is not the case today as most manufacturers are focusing on 802.11ac as the standard for their products and 802.11ac only operates in 5 GHz.

If you absolutely must deploy a critical function on 2.4 GHz understand why and what is driving that requirement (specifically which devices) and consider replacing these with updated hardware. You can only put so many 2.4 GHz radios in close proximity to one another and once the channels are full – they are full.

A look at the Wi-Fi Alliance certification database (Wi-Fi Alliance certification product-finder) confirms that 5 GHz support is plentiful in todays devices. Consider these findings from the latest results

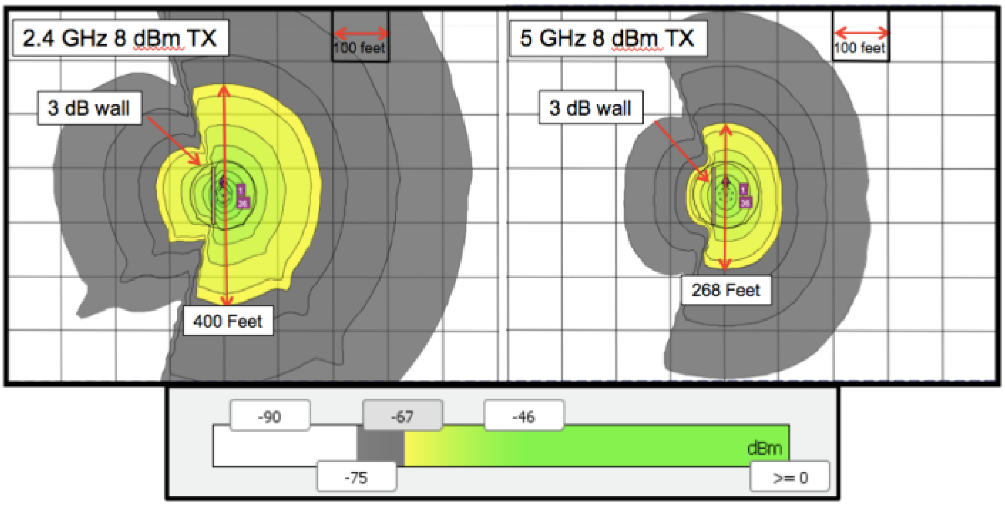
- As of August 2015 – 2,409 Smartphones/tablets have certified 5 GHz 802.11n operation.
  - 477 of which where certified in 2013
  - 591 in 2014/15 – all 802.11ac
  - Total WFA certifications for the same period is 3167 putting 2.4 GHz only devices at 24% of the current Market (this down from 32% 6 months previous)
  - The majority of these being low end consumer gear

Table 3-4 Pro's and Con's 2.4 vs. 5 GHz

Frequency Band	Pro	Con
2.4 GHz	Good Range - As frequency increases, propagation distance decreases (assuming equivalent transmit power)	Less AP's can be configured in the same physical space due to mutual interference, less capacity
	Higher penetration of objects - better range indoors	Less AP's can be configured in the same physical space due to mutual interference, less capacity
	Less Spectrum/channels	Increased congestion
		Increased risk of interference from improper implementation-rogues
		Favorite band for non-Wi-Fi devices - increased interference in general
		Not enough channels to use bonded channels and increase throughput - increased interference
5 GHz	Less range/ self interference, more AP's possible, more users	Less range generally means more AP's possibly required (higher power levels for UNII_3 is generally only supported by the AP side
	More Channels - bandwidth - Capacity	
	Less consumer Wi-Fi devices and non Wi-Fi. Less congestion	
	802.11ac - only in 5 GHz	
		less range - not as suitable for low density hotspot coverage models

In Figure 3-6 you can see the difference in usable signal for both the 2.4 GHz band on the left, and the 5 GHz signal on the right using the same Tx power setting. In the Unii-3 band – power can be increased to 23 dBm and 5 GHz can cover more than 2.4 GHz but only in that band. The numbers of people who will share the fixed bandwidth available for the AP in each are contained within the cell's footprint.

Figure 3-6 Propagation Distance of 2.4 GHz and 5 GHz



What Protocols should I enable?

There are multiple protocol standards available in the 802.11 standard, in fact everything that has been ratified since 1999 is still required for WFA certification and present in all hardware that supports the band it belongs to. That doesn't mean that you need to use it though. The choices you make in deciding which protocols to support (and which NOT to) can have a big impact on your networks efficiency.

By efficiency we mean the use of airtime. The faster a station can get onto and off of the air, the more airtime will be available for other stations. 802.11b as previously mentioned was one the first protocols implemented in 2.4 GHz. Today it is truly a unique example amongst all other Wi-Fi protocols as both the coding and modulation methods are completely different than every other protocol that has been ratified since.

As a group – the legacy protocols of 802.11b, a and g all used a wide guard interval of 800 ms. The guard interval is a time space between radio symbols (characters) being transmitted that ensures they do not collide in the air. 802.11n and 802.11ac have an optional short Guard Interval, but in practice all products implement this option. You can see the gains that a short guard interval provides in the 802.11n data rate chart (Table 3- 1 802.11n MCS 1-23 data rates), they are significant.

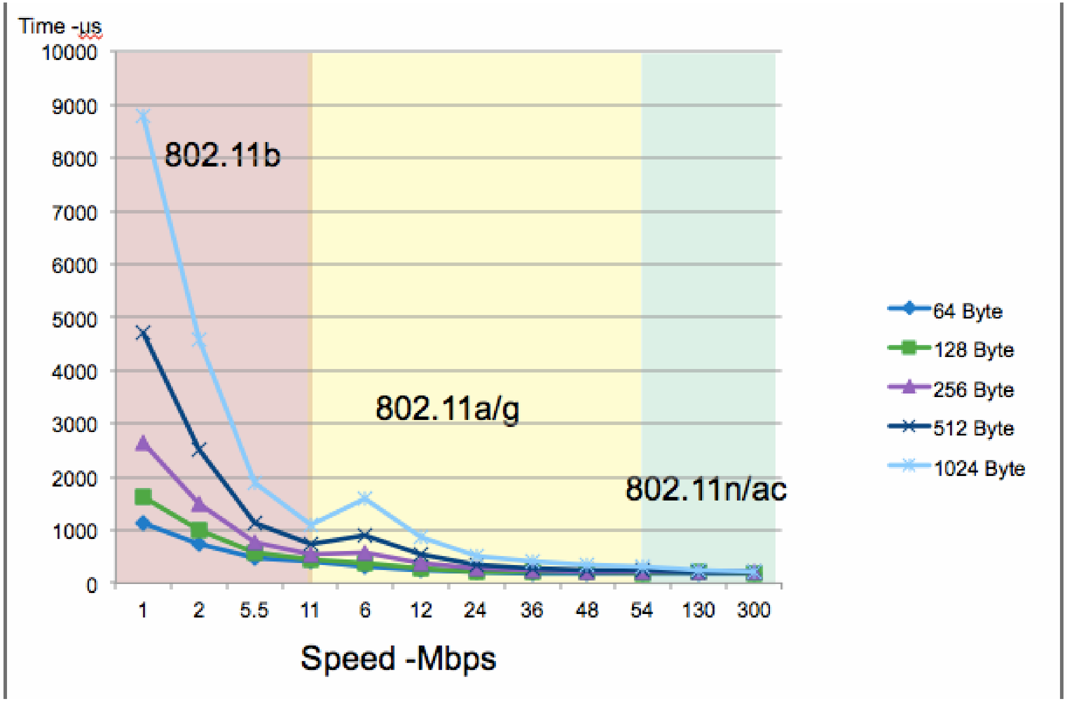
802.11n and 802.11ac also provide for block ACK, or block acknowledgments, which allows for higher efficiency gains by allowing a large block of packets to be acknowledged all at one. The legacy protocols all send a packet – get a response – one by one. This adds a considerable number of frames to the transaction for reliability that is largely no longer needed with modern standards.

Think about it this way - a golf cart has 4 wheels and a steering wheel just like an automobile– but you would hardly let it enter a formula one race. Imagine the outcome of that – and that's pretty much what happens in a no holds barred Wi-Fi network.

Figure 3-7 below compares the airtime requirements of different protocol standards and data rates using different sized packets over the air. This shows airtime (µs) consumed per packet, before any gains from aggregation are realized. It is easy to see that even a modest 802.11n or ac speed can move twenty 1024 byte packets before 802.11b can move 1.

Note The lower the data rate – the longer the airtime required for a given packet size. Less over all data can be accommodated within each second. Less available bandwidth is the result.

Figure 3-7 Airtime of Packets by Speed and Size



As a network architect, the concern is to provide services that everyone can use. The good news is that by and large there are very few environments where you will find a "real" requirement for native 802.11b or legacy protocols today.

Cisco WLC's have several options available for implementing the most popular and necessary speeds. The various network types and decision points is detailed later in this document to ensure you to understand the need of implementing a well-tuned network from the start.

What is a DFS channel, should I use them?

Many of the channels available in 5 GHz are known as DFS channels. DFS stands for Dynamic Frequency Selection and along with TPC (Transmit Power Control) define co-existence mitigations (i.e., detect and avoid) for radar while operating in the UNII-2 and UNII-2e bands (channels 52-144). These mechanisms are detailed in an amendment to the 802.11 standard.

The 802.11h standard was crafted to solve problems like interference with satellites and radar which also legally use the 5 GHz band as primary users. A primary user has priority over the frequency range of UNii-2 and UNii2e. It is Wi-Fi's job, as a condition of using these frequencies, to not interfere with any primary users. While this standard was introduced to primarily address European regulations, it is used by many other regions of the world today to achieve the same goals of more operational 5 GHz spectrum for Wi-Fi.

In 2004, the US added channels 100-140 in the UNII-2e (e stands for extended) band with rules requiring 802.11h certification which allow us to peacefully coexist with Primary licensed users of the 5 GHz frequencies in this range. For Europe these channels represent most of their available 5 GHz spectrum today. Before the rules and mechanisms where worked out, Europe was limited to only 4 channels in 5 GHz. At the same time in the US we had UNII-1, 2 and 3 for a total of 13 channels.

In order to not interfere with licensed band users – the requirement is pretty straightforward:

1. The Wi-Fi equipment must be able to detect radar and satellite emissions
2. Before using a channel in this range – a "channel master" (an Infrastructure AP) must first listen for 60 seconds and determine that the channel is clear of Radar
3. If a radar signal is detected, the Wi-Fi channel master – and all the clients associated to it have to abandon the channel immediately and not return to it for 30 minutes at which time it can be cleared again for Wi-Fi use if no radar emissions are detected.

Unii-2e channels got a bad name early in 2004 in the US. Clients were slow to adopt the new rules initially – so using these channels in the infrastructure meant you could inadvertently configure a channel that some clients wouldn't be able to use – creating a coverage hole for that client type. There was also undue concerns about DFS operations in a production network. The concern was if DFS detected radar, a channel change followed by waiting a full minute before resuming transmissions was viewed as disruptive – however the behavior is not disruptive as RRM places the AP into a non DFS channel. The channel is blocked for 30 minutes and then made available again to RRM by means of background scanning. Once the channel is available we can choose to use it or remain on the current channel – depending which is better for the clients.

It has been a decade since the addition of these channels and 802.11h logic. In Europe DFS is and has been making 5 GHz Wi-Fi possible and even flourish. Client vendors vary, the majority support the DFS channels just fine as there is no additional logic required by the client.

If you are within 5 Miles of an airport or shipping port and have concerns, evaluate by monitoring the channel range with Cisco AP's. Cisco leads the industry in certified hardware models and function for DFS operation and flexibility, monitoring the channels will alert you to any potential interference and identify the affected channels.

Site Survey

A site survey is an important tool. It will tell you who is operating around you – and more importantly where and how much that interferes with your intended coverage zones. It also allows identification of mounting locations, existing cable plants, infrastructure requirements, architectural oddities, and yields a plan to get the coverage your particular application requires. Because RF interacts with the physical world around it, and all buildings and offices are different so is each network to a degree. Unfortunately, there is no one size fits all for Wi-Fi. There are recommendations by deployment type and it is possible to generalize what is likely to be encountered. If you have not done a site survey in a while – keep in mind what has changed since the last one before you decide against it.

1. The protocols and radio technology
2. How the users will use the network (likely everyone, and for almost anything)
3. How many clients the network supports (likely a lot more users count as atleast two devices these days and many have more)
4. The primary use of the network (very likely changed since the initial plan and implementation)

While early WLAN designs focused on coverage in order to get a few casual users signal everywhere, todays WLAN designs are more focused on capacity – as the number of users has increased – and what we are demanding of the network has gone up exponentially. A capacity design requires more AP's in closer proximity to manage the number of users who are sharing the bandwidth of the cell. Increasing placement density should have a plan.

If you decide to conduct your own survey and plan – tools are important. There are multiple free tools on line and available as downloads. However if you want professional results – you need professional tools.

The free tools can provide simple solutions for smaller less complex projects. But if you are looking to provide ubiquitous multi media coverage in a multi-floor/multi building campus – you need a good tool to balance the elements that will be required for success. Planning tools have evolved with the radio technologies and applications in use today. A familiarity with the design elements and applications is required to produce a good plan.

Cisco Prime Infrastructure has a planning tool built in – and you can import and export maps and plans between CPI and many top Survey and Planning applications such as Ekahau ESS, Airmagnet Pro Planner and Survey.

For more on Site Surveys – *See* Site Survey Guidelines for WLAN Deployment

Having a site survey done for 802.11ac now – will yield good information that can be used again and again as the network grows and continues to evolve. It depends on the size of your project and level of knowledge with regards to Wi-Fi if this is something that you should contract out in part or as a whole.

Planning for RF Deployment

Different Deployment Types of WLAN Coverage

How much WLAN coverage you set in the design of your wireless network depends largely on the usage and density of clients you require. With limited exceptions, all designs should be deployed to minimize retransmission and data rate shifting while supporting good client roaming and throughput. Wireless networks can be deployed for data-only, voice, video, and location-aware services or more frequently these days, a combination of all of these. The difference between these application types is minimal today with the requirements of each largely describing good solid capacity based coverage. Location Aware services adds some AP placement criteria for good location triangulation and guidelines on Hyper-Location technologies. Real Time Multi-media (voice and video) applications have different latency requirements for two way live implementations. But by and large all describe a minimum coverage level that needs to be achieved to make the application viable for the number of users you expect in any given area.

For the majority of campuses and enterprise installations coverage and capacity are the primary concern and easily achievable. High Density Client implementations or High interference locations – like shopping malls or apartment buildings may require additional equipment like external antenna's to properly implement to scale. For more on application specific guidelines, recommendations and configurations – see the following guides for in depth information:

- Best Practices Location-Aware WLAN Deployment guide
- Microsoft Lync Client/Server in a Cisco Wireless LAN
- Cisco Jabber and UCM on a Cisco Wireless LAN
- Application Visibility and Control Feature Deployment Guide 8.1

- Wireless LAN Design Guide for High Density Client Environments
- Cisco Wireless Mesh Access Points, Design and Deployment Guide, Release 8.1

Coverage Requirements

Most application specific coverage guidelines describe the signal level or coverage at the cell edge required for good operation as a design recommendation. This is generally a negative RSSI value like -67 dBm. It's important to understand that this number assumes good signal to noise ratio of 25 dB with a noise floor of -92 dBm. If the noise floor is higher than -92 dBm then -67 dBm may not be enough signal to support the minimum data rates required for the application to perform it's function.

For Location-Aware services, deploying a network to a specification on -67 dBm is fine – however what matters to Location-Aware applications is how the network hears the client – not how the client hears network. For Location-Aware we need to hear the client at three AP's or more at a level of >= -75 dBm for it to be part of the calculation. (-72 is the recommended design minimum)

Clients are a big consideration when planning coverage. They come in all shapes and sizes these days, and as a result individual implementations can and do vary widely on their opinion of a given RF signal. For instance, the laptop you are using for Surveying may show -67 dBm at the cell edge, the tablet might show -68 dBm, and the smartphone may show -70 dBm. These are all very different opinions and affect roaming and data rates that each individual will use. Overbuilding to accommodate this varying opinion assures a trouble free installation. When taking measurements using the device that will support the application is the best approach. Understanding that your smartphones are generally 5 dB off your survey tool will let you develop good rules for design (like add or subtract 5 dB to what ever the reading is from your survey tool). Then test and tune the resulting implementation.

High Density Client Coverage Requirements

One thing that can dramatically affect the success of a network is High Client Density areas. As mentioned earlier – every client contained within an AP's Cell Boundary is sharing the potential bandwidth (airtime) of that cell. Using simple math to illustrate this – we will use the rule of 555 simply for illustration of the concept. Sharing 1 Gbps equally for 200 concurrent clients at 5 GHz each client will cost you 5 msec of airtime and receive 5 Mbps.

1000 Mbps/200 = 5Mbps

1 sec/200 = 5 msec

In reality, more clients will bring more overhead, collisions and errors with the varying conditions across a cell. Some clients will get more than 5 Mbps, and some will get less. This is an average view of the cell only. A good average cell throughput under similar conditions will provide an accurate prediction of the mileage you will get.

Providing more bandwidth is as simple as changing the equation, if you need to support 100 clients at 2-5 Mbps, you will need another AP on a different channel to provide more bandwidth to share between the clients. You can add more AP's to get additional capacity, as long as you use different channels. You can re-use existing channels to accomplish this at scale, provided that the first re-use of a channel cannot be heard by another AP using that channel.

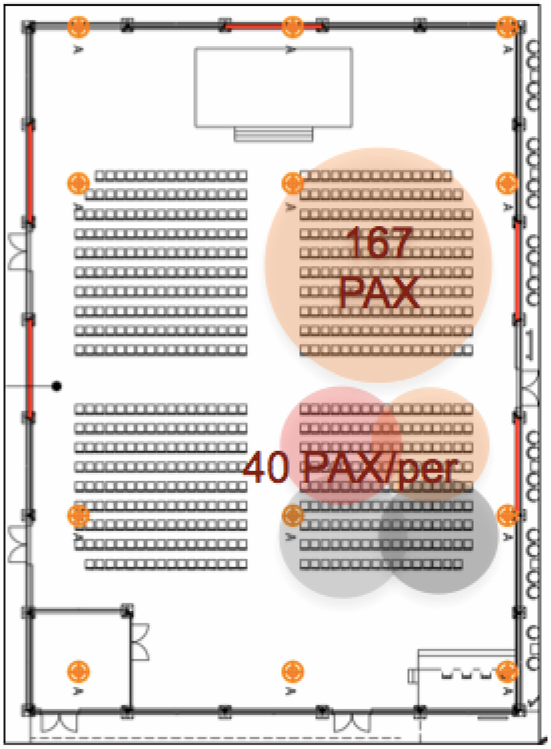
If two AP's on the same channel can hear one another, then they will share the channel equally (assuming each is equally busy). The 802.11 specifications have contention mechanisms built into the specification that ensure this. But you really have not increased the bandwidth for these users – since both cells are sharing a channel (each getting 50% of the airtime), and now we have 2 AP's which effectively doubles the management traffic further reducing the available airtime.

In 2.4 GHz where we only have 3 usable channels, channel re-use becomes a problem far sooner than at 5 GHz where we have many more channels to choose from. Propagation characteristics also come into play – since 2.4 GHz will be heard farther away than 5 GHz you are further limited to the number of re-uses in a smaller physical area with 2.4 GHz options.

In 5 GHz, we have multiple channel widths to consider. The wider the channel width selection the fewer overall channels you will have (but in exchange, the greater capacity per cell).

Larger cells cover more users, in order to increase bandwidth in a given physical area; smaller cells will yield more capacity. In the graphic below, each seating section accommodates 167 seats (seats are represented as PAX in Figure 3-8), we could cover the entire section with one access point, or by designing smaller cells we can get 4 AP's serving the same area for a 4x increase in available bandwidth.

Figure 3-8 User vs. Cell Density



For most Enterprise installations higher density conference rooms and the like can be handled just fine using internal Omni Directional antenna AP's. Cisco's RRM will handle the channel and power required to make it work. At a certain point – with too many AP's being too close together – RRM will configure for the most optimal efficiency possible, but there must be spectrum available or it can do nothing. You can only turn the AP's power down so much, and the Omni directional antenna pattern will hear other adjacent AP's and the user experience will suffer. Coverage levels at 2500 sq feet per AP and up should be fine at 5 GHz with 20/40 MHz channels. For 2.4 GHz requirements at cell densities going below 2500 sq feet, you will likely need directional antennas to physically limit the transmit and receiver patterns of the AP and get useful smaller cells.

There are many features that have been specifically developed to manage and configure High Density client/AP environments; they are part of a group of features known as HDX (High Density Experience). See the HDX deployment guide below for specifics of each feature:

High Density Experience (HDX) Deployment Guide

Roaming and Voice Coverage Requirements

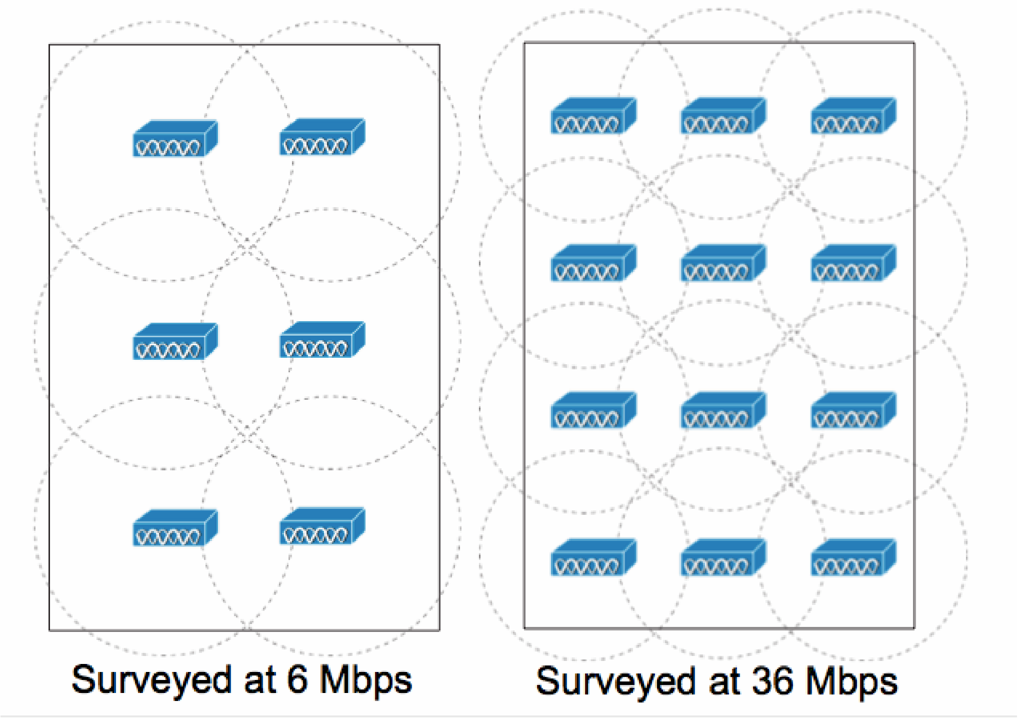
Client Roaming enables a client to move from one AP's coverage zone into another AP's coverage zone minimizing interruption in service/coverage. This is the very essence of mobility. There are many factors that must be considered in order for this to be effective. For instance, how the client transitions it's association and authentication from one AP to another must be considered as well as the time it takes to do so. An often-overlooked aspect is the network design itself. In order for a client to roam – there must be something to roam to. Cells must overlap with good coverage in order for a client to gracefully leave coverage of one cell and establish association within coverage on another without delay. Too little overlap encourages "sticky" clients, meaning a client holding onto an AP well after it moves into the coverage area of another AP.

When designing for network coverage, consider the amount of overlap in the required signal range you are getting. Overlap should be 10-15% (15-20% for Voice) of the total coverage area. Voice is particularly sensitive as the conversation is real time – and any coverage lapse will result in broken audio or potentially a lost call. An easy way to calculate overlap – measure the distance from the AP that you reach -67 dBm – multiply that distance x 1.4 for 15-20% or 1.3 for 10-15% and that's where your next AP goes.

Data rates are also matter, as the usable cell size increases with lower data rates and decreases with higher data rates. Higher Data Rates require a higher SNR, and since the noise floor is theoretically constant – the closer the client is to the signal (the AP) the higher the SNR and the resulting data rate will be. We can enforce minimum data rates in configuration, and when a client can no longer support a given data rate – it will have to move.

Figure 3-9 shows the Cell overlap and the effect that data rates have on cell size.

Figure 3-9 Cell Density and Overlap at different data rates



A good physical design enables and supports roaming at the physical layer. Only the client decides when to roam though and the decisions it makes are based on the clients observation of the network. There have been multiple amendments added to the 802.11 specification specifically to help clients make better decisions based on network infrastructure observations. See these guides for additional information on Roaming and configuring Cisco hardware/software to enable good roaming transitions. Cisco supports 802.11r, 802.11k, and 802.11v which assists capable clients in making good decisions and affords some control from the infrastructure to enforce design goals:

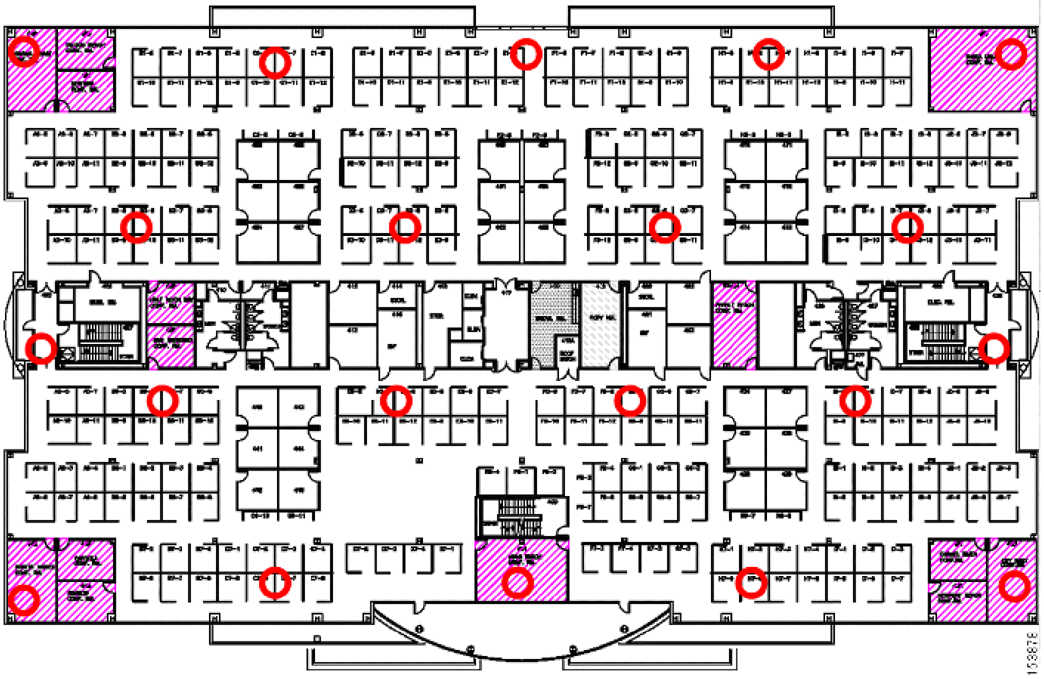
- High Density Experience (HDX) Deployment Guide - see Optimized Roaming
- 802.11 WLAN Roaming and Fast-Secure Roaming on CUWN
- 802.11r, 802.11k, and 802.11w Deployment Guide, Cisco IOS-XE release 3.3

Location-Aware Coverage Requirements

Location –Aware deployments differ slightly from other types in that the goal of the installation is to provide good location resolution of Clients, Tags, and IOT sensors in context of where they are on a given map. We derive this information in its most basic form Client RSSI readings obtained by multiple AP's (a minimum of 3 AP's are required to Triangulate on the clients position). The pattern that you choose to deploy your AP's can have a big effect on the networks ability to "locate" a client accurately.

For good Location resolution, the APs are laid out in a staggered pattern with AP's defining the borders and corners. It is possible to get coverage using AP's in a straight line down the middle of both sections – however this would not provide enough AP's to hear and triangulate on clients in all locations (remember – we need 3). Coverage and capacity requirements for this floor require so many AP's to start with, so it is quite likely given your coverage requirements that you already have what is needed to perform good location calculations.

Figure 3-10 2.4 Example of a Single Floor Location AP Placement



The Best Practices-Location Aware-WLAN Design Considerations is a must read chapter and still quite relevant as the physical requirements for the design have not changed. The entire document Wi-Fi Location Based Services 4.1 Design Guide is a good reference for Theory, particularly the first chapter Location Tracking Approaches will familiarize you with the technology.

Power Level and Antenna Choice

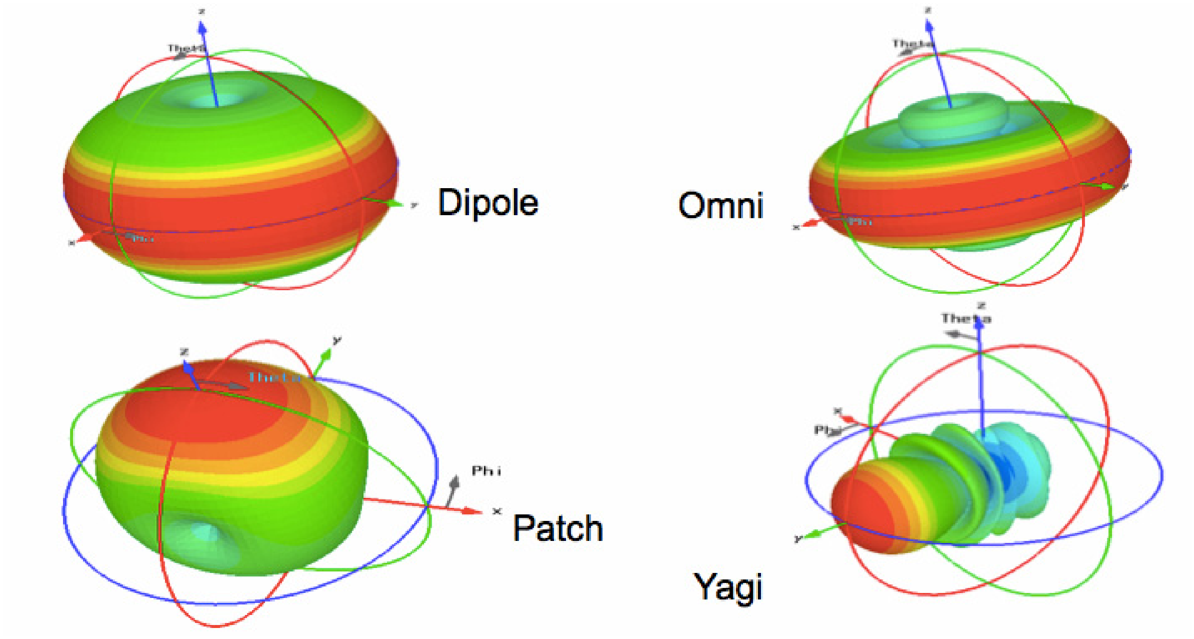
Power level and antenna design choice go hand-in-hand to determine AP placement/coverage results. Together, these two variables determine where and how powerful the RF is in any given place in the environment. Along with choosing the correct antenna to produce the required coverage area, we recommend you to use RRM to control the power level and provide the optimal channel/power plan. For more information, see *RRM* section below in this document.

An antenna gives the wireless system three fundamental properties:

- Gain—A measure of increase in power introduced by the antenna over a theoretical (isotropic) antenna that transmits the RF energy equally in all directions. Gain also affects received signals and can assist weaker client devices by increasing the signal presented to the receiver.
  - Front To Back Ratio or FTB – the opposite of gain is signal rejection – the opposite direction of the gain in an antenna is less sensitive than the focus of the antenna, and this property can be used to isolate your cell from unwanted signals behind the antenna for instance.
- Direction—The shape of the antenna transmission pattern. Different antenna types have different radiation patterns that provide various amounts of gain in different directions. A highly directional antenna will produce a very tight beam pattern. Outside of the area of focus, signals erode quickly which allows more cells to be placed in the same physical space without interference.
- Polarization—Indicates the direction of the electric field. An RF signal has both an electric and magnetic field. If the electric field is orientated vertically, the wave will have a vertical polarization.

A good analogy for how an antenna works is the reflector in a flashlight. The reflector concentrates and intensifies the light beam in a particular direction similar to what a parabolic dish antenna does to an RF source in a radio system. The antenna however is both the ears and the mouth of the AP – so characteristics of a given antenna work for both transmit and receive. Many different antenna designs exist to serve different purposes some of the more familiar designs appear below in Fig. 11

Figure 3-11 Antenna design types



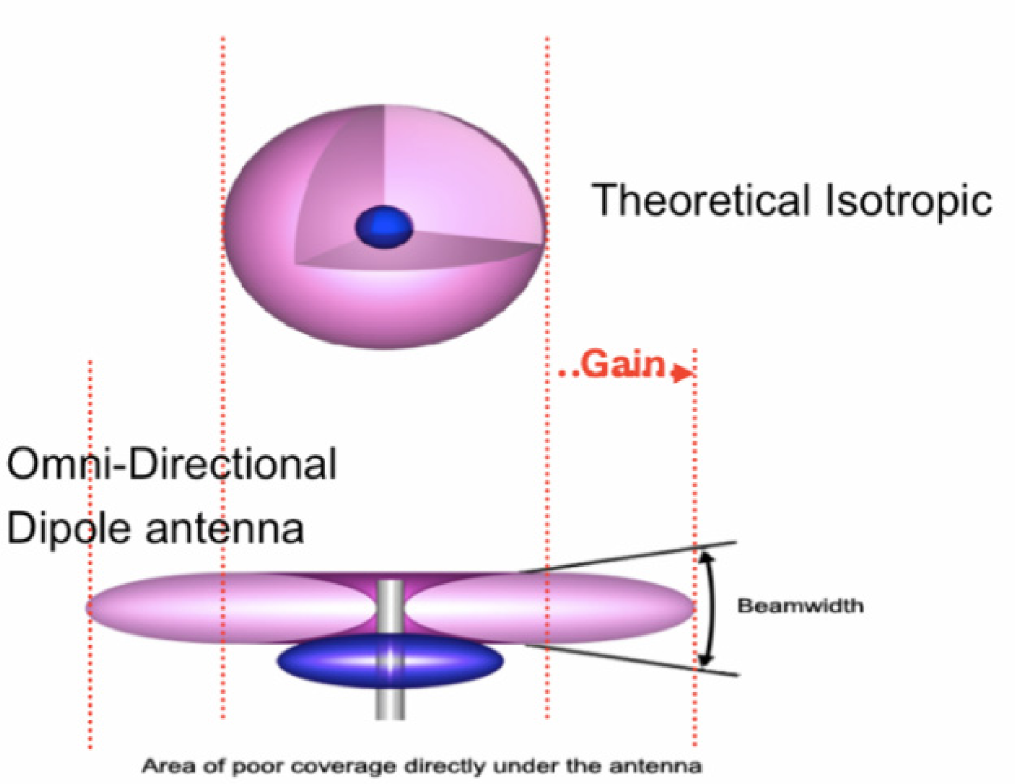
Gain and direction mandate range, speed, and reliability while polarization affects reliability and isolation of noise.

For more information on antenna selection, see the Cisco Aironet Antennas and Accessories Reference Guide

Omni-Directional Antennas

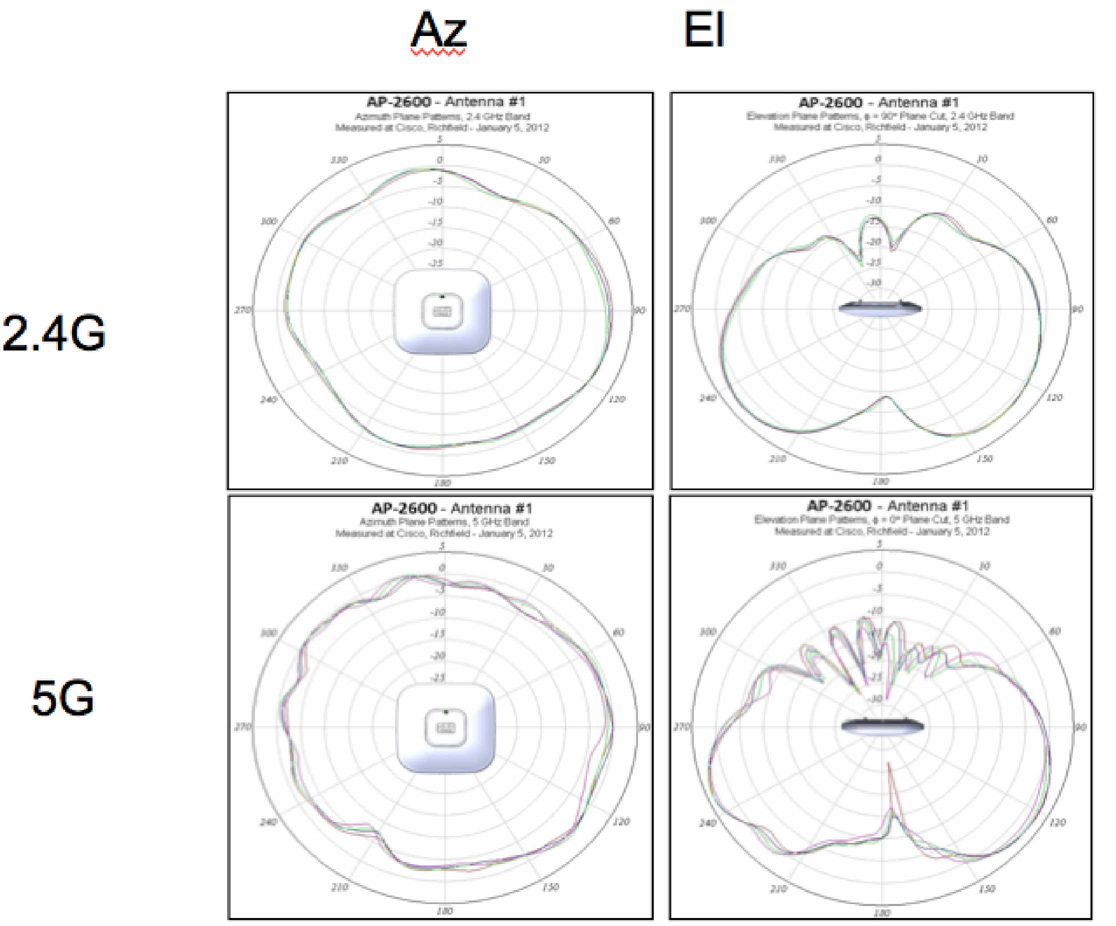
Omni-directional antennas have a different radiation patterns compared to isotropic antennas; the isotropic antenna is theoretical and therefore all physical antennas are different to the isotropic antenna. Any change in shape of the radiation pattern of an isotropic antenna is experienced as gain and increases directionality. The dipole Omni-directional antenna features a radiation pattern that is nearly symmetric about a 360 degree's axis in the horizontal plane and 75 degrees in the vertical plane (assuming the dipole antenna is standing vertically). The radiation pattern of an Omni-directional antenna generally resembles a donut in shape and hence is directional. The higher the rated gain in dBi of a given Omni-Directional antenna, the more focused the energy is (generally in the vertical plane) and directional it becomes. See the comparison between an isotropic and Omni-Directional dipole antenna in Fig. 12 below. Note the views are from the side.

Figure 3-12 Isotropic Antenna vs. Omni-Directional



Most modern day internal antenna AP models beginning with the AP 1140 use internal antenna stubs with multiple transmitters and receivers. Unlike the simple Dipole antenna, this produces a pattern that has an improved donut shape. In the antenna plots below – note the elevation plane and how the energy is predominantly focused downward in Fig. 13.

Figure 3-13 Cisco AP 2600i 2.4 and 5 GHz Radiation Patterns



This makes the AP least sensitive on the back – the part that is facing the ceiling in most installations.

Omni-Directional antenna's work well, and are easy to implement – to a point. If you are faced with increasing the density of AP's to accommodate more capacity requirements, then you will see increasing channel utilization from self-interference. This happens because the antenna pattern is designed for maximum coverage. 3000-6000 sq ft (280 -560 sq meters) of coverage per AP can be managed with the internal antennas, if your coverage requirements are at the minimum or denser than this, you should consider directional antennas.

Directional Antenna's

A directional antenna differs from an Omni-Directional antenna in that the energy is focused in a particular way to achieve different coverage goals. Most people assume that a directional antenna is used specifically for gain – to increase power. While it can be used for that reason and achieve greater distances, it is more often used in Wi-Fi to control the size (and shape) of the transmit and receive cell.

For current Cisco indoor AP's (3600e, 2600e, 3700e, 2700e the antenna selections are all dual band (each antenna covers 2.4 and 5 GHz) patch type antenna's designed for different coverage distances. The 3 most popular are below.

Figure 3-14 Cisco Directional Antenna's for High Density applications

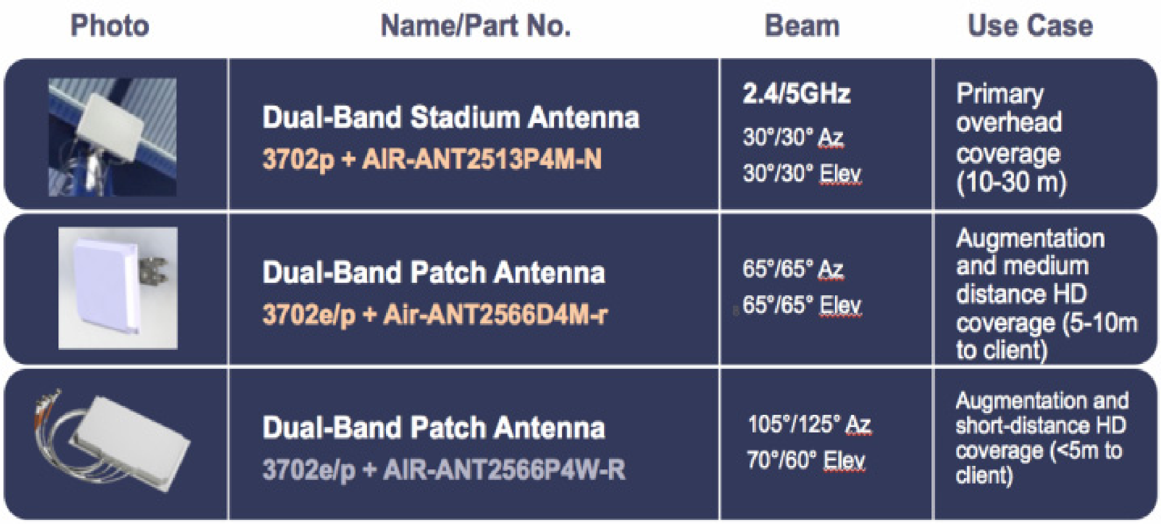
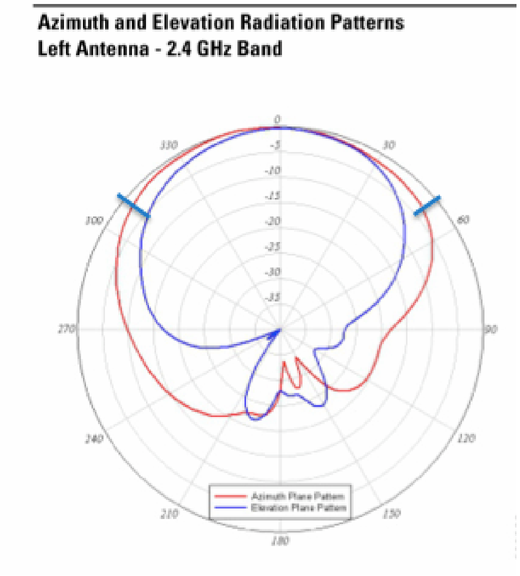


Photo	Name/Part No.	Beam	Use Case
	Dual-Band Stadium Antenna 3702p + AIR-ANT2513P4M-N	2.4/5GHz 30°/30° Az 30°/30° Elev	Primary overhead coverage (10-30 m)
	Dual-Band Patch Antenna 3702e/p + Air-ANT2566D4M-r	65°/65° Az 65°/65° Elev	Augmentation and medium distance HD coverage (5-10m to client)
	Dual-Band Patch Antenna 3702e/p + AIR-ANT2566P4W-R	105°/125° Az 70°/60° Elev	Augmentation and short-distance HD coverage (<5m to client)

Each antenna is designed for a specific purpose in mind. One of the things about antenna selection that must be considered is the Beamwidth. Beamwidth describes coverage area of an antenna, however it does not describe how hard or soft the edge of that coverage is. For that you need to look at the antenna’s pattern in a plot.

The plot below is from one antenna of the AIR-ANT2566D4M-R antenna, it is designed to provide good coverage over a general area. The beamwidth of this antenna at 2.4 GHz 105° x 70° and describes the point where the peak gain of the antenna falls by 3 dB. What’s important in a directional antenna is what happens after that 3 dB. Note the blue marks on the antenna plot below at the rated beamwidth, the gain falls sharply after the rated beamwidth. This is exactly what needs to happen to put more AP’s closer together for higher capacity.

Figure 3-15 Antenna Plot for AIR-ANT2566D4M-R antenna



If the antenna can not hear, it may not interfere with your AP. We only have 3 channels in 2.4 GHz; channel re-use in a dense deployment is already a problem there. With a good antenna, you can make the cell size smaller and get more radios closer together and provide adequate capacity in your design for 2.4 GHz users. 5 GHz has more channels, however with 20/40/80 MHz Channel widths, we are using channels up faster, and cell isolation is becoming more of a problem.

Other problems that can be solved using directional antennas include high interference environments – a shopping mall for instance – most of the stores in a shopping mall will have installed some kind of Wi-Fi, and this creates interference for your Wi-Fi. Using directional antennas, you can isolate your store from the neighbors by focusing the ears of the AP inward, and making the receive sensitivity less behind the antenna. The front to Back ratio of an antenna is responsible for this – think of it like cupping your hands over your ears to hear a distant sound – when you do this you focus the sound energy into your ears, but you also shield your ears to the surrounding noise and this produces a better Signal to Noise ratio – you experience it as better more intelligible sound. Putting a directional antenna on your AP will focus it's ears and it will experience a better sound with less noise as well.

RF Deployment Best Practices

Some design considerations can be addressed by general best practice guidelines. The following applies to most situations:

- We recommend, for a given AP the number of users per AP be:
  - 30 to 50 for data-only users
  - 10 to 20 voice users

This number should be used as a guideline and can vary depending on the AP model, handset or application in use. Check your handset/application requirements

- The AP data rates should be limited to those designed and for which the site survey was performed. Enabling lower data rates can cause increases in co-channel interference and greater throughput variations for clients. A common minimum data rate to start with is 12 Mbps.

- The number of APs depends on coverage and throughput requirements, which can vary. For example, the Cisco Systems internal information systems (IS) group currently uses one AP per 3000 square feet of floor space.

Radio Resource Management - RRM

Cisco RRM, Radio Resource Management has been around for a long time now. What most people are not aware of is that RRM’s collection of algorithms has seen updates with every release of code since 4.1. The rate of change in these algorithms is for a good reason; the questions keep changing and so must the answers. Technology has gone from balancing simple coverage based Wi-Fi networks operating in a single 20 MHz channel to accommodating channel and power solutions for 20, 40, 80, and soon 160 MHz channels all inter-operating in the same spectrum. And in most cases – backward compatibility and a mix of protocols must be considered as well. Even if your organization has standardized – you almost assuredly have neighbors and internal resources that have not.

What RRM Does

RRM consists of four algorithms:

1. RF Grouping
2. DCA (Dynamic Channel Assignment)
3. TPC (Transmit Power Control)
4. CHDM (Coverage Hole Detection and Mitigation)

RRM is a big subject, but it was designed to manage the RF environment in a dynamic way with little to no user intervention. A brief description of the algorithms will be useful in understanding the configuration tasks. RRM’s default settings are generally the best fit initially. In a new controller the Day 0 setup wizard will allow you to fine tune many settings by picking the deployment type that you are working with. Advanced configuration can also be achieved manually

RF Grouping

The RF Grouping Algorithm is responsible for identifying and grouping under an elected or chosen leader – all resources that belong to the same network – WLC’s and AP’s alike. This forms the RF Group and becomes a logical configuration domain. The Network resources are identified by the RF Group Name, which was entered on the initial controller configuration. The group name is shared by all the WLC’s on the same network. AP’s connected to the controllers learn the group name from their controller and in turn broadcast it over the air in NDP messages for other AP’s to hear and report back to their controllers.

Automatic RF Grouping

RF Grouping is automatic by default, and in a multiple controller configuration – any controller belonging to the same RF group will participate in an election process designating 1 or more WLC’s as the RF Group Leader(s). The 2.4 GHz (802.11b,g,n) band and the 5 GHz (802.11a,n,ac) band each must have their own RF Group Leader. Both RF Group Leaders can, but do not have to reside on the same physical controller. Seeing 2 RF Group Leaders – each controlling just one band is not unusual.

Automatic RF Groups must have AP's that can hear one another over the air in order to form. You MUST, connect your AP's to the controllers that you want to form as a group first else each controller will assume that it is it's own RF Group Leader. If your design incorporates a single controller on each site, and the sites are geographically separated each controller will be it's own group leader for both bands at each site.

Static RF Grouping

Static RF Grouping allows user selection of the RF Group Leader(s) and manual assignment of group members. All WLC's must have a wired network path to one another – there is no over the air component so active AP's are not necessary to form a static group but wired connectivity between the controllers is a must. Once the RF Group is created – RRM operates the same using over the air metrics.

RF Group Leader WLC Hierarchy

There are a number of controller models, and some are more capable than others. In both Auto and Static mode, there is a hierarchy applied that prevents a 2500 series controller from becoming the group leader over an 8520 controller. The largest most capable controller should be selected as the group leader.

The RF Group Leader is where all measurements, configurations, and calculations that are being used to manage the RF Group and RRM will be sent and stored. The WLC configuration on the RF Group Leader is the configuration that is used by RRM for the RF Group. It is important to synchronize the RRM configurations on all of your controllers, in automatic RF Grouping mode – the RF Group leader can change for several reasons – and if the configuration is different, then the behavior of the RF Group will change when the leader changes.

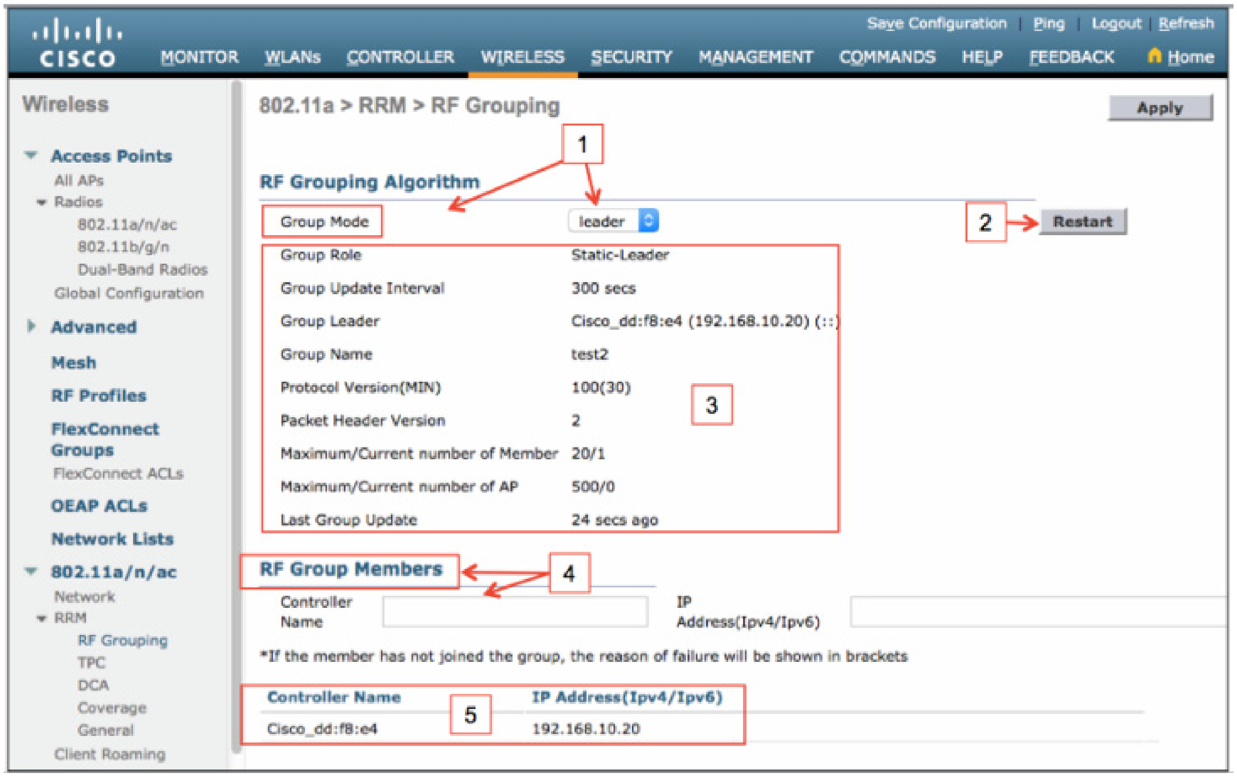
Configurations at the RF Group Leader level are considered Global – as they affect the entire RF Group. RRM allows for RF Profiles; which can be created and applied to individual AP groups that span multiple controllers and override the global configurations to allow localization for a different RF environment. A High Client Density vs. a Coverage model design will require different Data Rates and TPC thresholds at a minimum to function properly. RF Profiles can be applied to AP Groups (collections of AP's in different coverage models for instance) and a separate configuration can be applied to each.

For more information on the specifics of RRM's RF Grouping Algorithm see - RRM RF Grouping Algorithm which covers grouping mechanisms, as well as over the air measurement activities and intervals.

RF Grouping Configuration

On the WLC GUI, Navigate to the Wireless, 802.11a/n/ac or 802.11b/g/n, RRM, RF Grouping

Figure 3-16 *RRM RF Grouping UI configuration*



802.11a > RRM > RF Grouping

RF Grouping Algorithm

Group Mode	leader
Group Role	Static-Leader
Group Update Interval	300 secs
Group Leader	Cisco_dd:f8:e4 (192.168.10.20) (::)
Group Name	test2
Protocol Version(MIN)	100(30)
Packet Header Version	2
Maximum/Current number of Member	20/1
Maximum/Current number of AP	500/0
Last Group Update	24 secs ago

RF Group Members

Controller Name

IP Address(Ipv4/Ipv6)

*If the member has not joined the group, the reason of failure will be shown in brackets

Controller Name	IP Address(Ipv4/Ipv6)
Cisco_dd:f8:e4	192.168.10.20

1. Group Mode—The default mode for the RF Grouping algorithm is AUTO this should be fine for most installations Use the Static mode – by selecting Leader and adding member WLC’s if you have many controllers operating in a shared RF domain. If you are selecting Static, there is a practical limit to the number of AP’s that can be configured within an RF Group. For all controllers up to the 5500 series this is 2x the licensed AP count, for 75xx and 85xx the limit is 6000 AP’s. Design your RF Grouping to keep groups of AP’s and controllers together for like spaces and buildings. Whats important to the RF group is AP’s that can hear one another and need to be configured together should be in the same RF Group and managed by the same RF Group Leader. Create a new RF Group for geographically separated facilities.
2. Restart—after changing the mode – and applying the changes – the restart button –“restarts” the grouping algorithm
3. Information—informs the user of the status for the viewed controller on current mode, the current RF Group Leader, the protocol version (important as not all version will play together – see Cisco Wireless Solutions Software Compatibility Matrix IRCM section, the algorithms interval, current AP and member controller counts.
4. RF Group Member—used for adding member controllers to a Static leader
5. List of current members and status—full list of member status messages can be found in - RRM RF Grouping Algorithm

DCA – Dynamic Channel Assignment

Dynamic Channel Assignment is responsible for monitoring the spectrum, and choosing the best channel plan to place the AP's on. Interference is the primary concern, the less interference there is the more bandwidth (airtime) we can use. To do this DCA monitors four parameters

- Signal—any Wi-Fi signal created by my network/RF Group
- Noise—any RF signal that is not identified as Wi-Fi; this includes collisions and packets to low to be demodulated as well.
- Interference—any Wi-Fi signal that is from Rogue devices or devices not part of my RF Group
- Load—The relative channel utilization of AP's in the RF Group

The user has control of how to prioritize the above metrics in DCA configuration, all 4 are always used but weighting in the calculation can be adjusted. DCA will grade each channel based on the 4 factors above as observed by each individual AP and make a determination on the best channel for that AP to operate on in it's environment.

DCA selections include Channel Bandwidth, for 802.11n and 802.11ac AP's this selects the operating channel width that will be configured, 20/40/80 MHz selections may be made. Unless you are certain of your operating environment and design, current best practice is 40 MHz (2 x 20 MHz channels) operations in most enterprise locations. Using 80 MHz channels consumes 4 x 20 MHz channels for each channel and can introduce unwanted interference in the infrastructure unless you have designed for this specifically.

DCA knows the regulatory for every connected AP, and can manage multiple countries and domains without fear of violating local rules. DCA also monitors all DFS channels for Radar; it manages the channels that are available and selects alternate channels if Radar is detected. Decisions for every AP in the RF Group are made at the RF Group Leader level, and sent back to the local controller for configuration to the associated AP.

Channel Changes can be disruptive on an active network, for that reason DCA has two main operating modes.

- Steady State—Normal
- Startup Mode—Aggressive

Under normal operation – we assume a good initial channel plan after startup has run (see Startup Mode below for more information). DCA then dampens channel changes slightly by applying a hysteresis for operational steady state. This hysteresis determines just how much better a channel must be before allowing the AP to switch to that channel. The Hysteresis is user selectable; the default is medium and is generally adequate. Wi-Fi is bursty in nature and RF conditions can and do change frequently, though mostly for short durations. Channel changes based on short duration bursts will result in frequent and disruptive channel changes; DCA manages whole network channel plans based on trends. Basing network wide changes on isolated or short peak events tends to create problems for clients. RRM does remain sensitive to serious issues and can manage very quick changes for emergencies. See EDRRM in DCA configuration below for the notable exceptions to this rule.

Startup Mode assumes no hysteresis; it is intended for aggressively selecting an initial channel plan and spreading out the radios coverage in the selected spectrum.

This is important to remember when you are making changes to your network such as–

- Adding additional radios
- Changing channel width assignments (adding 802.11n or 802.11ac radios)
- Removing Radios from service

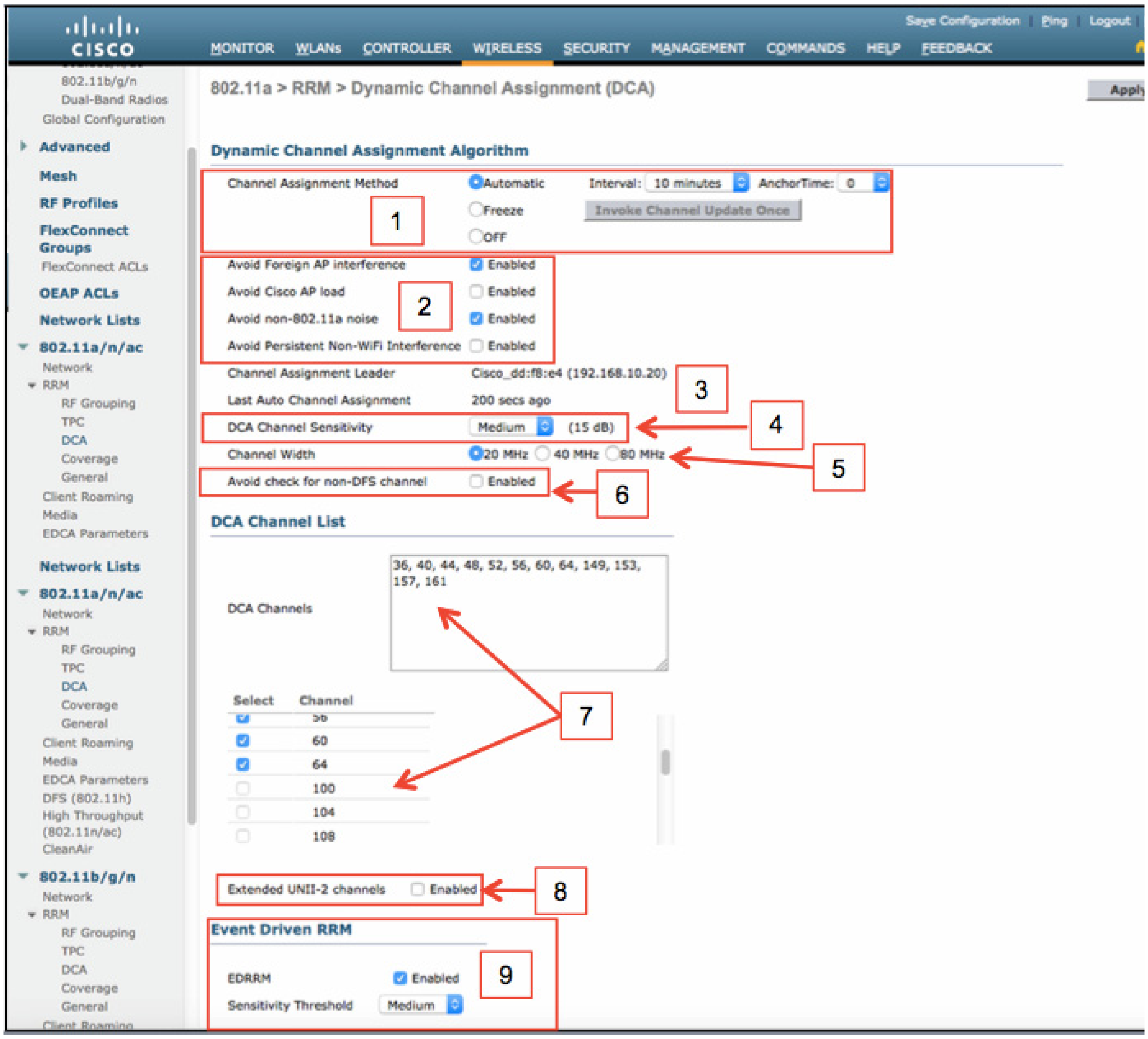
All of these things represent a major change to the operating environment, and invoking startup mode will ensure the best solution to the new question. RRM will adjust for these under normal conditions but it will do so with the Hysteresis applied and may not result in the most optimal answer for the new operating environment.

The default DCA settings are quite adequate; a majority of networks are running with these settings today. Changes to the defaults should be understood and implemented only to solve issues.

DCA Configuration

Default settings for DCA are shown below. The defaults should be adequate for most installations, exceptions will be noted below. The DCA configuration screen is displayed below – 5 GHz is shown here for example, the notable differences from the 2.4 GHz screen is the channel width selection (4) below. We do not support Bonded channels in 2.4 GHz as there are not enough channels or spectrum for this to be practical in a multi AP installation.

Figure 3-17 DCA Configuration at 5 GHz



802.11a > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

Channel Assignment Method ● Automatic ○ Freeze ○ OFF Interval: 10 minutes AnchorTime: 0

Avoid Foreign AP interference ☑ Enabled

Avoid Cisco AP load ☐ Enabled

Avoid non-802.11a noise ☑ Enabled

Avoid Persistent Non-WiFi Interference ☐ Enabled

Channel Assignment Leader Cisco_dd:f8:e4 (192.168.10.20)

Last Auto Channel Assignment 200 secs ago

DCA Channel Sensitivity Medium (15 dB)

Channel Width ● 20 MHz ○ 40 MHz ○ 80 MHz

Avoid check for non-DFS channel ☐ Enabled

DCA Channel List

DCA Channels 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

Select	Channel
☑	56
☑	60
☑	64
☐	100
☐	104
☐	108

Extended UNII-2 channels ☐ Enabled

Event Driven RRM

EDRRM ☑ Enabled

Sensitivity Threshold Medium

DCA Configuration elements:

1. Change Assignment Method - controls how and if DCA runs, Automatic is the default setting.

- Automatic—DCA runs every 10 minutes (600 seconds)
  - The DCA Interval may be changed using a range of 10 minutes to 24 hours, and an anchor time may be selected. Selected Anchor times are 0-23 representing a 24 hour clock – setting the anchor time of 3 (3 AM) with an interval of 4 will run DCA every 4 hours beginning at 3 AM.
- Freeze—After a DCA run is completed, the channel plan is frozen, DCA continues to run but makes no changes. Depressing the Invoke Channel Update Once button – does exactly that – and will run channel changes in conjunction with the NEXT scheduled DCA run – this overrides the Freeze on demand – for one cycle and permits channel changes for that cycle only.
- Off—Turns the DCA function Off (not recommended – see below)

2. These selections allow for tuning of what and how DCA makes decisions

- Avoid Foreign AP interference—Default is selected, this counts neighbor rogue AP's and encourages DCA to work around them. If you are in a congested area, it may be better to disable this contribution. In a congested neighbor environment this can initiate a lot of channel changes – try the default first though.
- Avoid Cisco AP Load—The default is Disabled. This measures Load only on Your (Cisco) AP's. This contribution makes DCA more sensitive to conditions and encourages MORE channel changes. In practice, Client experience is better riding through transient load peaks.
- Avoid Non-802.11 Noise—The default is selected – This prioritizes Noise contribution which is defined as any signal that can not be demodulated as 802.11, this includes a lot of noise which is unintelligible 802.11 due to collisions, or simply being to low for proper demodulation. This should always be selected.
- Avoid Persistent Non-WiFi Interference—The default is Disabled, if you have CleanAir AP's, this selection allows for contribution of Non-Wi-Fi persistent signals such as Microwave Ovens, Outdoor Bridges, Video Surveillance Cameras and should be selected. When CleanAir discovers such a device, it allows for the addition of a Bias to the affected channel for the detecting AP to encourage a better channel selection – even if the device is not active at the moment. Microwave oven's operate heavily during the lunch hour and again late afternoon – this makes RRM remember and avoid the impacted channels on devices that can hear the interference full time for 7 days and expires if no other detections have been made in that time.

3. Channel Assignment Leader – identifies the group leader mac and IP address of the Group leader for this band, Last Auto Channel Assignment tells you in seconds how long ago DCA ran.
4. DCA Channel Sensitivity – The default is Medium. This setting determines the Hysteresis used to make a channel change decision. DCA compares the score of the current channel against all other possible channels – and will change to a better channel IF it meets or exceeds this metric. Medium is 10 dB better in 2.4 GHz and 15 dB better in 5 GHz. Low= 5 dB (more aggressive) and High=20 dB (less aggressive) for both bands. This determines how Much better a channel must be in order to change.
5. Channel Width – The Default is 20 MHz This selects the Global Channel Width, selections can also be overridden at the RF profile, or individual radio level. This only affects 802.11n and 802.11ac capable AP's, a selection of 80 MHz will set 802.11n Radios to 40 MHz
6. Avoid Check for non-DFS channels – The default is disabled. DFS requires that there be at least one non-DFS channel available in the DCA channel list. If you are deploying Outdoor AP's in ETSI regulatory – there are no non DFS channels available for outdoor – selecting this prevents the enforcement of requiring a NON-DFS channel.
7. DCA Channel List – the top part shows you what channels are currently configured, the list allows you to select and deselect channels. Adding or deleting channels requires that the band (2.4 or 5 GHz) be disabled before making changes.
8. Extended UNii2 channels- the default for this is disabled, enabling will add channels 100-144 automatically to the DCA channel List. This is a best practice today – especially for 802.11n/802.11ac 40/80 MHz channel selection.
9. Event Driven RRM – EDRRM is enabled by default – best practice is to enable. EDRRM allows RRM to work with CleanAir Air Quality (AQ) and permits a CleanAir AP that experiencing a classified catastrophic interference to mitigate it by changing channels. What do we mean by catastrophic? In the event a non Wi-Fi interference source broadcasts at 100% duty cycle, it will completely block the channel for that AP, neither clients or AP will be able to speak because they listen before they talk – and every time they listen, they will hear energy. The decision is made on the AP and independent of DCA (this happens within 30 seconds). RRM will know of this change and prevent the AP from changing back for a period of 1 hour. There are 4 sensitivity thresholds

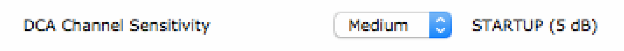
Table 3-5 ED-RRM AQ Event Threshold Mapping

Low	AQ=35
Medium	AQ=50 (default)
High	AQ=60
Custom	User Threshold - be careful here

1. For new installations – ensure that ALL of your AP's are mounted and associated with the controller before restarting the controller or initiating DCA reset

- DCA can be restarted and initialized at the command line with the command config 802.11a/b channel global restart - to verify operation check the DCA config page in the GUI under wireless=>802.11a/b=>RRM=>DCA will display Startup.

Figure 3-18 DCA



DCA Channel Sensitivity Medium STARTUP (5 dB)

2. Re- initialize DCA any time there is a major change to the requirements of the channel plan

- Change in channel bandwidth (20/40/80)
- Adding additional AP's
- Changing DCA channels (adding or subtracting UNII2e channels for instance)

3. Default options are best, with the exception of "Avoid Foreign AP Interference" which may be unchecked if your installation has a lot of rogue neighbors and channel changes happen daily for this reason.

TPC – Transmit Power Control

The other component critical in Wi-Fi is the transmit power of the Radios in the AP. TPC uses over the air messages to hear and measure every AP in the RF Group. By keeping track of how each AP hears other AP's and how other AP's hear our own AP we can adjust the power dynamically to provide the best coverage (cell size) without causing interference to our neighbors. The TPC calculation keeps track of regulatory requirements like Maximum Power as this changes in most regulatory region depending on which channel and band you are using. There are two different methods for TPC calculation presently with TPCv1 being the default and TPCv2 as an alternative for higher density deployment coverage.

Since TPC relies on measurements over the air between AP's to calculate the optimal power levels, it really does not know how the client at the floor level will hear it. For that reason there is a range of coverage levels than can be selected within the algorithm to tune the environment the value is a dBm value that you want at the edge of the cell you are configuring and allows for tuning to different AP placements and mounting solutions. For instance, in a high ceiling environment the AP's may be located 60 feet (18 meters) apart, with the floor being 25 feet (8 meters) below, in this case the default value of -70 may be inadequate to allow for sufficient power and coverage at the floor level and a value of -60 will.

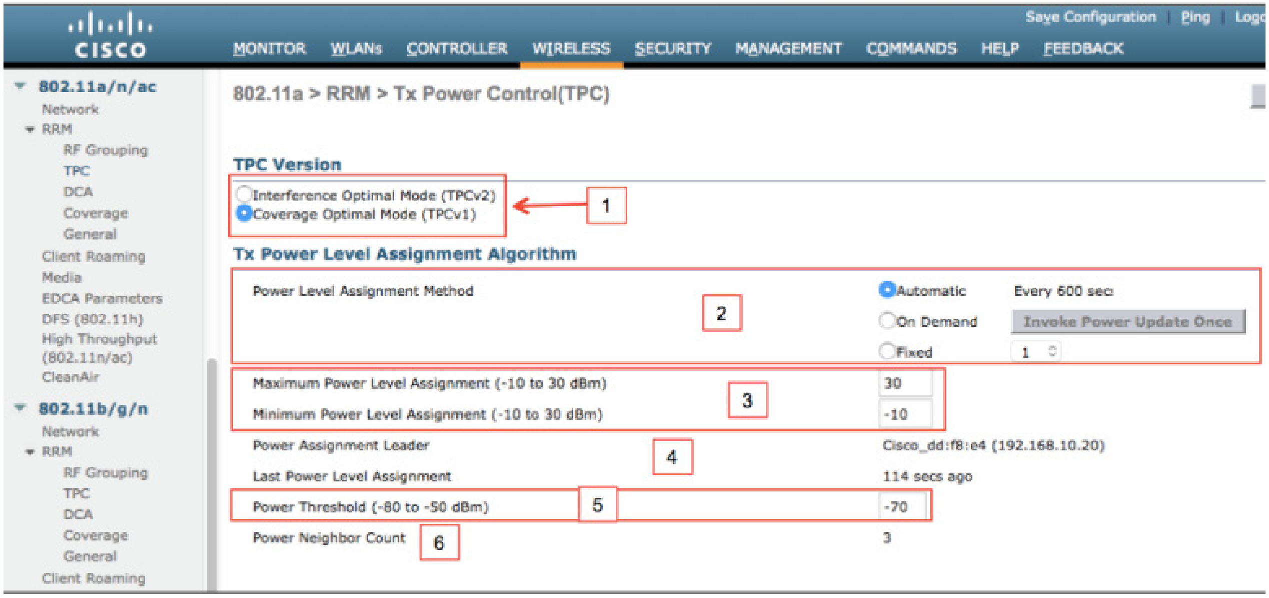
TPC also has overrides that can be applied through RF Profiles or at the global level for a whole WLC that allow the administrator to designate a minimum and maximum power level that the AP's will not exceed. This is useful for tuning in High Client Density environments and can correct for poor AP placement options as well.

We will cover more on how to tune TPC for optimal coverage in the best practices below.

TPC Configuration

The default selections for TPC should be adequate for a normal enterprise office environment. The default TPC user threshold assumes a 10 ft (3 meter) ceiling height.

Figure 3-19 TPC Configuration UI



802.11a > RRM > Tx Power Control(TPC)

TPC Version

○ Interference Optimal Mode (TPCv2)
● Coverage Optimal Mode (TPCv1)

Tx Power Level Assignment Algorithm

Power Level Assignment Method	● Automatic	Every 600 secs
	○ On Demand	Invoke Power Update Once
	○ Fixed	1
Maximum Power Level Assignment (-10 to 30 dBm)	30	
Minimum Power Level Assignment (-10 to 30 dBm)	-10	
Power Assignment Leader	Cisco_dd:f8:e4 (192.168.10.20)	
Last Power Level Assignment	114 secs ago	
Power Threshold (-80 to -50 dBm)	-70	
Power Neighbor Count	3	

1. Choose TPC Version – TPC v1 is the default selection. TPCv2 can be used for higher density designs and coupled with channel mode will yield better capacity if AP's are closer together with less reduction in power. Installations where AP cell size is 3K sq feet and under in large open areas should consider this – coupled with the command line argument "channel mode". This limits TPCv2 functionality to only looking at neighbors on the same channel. Only one version may be selected as this is a global command affecting the entire RF group. If this is selected on a member controller – it will have no effect on the RF group unless that controller becomes the Group Leader.
2. Power Level Assignment Algorithm

- Automatic—Default and runs at 600 second (10 minute) intervals.
- On Demand—Will only run on the next scheduled interval (600 seconds) if Invoke Power Update is depressed. Power levels are frozen unless the Invoke command is received but TPC continues to run in the background.
- Fixed—Allows a manual power level to be assigned to all AP's; this is not recommended for several reasons.
  - All AP's will be on the Selected Power Level indication; however depending on the 5 GHz channel assignment, may have very different power output in dBm. See Reference Guides under Access points and refer to Channels and Maximum Power for your model under documentation.
  - This excludes all AP's from the TPC algorithm.

3. Min/Maximum power level assignment—Default is “Disabled” (note that values of -10 and 30 dBm are not supported on ANY Cisco AP). This is a per controller override – and allows setting a minimum and maximum power level that will be allowed on ALL AP’s attached to that controller. If TPC attempts to apply a setting higher or lower than the local controllers Min/Max, it is overridden by this setting. See above for Channels and Maximum power as the entry is in dBm and will produce the closest max or minimum power to an actual allowed power on the AP being applied to. This setting can also be made at the RF Profile level and applied to a select AP group – this is recommended for larger deployments containing multiple coverage and capacity zones.
4. Power level assignment leader – identifies the active RF Group leader for the band. Last power level assignment shows seconds since last assignment was made.
5. Power Threshold (-80 to -50 dBm) – This tells the TPC algorithm the value you want for the cell edge. TPC uses this the threshold value for neighbors in the calculation to determine the optimal power level of the AP’s.

- TPCv1—The default is -70 dBm and assumes a normal office space with 10 foot ceilings, if your application has High Ceilings – 15-20+ feet you may need to adjust this threshold up to receive adequate power at the floor. The measurement is made using NDP packets between AP’s. If the AP’s have all been placed in a hallway, this can negatively affect coverage in rooms on either side of the hallway – measurements should be taken – mitigation may require different placement of the AP’s.
- TPCv2—The default is -65 dBm.

6. Power Neighbor Count – Display only – three neighboring AP’s are required for TPC to work properly. This means that three AP’s must Logically see each others as neighbors – as they should if in close proximity to one another. If this is not the case, a power level will be chosen based on the nearest neighbors settings for consistency. This condition can affect AP’s that are at the very edge of a covered area.

CHDM- Coverage Hole Detection and Mitigation

CHD measures the client. The goal for the rest of RRM is to produce the best coverage possible, CHD monitors the clients associated to each AP to determine if the client is receiving adequate coverage based on the AP’s measurement of the client RSSI. This assumes that the client is not willfully maintaining a connection to an AP when there is a closer AP available. Clients alone decide when to roam, and there is the phenomenon of a “sticky” client. CHD monitors for those as well by looking at all AP’s that can hear the client, if the client should and could be on a better AP, it is marked as a false positive event. If a client is not sticky, and it’s RSSI is falling below the threshold of coverage, we will alert and report on the clients location and the AP it was associated with.

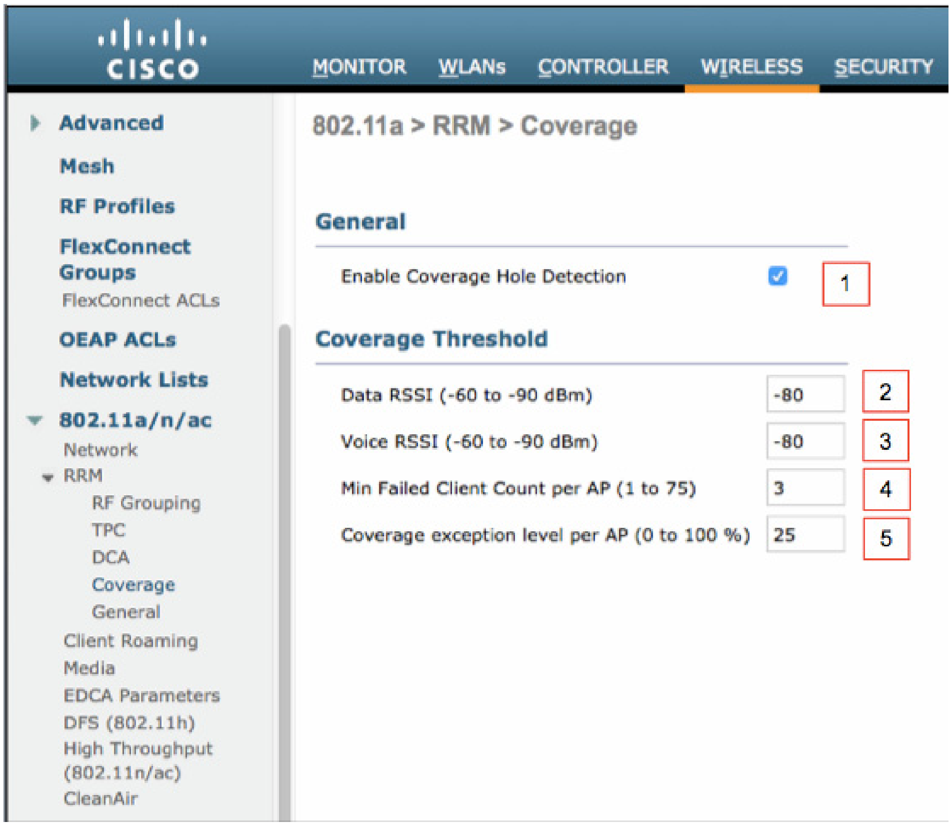
In the early days, CHD also has a mitigation component that would increase the power output of the AP it is associated too to mitigate the coverage problem. This functionality is still in the algorithm, however it is heavily weighted to ensure that is a good decision. These days, we take a more direct approach using a feature called Optimized Roaming which takes it’s direction from CHD derived metrics and for sticky clients actively intervenes by sending a Dis-associate to encourage the client to roam to a better AP.

Sticky clients operate at lower data rates generally and can drag down the performance of an entire cell. CHD monitors the client RSSI as well as SNR, and even the data rate to ensure that we understand how the network is perceived by the associated clients. The default configurations are generally sufficient, optimized Roaming is a separate configuration and will also be covered in Best Practices below.

Coverage Hole Detection and Mitigation (CHDM)

Coverage Hole Detection monitors the Client RSSI on the associated AP.

Figure 3-20 Coverage Hole Detection Configuration UI



802.11a > RRM > Coverage

General

Enable Coverage Hole Detection ☑

Coverage Threshold

Data RSSI (-60 to -90 dBm) -80

Voice RSSI (-60 to -90 dBm) -80

Min Failed Client Count per AP (1 to 75) 3

Coverage exception level per AP (0 to 100 %) 25

1. Enable/Disable Coverage Hole Detection—The default is enabled. This can be overridden on individual WLAN's as well as in RF Profiles.
2. Data RSSI threshold—The default is -80 dBm
3. Voice RSSI Threshold—The default is -80 dBm
4. Minimum Failed Client Count per AP—The default is 3. This determines how many clients must exceed either the voice or the data threshold from above in order for a Coverage Hole to be alerted, this also works in conjunction with the Coverage Exception Level below.
5. Coverage Exception Level per AP – this setting determines what percentage of total clients on a given AP need to exceed the threshold to declare a coverage hole and woks in conjunction with minimum Failed Clients from above.

Coverage Hole detection and Mitigation is highly tunable with the exception of the thresholds, the default settings are generally sufficient. Minimum client count and coverage exception work together and the default count of 3 clients with a coverage exception of 25% says for example that if 3 clients are below the threshold – in order to act there must be 12 clients currently associated (3=25% of 12). CHDM also listens for clients on every AP in order to determine if a failed client is really in a coverage whole, or if it is simply not roaming. In the event that we can hear a client from an AP better than the one it is currently associated too, this will be counted as a false positive and not count towards a coverage hole event. If both conditions are met, Coverage Hole Mitigation can increase the AP's power by one power level to attempt to fix the coverage. RRM will then re-evaluate coverage requirements on the next DCA and TPC run.

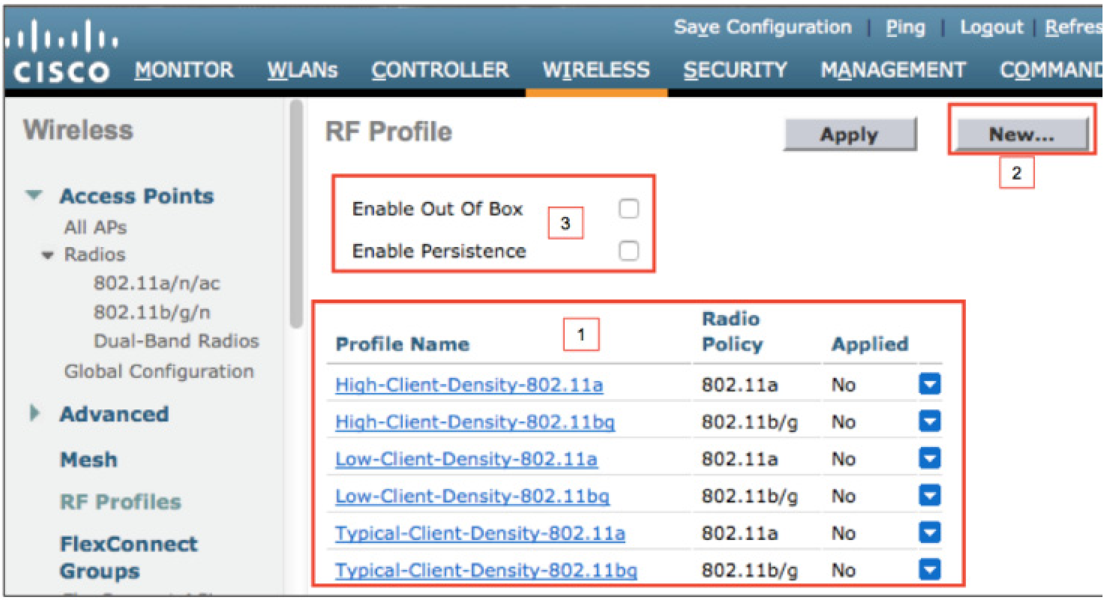
RF Profiles

RRM at the Global Level set's configuration parameters that apply to every AP associated with the RF Group. Back when Wireless LAN Controllers had relatively low maximum numbers of AP's (e.g.,100), that was fine. Things change, and not only have AP limits jumped up so have users consumption of network resources. Different use cases like High Client Density or Capacity model vs. Coverage models require different optimizations to be efficient and meet design goals. In High Density, we are asking to optimize users experience when close to a lot of AP's – at minimal distances. For Coverage we are optimizing for maximum cell coverage and reliable connection at distance from the AP in thin coverage.

RF Profiles allows for modifications to be applied to select groups of AP's contained in the same AP Group. You can configure an RF Profile for each radio on the AP, 2 RF Profiles per AP Group may be applied. The classic use case for this is a lecture hall or large theater where a high Capacity design is required to manage a high client density. Surrounding this theater however are hallways and open areas where coverage is the bigger concern. A single global RRM setting for all of these AP's will result in a configuration that is likely not optimized for either environment. Placing the AP's inside the theater in one AP group (perhaps grouped with AP's from other High Client density locations) and the AP's in the coverage areas like hallways and open areas in another AP group. Now you can configure RF Profiles that optimize the required configurations to the intended design.

RF Profiles allow control over many functions beyond RRM's algorithms; many of the HDX features can also be customized for a specific group. On the controller's Wireless menu – select /Wireless/Advanced/RF Profiles:

Figure 3-21 Pre-configured RF Profiles



Enable Out Of Box ☐

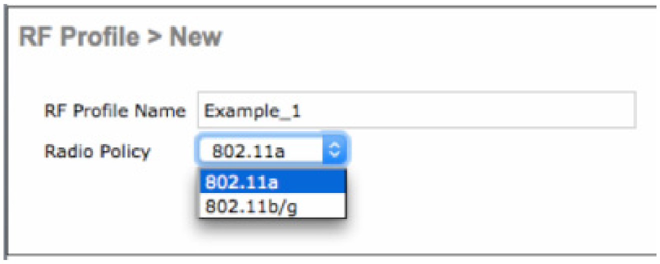
Enable Persistence ☐

Profile Name	Radio Policy	Applied
High-Client-Density-802.11a	802.11a	No
High-Client-Density-802.11bg	802.11b/g	No
Low-Client-Density-802.11a	802.11a	No
Low-Client-Density-802.11bg	802.11b/g	No
Typical-Client-Density-802.11a	802.11a	No
Typical-Client-Density-802.11bg	802.11b/g	No

1. Example pre-built RF Profiles
2. New—To create a custom RF Profile
3. Enable Out of box—To place any new AP's into the Out of Box AP group; which has the radios disabled. Persistent is checked if you want Out of Box (OOB) to remain in effect across re-boots of the controller.

We'll cover the configuration options contained in an RF Profile first. Then we'll cover the intended use and configurations for the example profiles. In order to create a new RF Profile, go to **Wireless** > **RF Profiles** and select "**New…**" (Fig. 19 bullet 2) and open the New RF Profile dialogue.

Figure 3-22 New RF profile dialogue



RF Profile > New

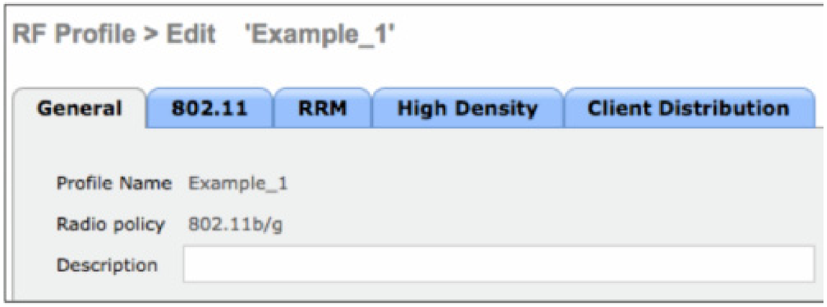
RF Profile Name Example_1

Radio Policy 802.11a

We will cover the configuration options contained in an RF Profile first. Then we will cover the intended use and configurations for the example profiles. In order to create a new RF Profile, go to **Wireless** > **RF Profiles** and select "**New…**" (Fig. 19 bullet 2) and open the New RF Profile dialogue.

RF Profile - General

Figure 3-23 RF Profile General Tab



RF Profile > Edit 'Example_1'

Profile Name Example_1

Radio policy 802.11b/g

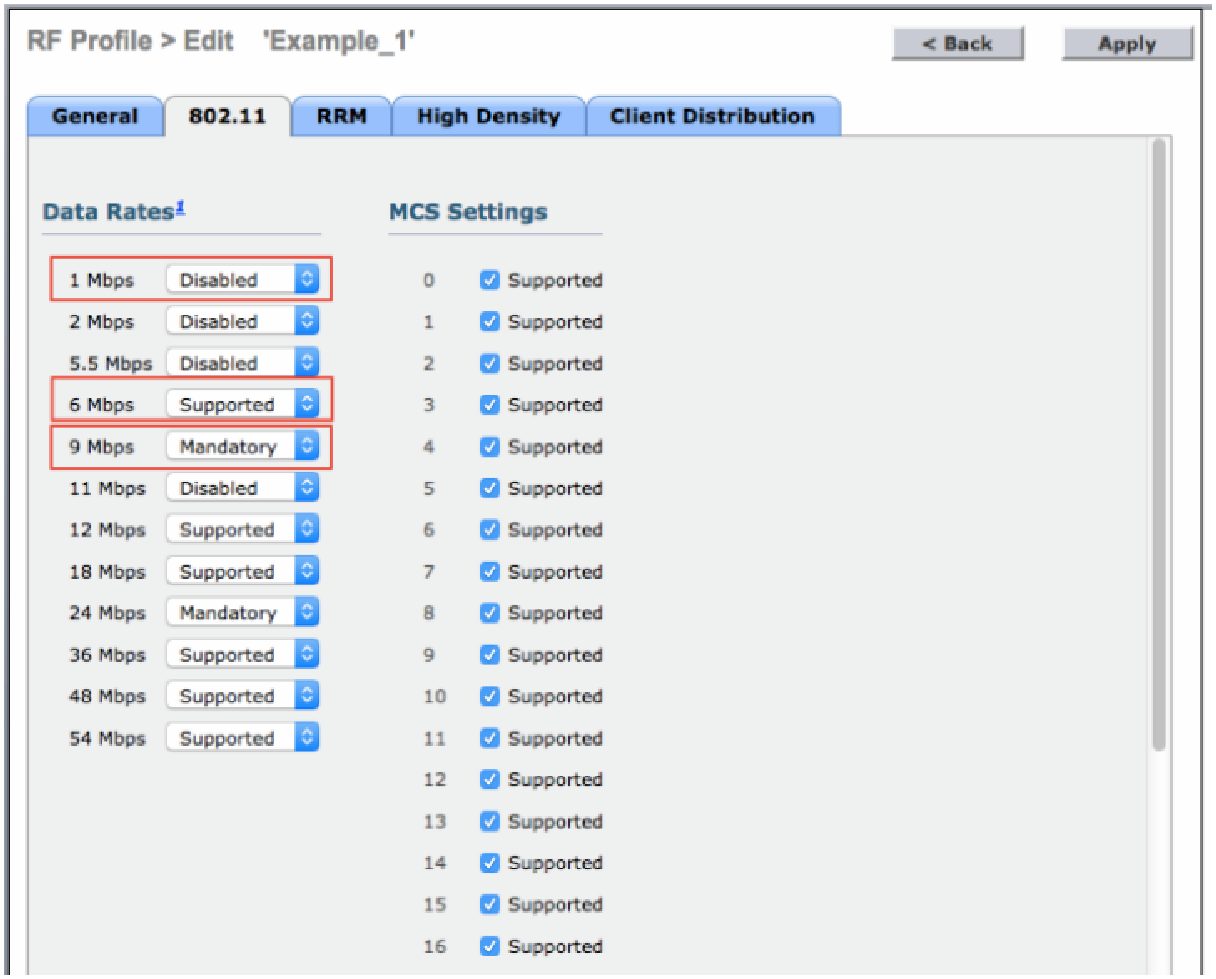
Description

On the general tab – you can enter a short description regarding the use of this profile; you have 64 characters max. The general Tab Identifies what band the profile is created for and the RF Profile name – neither of these can be edited after creation. If a mistake was made on the name during creation, you need to delete the profile and re-create with the correct name.

RF Profile - 802.11

The 802.11 tab gives you control over the network settings which are controller specific not global. These settings in RF Profiles override the controller Global configuration for the AP group it is applied to

Figure 3-24 RF Profile 802.11 tab



RF Profile > Edit 'Example_1'

Data Rates[1]

1 Mbps	Disabled
2 Mbps	Disabled
5.5 Mbps	Disabled
6 Mbps	Supported
9 Mbps	Mandatory
11 Mbps	Disabled
12 Mbps	Supported
18 Mbps	Supported
24 Mbps	Mandatory
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

MCS Settings

0	☑ Supported
1	☑ Supported
2	☑ Supported
3	☑ Supported
4	☑ Supported
5	☑ Supported
6	☑ Supported
7	☑ Supported
8	☑ Supported
9	☑ Supported
10	☑ Supported
11	☑ Supported
12	☑ Supported
13	☑ Supported
14	☑ Supported
15	☑ Supported
16	☑ Supported

The 802.11 tab allows selection of data rates and their mode. On a Cisco AP a data rate can be in one of 3 states

1. Disabled—not allowed by the AP
2. Supported—allowed but not required by the AP
3. Mandatory—The client must support this data rate

The Minimum (lowest) Mandatory Data Rate (in the example above 9 Mbps) determines the speed at which the beacon and all other subsequent broadcast messages will be sent at. In order for a client to associate with an AP using 9 Mbps as the minimum Mandatory data rate, the client must be able to complete association at 9 Mbps or faster or the client will not be allowed to join the AP. This effectively limits the cell size of the AP to clients close enough to support 9 Mbps. This is a good default value for average installations. In higher client density the value may be 12 Mbps, or in extreme high client density designs where cell sizes are at their minimum you may even select 18,24 or 36 Mbps depending on the design requirements.

The second Highest Mandatory data rate (24 Mbps in the example above) will be the default multicast speed if auto multicast is not set (it is by default)

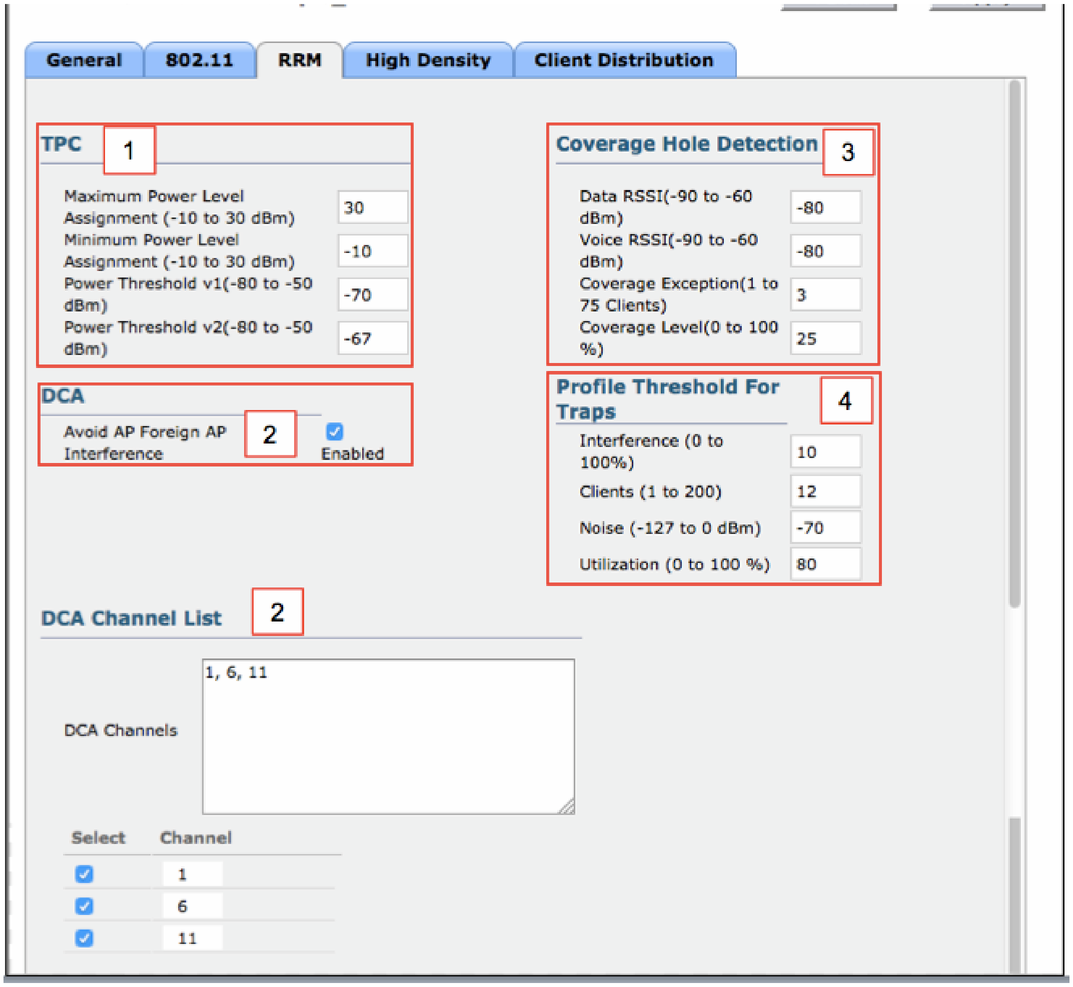
A data rate that is marked as supported, may be used by the client and the AP will honor it.

A data rate that is marked disabled will not be honored by the AP.

MCS data rates can be selected or de-selected only. Deselecting these rates will prevent the AP from using them. All Data rates and selections are broadcast to potential clients in the beacon frame, and your changes here will be reflected in the beacon message.

RF Profile - RRM

Figure 3-25 RF Profiles RRM tab



TPC

Maximum Power Level Assignment (-10 to 30 dBm): 30
Minimum Power Level Assignment (-10 to 30 dBm): -10
Power Threshold v1(-80 to -50 dBm): -70
Power Threshold v2(-80 to -50 dBm): -67

DCA

Avoid AP Foreign AP Interference: ☑ Enabled

Coverage Hole Detection

Data RSSI(-90 to -60 dBm): -80
Voice RSSI(-90 to -60 dBm): -80
Coverage Exception(1 to 75 Clients): 3
Coverage Level(0 to 100 %): 25

Profile Threshold For Traps

Interference (0 to 100%): 10
Clients (1 to 200): 12
Noise (-127 to 0 dBm): -70
Utilization (0 to 100 %): 80

DCA Channel List

DCA Channels: 1, 6, 11

Select	Channel
☑	1
☑	6
☑	11

The RRM tab within an RF Profile allows for overriding the global parameters set at the RF Group Level.

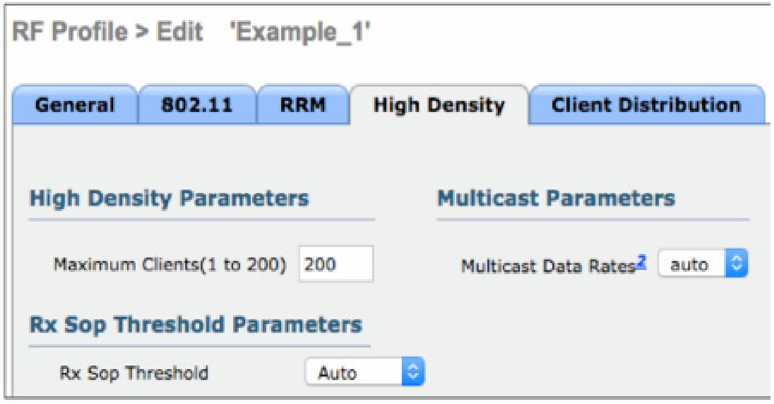
1. TPC, allows for a custom Min/Max power level to be assigned for the entire AP Group, also a custom TPC threshold for either TPCv1 or 2. NOTE: Selection of the TPC version is a global selection only and either the TPCv1 or v2 threshold will be used as appropriate.
2. DCA, while not all the features of DCA are included at the RF Profile level the most important are, for instance avoiding foreign AP interference may well perform better disabled in a rogue rich environment. You can also set custom channel plans using a copy of the DCA channel list. In order for a channel to be available within the RF Profile – it must be selected at the global DCA channel List.

3. Coverage Hole Detection, is replicated completely and applies to all WLAN's assigned to the AP Group, individual WLANs may have coverage hole enabled or disabled on the global configuration per controller.
4. Profile Threshold For Traps, allows setting of other thresholds within the RF profile – for instance in a high client density area – more of everything will be normal – this allows you to make trap alert messages useful for an AP group which otherwise may be set too low.

RF Profile - High Density

The High Density tab allows for optimizing certain HDX features at the RF Profile level on an AP group.

Figure 3-26 RF Profile High Density tab



Maximum Clients(1 to 200) 200

Multicast Data Rates[2] auto

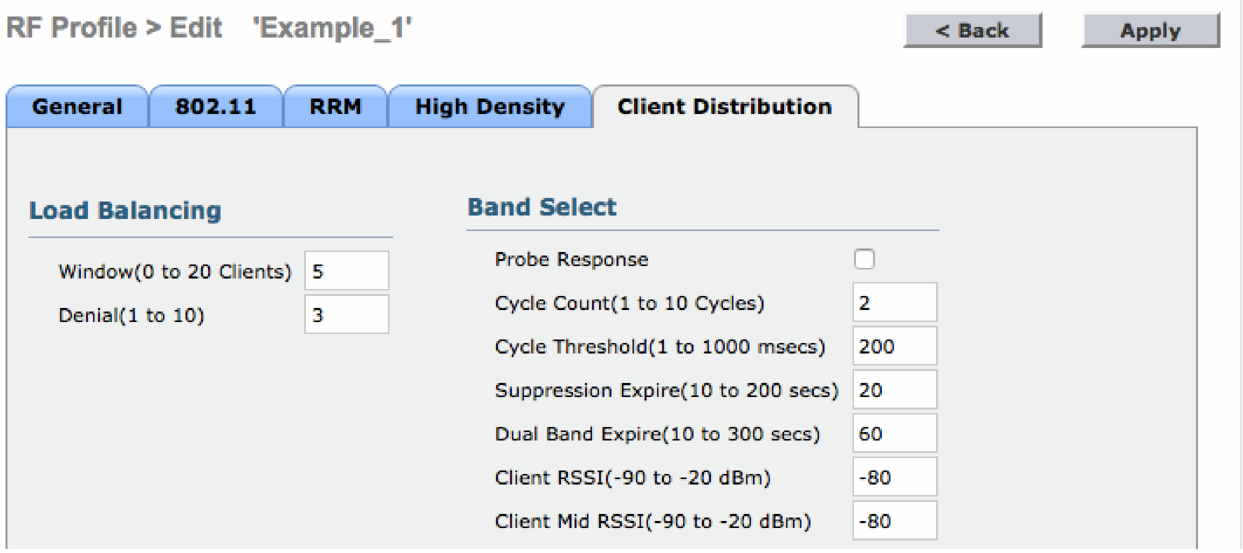
Rx Sop Threshold Auto

- High Density Parameters, allows selection of the maximum number of allowed clients on a radio interface. This selection will simply deny access to any client number over the selected number. The default value is 200. It is recommended to leave this at the default value.
- Rx SOP, allows selection of a RX Start Of Packet Sensitivity threshold – the selections are High, Medium, Low, auto – the default is Auto. A thorough understanding of RX-SOP how it works and the settings is highly advised. RX-SOP changes the receive sensitivity by setting a threshold RSSI that a logical packet must meet in order to be received as Wi-Fi. *See* – High Density Experience Features Release 8.0 for more on RX-SOP settings.
- Multicast Parameters – the default is Auto, or you may select a single dedicated data rate that all multicast packets will use.

RF Profiles – Client Distribution

The Client Distribution tab gives you control over Load Balancing and Band Select options

Figure 3-27 RF Profiles Client Distribution tab



RF Profile > Edit 'Example_1'

Load Balancing

Window(0 to 20 Clients)	5
Denial(1 to 10)	3

Band Select

Probe Response	☐
Cycle Count(1 to 10 Cycles)	2
Cycle Threshold(1 to 1000 msecs)	200
Suppression Expire(10 to 200 secs)	20
Dual Band Expire(10 to 300 secs)	60
Client RSSI(-90 to -20 dBm)	-80
Client Mid RSSI(-90 to -20 dBm)	-80

- Load Balancing, allows setting of a threshold on an AP at which additional clients will be denied with a status code of 17 which states that the AP can not process this request now because it has too many clients, you can select the number of clients 0-20 and the number of denials that will be sent before admission is granted. This is important, as client devices do not universally support status code 17. Load Balancing can be better ensured by the selection of proper data rates and good network design.
- Band Select, 802.11b/2.4 GHz profile only – Selection of the probe response box enables band Select configuration at the RF Profile level and overrides the configuration settings at the global level allowing for more aggressive band Select operation on a selected AP group only.

WLAN Express

With release 8.0 we've included a new day 0/1 startup dialogue that guides the user through questions targeting best practices for Wireless LAN Controller deployment. The configuration dialogue and options are designed to support the Cisco Wireless LAN Controller Configuration Best Practices. The dialogue supports the application of suitable RF settings for low, medium, and high Client/AP density and will apply suitable selections for data rates, and features designed to support higher density environments. While no building or installation is ever the same, generalizations can be applied based on the density of the Access Point deployment and intended number of clients.

In addition to the startup dialogue, there are 3 pre-configured RF profiles contained on the controller that you can use for reference or apply as is. The configuration settings for these are below.

Table 3-6 Pre-configured RF Profiles

	Dependency	**Typical (Enterprise - Default Profile)**	**High Density (Throughput)**	**Low Density (Coverage Open Space)**	**Legacy (if disabled RF opt)**
TPC Threshold	Global per band Specific RF Profile per band	Default	-65 dBm (5GHz) -70 dBm (2.4GHz)	-60 dBm (5GHz) -65 dBm (2.4 GHz)	Default
TPC Min	Global per band Specific RF Profile per band	Default	7 dBm	Default	Default
TPC Max	Global per band Specific RF Profile per band	Default	Default	Default	Default
Rx Sensitivity (rxsop)	Global per band (Advanced Rx Sop) RF profiles	Default	Medium	low	Default
Coverage RSSI Threshold	Global per band data and voice RSSI in (Coverage) RF Profile	Default	Default	Higher	Default
CCA Threshold	Global per band 802.11 a only (hidden) RF Profile	Default	Default	Default	Default
Coverage Client Count	Global Per band (Coverage Exception) RF Profiles (Coverage Hole Detection)	Default	Default	Lower (1-3)	Default
Data Rates	Global per band (network) RF Profiles	12 Mbps mandatory 9 supported 1, 2, 5.5, 6, 11 Mbps disable	12 Mbps mandatory 9 supported 1, 2, 5.5, 6, 11 Mbps disable	CCK rates enable 1, 2, 5.5, 6, 9,11,12 Mbps enable	default
Band Select	Per WLAN basis	Enable	Enabled	Disable	Enable

Table 3-6 Pre-configured RF Profiles (continued)

	Dependency	**Typical (Enterprise - Default Profile)**	**High Density (Throughput)**	**Low Density (Coverage Open Space)**	**Legacy (if disabled RF opt)**
SI ED-RRM PDA	Global per band (Clean Air) Global per band (DCA) Global per band (802.11a/802.11b channel…)	Enable Disable Enable	Enable Disable Enable	Enable Disable Enable	Enable Disable Enable
Load Balancing	Per WLAN basis	Disable	Enabled	Disable	Disable
DCA Sensitivity		Default	High	High	Default
Channel	Global per band (DCA) RF Profiles	Default	Default	Default	Default

High Density

High Density in this context should be thought of as any area where the average cell size is 3000-2000 sq feet (280-185 sq meters) and multiple AP's have been deployed for Capacity reasons. Typical client counts would be 50-100 clients per cell.

AP's spaced at a distance of roughly 60 feet (18 meters) = 3000 sq ft cell size.

AP's spaced at a distance of 50 feet (15 meters) = 2000 sq ft cell size

If you are engineering a specific theater, or lecture hall and increasing capacity to handle a density of 1 user per sq/meter you should follow the design recommendations for minimum data rates and power levels.

Typical Density

Typical density will apply to most every other area of an enterprise installation, or common areas and cube's where active clients are spread out a bit but continuous coverage is provided. The average cell size would be 3000 – 5000 sq feet (280-460 m sq) and the average number of users per cell would be 10-30.

AP's spaced at a distance of 60 feet (18 meters) = 3000 sq ft cell size.

AP's spaced at a distance of 80 feet (24 meters)= 5000 sq ft cell size

Low Density

The low density threshold is provided for very large cells of 5000 sq feet or more. In this profile – all data rates are enabled, and power levels are increased through the TPC threshold to provide coverage over the maximum distance of the cell edge. Lower data rates mean higher airtime utilization per user, so the capacity is limited by airtime in this configuration. This would be a fine configuration for an individual hot spot application or for outdoor coverage of an open field. This is also very close to the default AP configurations if no selection is made.

RF Power Terminology

The terms such as dB, dBi, dBr and dBm are used to describe the amount of change in power measured at points in a system, as perceived by the radio or compared to a reference power level. The following sections cover their differences and provide general rules for their use. Effective isotropic radiated power (EIRP) is also described.

dB

The term dB (decibel) is mainly used to describe attenuation or amplification of the signal level. dB is a logarithmic ratio of a signal to another standardized value. This means that the dB by itself is not a measurement For example, dBm is where the signal level value is being compared to 1 milliwatt of power, and dBW is where the value is being compared to 1 watt of power.

The mathematical equation is:

power (in dB) = 10 * log10 (signal/reference)

Substituting in real numbers (signal 100 mW, reference 1 mW) provides a value in dB of 20 (100 = 10 squared; taking the exponent 2 and multiplying by 10 gives you 20).

Keep in mind that it is logarithmic, meaning that it increases or decreases exponentially and not linearly, and it is a ratio of a given value to a reference. Also keep in mind that every increase of 10 dB represents a multiplication by 10 (for example, 0 dBm = 1 mw, 10 dBm = 10 mw, 20 dBm = 100mW, and 30 dBm = 1000mW (1W).

Given that it is logarithmic, there are general rules to take into consideration. An increase or decrease of 3 dB means that the signal doubled (double the power) or halved, respectively. An increase or decrease of 10 dB means that the signal went up by 10 times or down to 1/10th of the original value.

Indoor and outdoor WLAN deployments each offer separate challenges in RF deployments that need to be analyzed separately. However, there are a few general rules for indoor use. For every increase of 9 dB, the indoor coverage area should double. For every decrease of 9 dB, the indoor coverage area should be cut in half.

dBm

The term dBm (dB milliwatt) uses the same calculation as described in the dB section but has a reference value of 1 mW (0.001 W). Power in Wi-Fi is always below 1 mW.

Taking into consideration the example given above in the dB section, if the power increased from 1 mW to 100 mW at the radio, the power level would increase from 0 dBm to 20 dBm.

Besides describing transmitter power, dBm can also describe receiver sensitivity. Receiver sensitivity is in represented as minus dBm (-dBm) because the relatively low transmit power used in Wi-Fi – received signals are always below 1 mW. The sensitivity indicates the lowest power the receiver can effectively receive before it considers the signal unintelligible.

dBi

The term dBi (dB isotropic) describes the forward gain of a real antenna compared with the hypothetical isotropic antenna. An isotropic antenna (a theoretical or imaginary antenna) is one that sends the same power density perfectly in all directions.

Antennas are compared to this ideal measurement, and all FCC calculations use this measurement (dBi). For example, a Cisco omni-directional AIR-ANT4941 antenna has a gain of 2.2 dBi, meaning that the maximum energy density of the antenna is 2.2 dB greater than an isotropic antenna.

Effective Isotropic Radiated Power (EIRP)

Although transmitted power based on the radio setting is rated in either dBm or milliwatts, the maximum energy density coming from an antenna from a complete system is measured as EIRP, which is a summation of the dB values of the various components. EIRP is the value that regulatory agencies such as the FCC or ETSI use to determine and measure power limits, expressed in terms of maximum energy density within the first Fresnel of the radiating antenna. EIRP is calculated by adding the transmitter power (dBm) to antenna gain (dBi) and subtracting any cable losses (dB). For example, if you have a Cisco Aironet bridge connected to a solid dish antenna by a 50 foot length of coaxial cable, substituting in the numbers gives the following:

- Bridge: 20 dBm
- 50 Foot Cable: -3.3 dBm (negative because of cable loss)
- Dish Antenna: 21 dBi
- EIRP: 37.7 dBm

For more information and fun math *see* the Cisco tech Note: RF Power Values.

Cisco Unified Wireless Network Architecture—Base Security Features

The Cisco Unified Wireless Network solution provides end-to-end security of architecture and product security features to protect wireless local area network (WLAN) endpoints, the WLAN infrastructure, and client communications.

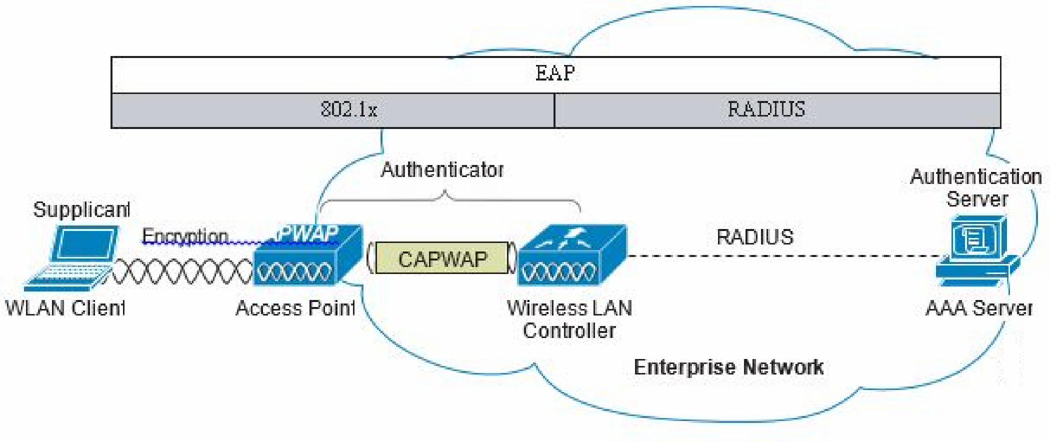
The Cisco Unified Wireless Network solution builds upon the base security features of the IEEE 802.11-2012 standard by enhancing radio frequency (RF) and network-based security features to ensure overall security.

Secure Wireless Topology

Figure 4-1 illustrates a secure wireless topology. The topology is made up of the following components with their basic roles in the 802.1X authentication process.

- WLAN client with 802.1X supplicant (wireless software) on the client.
- Access point (AP) and Wireless LAN Controller (WLC) using the control and provisioning of wireless access points (CAPWAP) protocol.
- RADIUS protocol carrying extensible authentication protocol (EAP) packets between the client and the authentication server.
- Authentication, Authorization, and Accounting (AAA) server as the Authentication Server.

Figure 4-1 Secure Wireless Topology



WLAN Security Mechanisms

Security is implemented using authentication and encryption in the WLAN network. The security mechanisms for WLAN networks are:

- Open Authentication (no encryption)
- Cisco WEP Extensions (Cisco Key Integrity Protocol + Cisco Message Integrity Check)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)
- Cisco Adaptive Wireless Intrusion Prevention System (wIPS) with Enhanced Local Mode (ELM)

Wi-Fi Protected Access (WPA)

The 802.11 WEP standard failed to address the issue of how to manage encryption keys. The encryption mechanism itself was found to be flawed, in that a WEP key could be derived simply by monitoring client traffic. The IEEE 802.11i standard addresses these security issues found in the original 802.11 WEP standard.

WPA and WPA2 are 802.11i-based security solutions as defined by the Wi-Fi Alliance. The Wi-Fi Alliance certifies inter-operability of IEEE 802.11 products and promotes wireless LAN standards across all market segments. The Wi-Fi Alliance's test suite defines how products are tested to obtain interoperability certification with other Wi-Fi Certified products.

WPA uses Temporal Key Integrity Protocol (TKIP) for encryption and dynamic encryption key generation with either a pre-shared key or a RADIUS/802.1x-based authentication. The mechanisms introduced in WPA are designed to provide more robust security to WEP solutions without requiring a hardware upgrade.

Wi-Fi Protected Access 2 (WPA2)

WPA2 is the next generation of Wi-Fi security based on the ratified IEEE 802.11i standard and is also approved by the Wi-Fi Alliance interoperability implementation of the 802.11i standard. WPA2 provides certification in both Enterprise and Personal classifications.

The Enterprise classification requires support for a RADIUS/802.1x-based authentication and pre-shared key; Personal classification requires only a common key shared by the client and the AP.

The newer Advanced Encryption Standard (AES) mechanism introduced in WPA2 generally requires a hardware upgrade of WLAN clients and APs; however, all Cisco CAPWAP hardware is WPA2 enabled.

802.1X

802.1X is an IEEE framework for port-based access control as adopted by the 802.11i security workgroup. The framework provides authenticated access to WLAN networks.

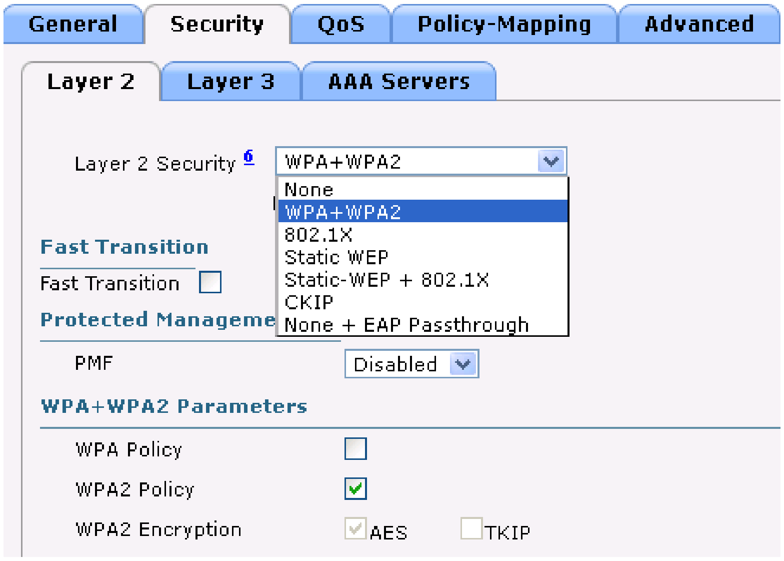
- The 802.11 association process creates a "virtual" port for each WLAN client at the AP.
- The AP blocks all data frames apart from 802.1X-based traffic.
- The 802.1X frames carry the EAP authentication packets, which are passed through to the AAA server by the AP.
- If the EAP authentication is successful, the AAA server sends an EAP success message to the AP, where the AP then allows data traffic from the WLAN client to pass through the virtual port.
- Before opening the virtual port, data link encryption is established between the WLAN client and the AP. This is to ensure no other WLAN client can access the port established for authenticating clients.

Authentication and Encryption

The Cisco Wireless Security suite provides options for security approaches based on required or pre-existing authentication, privacy, and client infrastructure. The Cisco Wireless Security suite supports WPA, WPA2, WEP Extension, and wIPS with the ELM feature.

The following options are available:

- Authentication based on 802.1X using the following EAP methods:
  - Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
  - PEAP- Generic Token Card (PEAP-GTC)
  - PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAPv2)
  - EAP-Transport Layer Security (EAP-TLS)
  - EAP-Subscriber Identity Module (EAP-SIM)
- Encryption:
  - AES-CCMP encryption (WPA2)
  - TKIP encryption enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation via WPA/WPA2 or WEP TKIP Cisco Key Integrity Protocol (CKIP)



Layer 2 Security [6] WPA+WPA2

Fast Transition

Fast Transition ☐

Protected Manageme

PMF Disabled

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☑

WPA2 Encryption ☑ AES ☐ TKIP

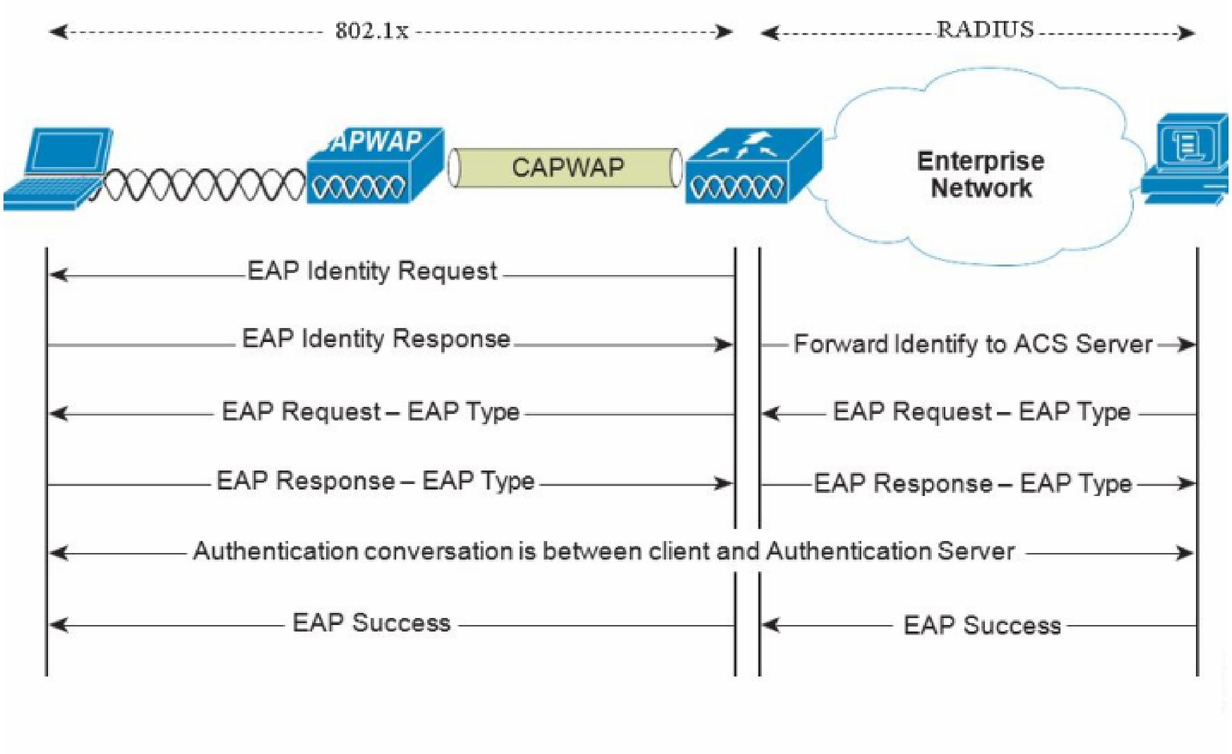
Extensible Authentication Protocol

Extensible Authentication Protocol (EAP) is an IETF RFC, stipulates that an authentication protocol must be de-coupled from the transport protocol. This allows the EAP protocol to be carried by transport protocols such as 802.1X, UDP, or RADIUS without making changes to the authentication protocol itself. The basic EAP protocol contains the following four packet types:

- EAP request—The request packet is sent by the authenticator to the supplicant. Each request has a type field that indicates what is being requested; for example, supplicant identity and EAP type to be used. A sequence number allows the authenticator and the peer to match an EAP response to each EAP request.
- EAP response—The response packet is sent by the supplicant to the authenticator, and uses a sequence number to match the initiating EAP request. The type of the EAP response generally matches the EAP request, except if the response is a negative-acknowledgment (NAK).
- EAP success—The success packet is sent, from the authenticator to the supplicant, when successful authentication occurs.
- EAP failure—The failure packet is sent, from the authenticator to the supplicant, when unsuccessful authentication occurs.

When using EAP in an 802.11i compliant system, the AP operates in EAP pass-through mode. Pass-through mode checks the code identifier and the length fields, and then forwards EAP packets received from the client supplicant to the AAA. EAP packets received by the authenticator from the AAA server are forwarded to the supplicant. Figure 4-2 is an example of an EAP protocol flow.

Figure 4-2 EAP Protocol Flow



Authentication

Depending on your requirements, various authentication protocols such as PEAP, EAP-TLS, and EAP-FAST are used in secure wireless deployments. Regardless of the protocol, they all use 802.1X, EAP, and RADIUS as their underlying transport.

These protocols allow network access control based on the successful authentication of the WLAN client and vice-versa. This solution also provides authorization through policies communicated through the RADIUS protocol, as well as RADIUS accounting.

EAP types used for performing authentication are described in more detail below. The primary factor affecting the choice of EAP protocol is the authentication system (AAA) currently used. Ideally, a secure WLAN deployment should not require the introduction of a new authentication system, but rather should leverage the authentication systems that are already in place.

Supplicants

The various EAP supplicants that are available in the marketplace reflect the diversity of authentication solutions available and customer preferences.

Table 4-1 shows a summary of common EAP supplicants:

- EAP-FAST—EAP-Flexible Authentication via Secured Tunnel. Uses a tunnel similar to that used in PEAP, but does not require the use of Public Key Infrastructure (PKI).

- PEAP MSCHAPv2—Protected EAP MSCHAPv2. Uses a Transport Layer Security (TLS) tunnel, (the IETF standard of SSL) to protect an encapsulated MSCHAPv2 exchange between the WLAN client and the authentication server.
- PEAP GTC—Protected EAP Generic Token Card (GTC). Uses a TLS tunnel to protect a generic token card exchange; for example, a one-time password or LDAP authentication.
- EAP-TLS—EAP Transport Layer Security. Uses PKI to authenticate both the WLAN network and the WLAN client, requiring both a client certificate and an authentication server certificate.

Table 4-1 Comparison of Common Supplicants

	Cisco EAP-FAST	**PEAP MS-CHAPv2**	**PEAP EAP-GTC**	**EAP-TLS**
Single sign-on (MSFT AD only)	Yes	Yes	Yes[1]	Yes
Login scripts (MSFT AD only)	Yes	Yes	Some	Yes[2]
Password change (MSFT AD)	Yes	Yes	Yes	N/A
Microsoft AD database support	Yes	Yes	Yes	Yes
ACS local database support	Yes	Yes	Yes	Yes
LDAP database support	Yes[3]	No	Yes	Yes
OTP authentication support	Yes[4]	No	Yes	No
RADIUS server certificate required?	No	Yes	Yes	Yes
Client certificate required?	No	No	No	Yes
Anonymity	Yes	Yes[5]	Yes[6]	No

1. Supplicant dependent
2. Machine account and machine authentication is required to support the scripts.
3. Automatic provisioning is not supported on with LDAP databases.
4. Supplicant dependent
5. Supplicant dependent
6. Supplicant dependent

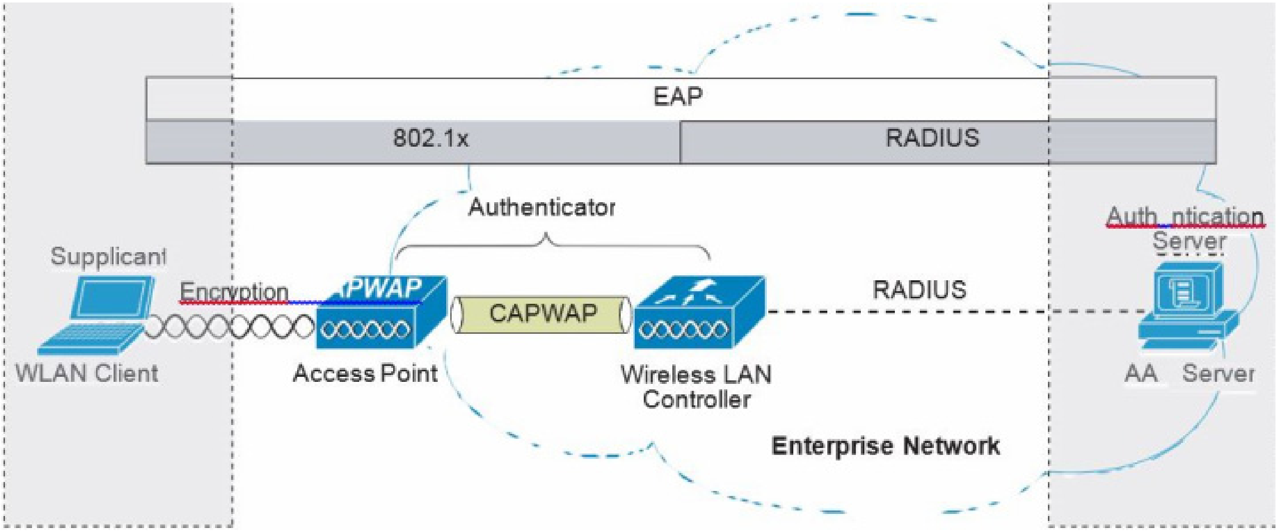
Authenticator

The WLC is the authenticator acting as a relay for EAP messages exchanged between the 802.1X-based supplicant and the RADIUS authentication server. Once authentication is completed successfully, the WLC receives the following:

- A RADIUS packet containing the EAP success message.
- An encryption key, which is generated at the authentication server during the EAP authentication.
- RADIUS vendor-specific attributes (VSAs) for communicating policy.

Figure 4-3 displays the logical location of the authenticator within the overall authentication architecture. The authenticator controls network access using the 802.1X protocol, and relays EAP messages between the supplicant and the authentication server.

Figure 4-3 Authenticator Location



The EAP exchange sequence is as follows:

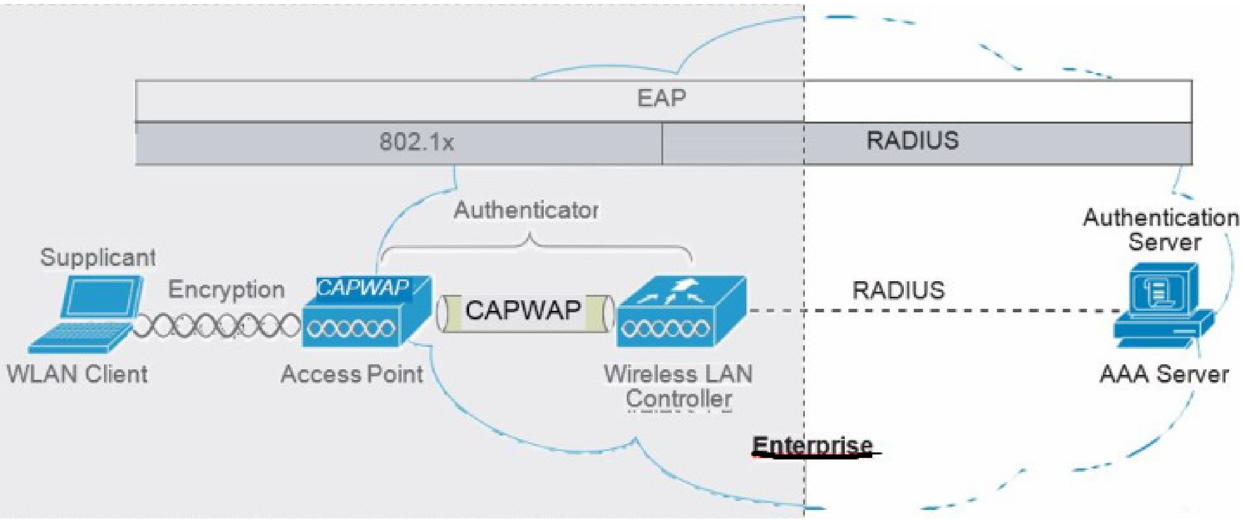
- Packet no.1 is sent by the AP to the client, requesting the client identity; this begins the EAP exchange.
- Packet no.2 contains the client identity, which is forwarded to the RADIUS server. Based on the client identity, in packet 2, the RADIUS server will determine to continue the EAP authentication or not.
- Packet no.3 contains a RADIUS server request to use PEAP as the EAP method for authentication. The actual request depends on the EAP types configured on the RADIUS server. If the client rejects the PEAP request, the RADIUS server can offer other EAP types.
- Packets no.4 through 8 are the TLS tunnel setup for PEAP.
- Packets no.9 through 16 are the authentication exchange within PEAP.
- Packet no.17 is the EAP message informing the supplicant and the authenticator that the authentication was successful; in addition, Packet no.17 carries encryption keys and authorization information, in the form of RADIUS VSAs, to the authenticator.

Authentication Server

The authentication server used in the Cisco Secure Unified Wireless Network solution is the Cisco Access Control Server (ACS) and the Cisco Identity Services Engine (ISE). ACS is available as software that is installed on a Windows 2000 or later servers, or as an appliance. ISE is available as software that is installed on the VM server . Alternatively, the authentication server role can be implemented within specific WLAN infrastructure devices such as local authentication services on an IOS AP, local EAP authentication support within the WLC, AAA services integrated in any AAA server that supports the required EAP types.

Figure 4-4 shows the logical location of the authentication server within the overall wireless authentication architecture, where it performs the EAP authentication via a RADIUS tunnel.

Figure 4-4 Authentication Server Location



After the completion of a successful EAP authentication, the authentication server sends an EAP success message to the authenticator. This message tells the authenticator that the EAP authentication process was successful, and passes the pair-wise master key (PMK) to the authenticator that is in turn used as the basis for creating the encrypted stream between the WLAN client and the AP.

Encryption

Encryption is a necessary component of WLAN security to provide privacy over a local RF broadcast network. Any new deployment should be using either TKIP (WPA/WPA2) or AES encryption.

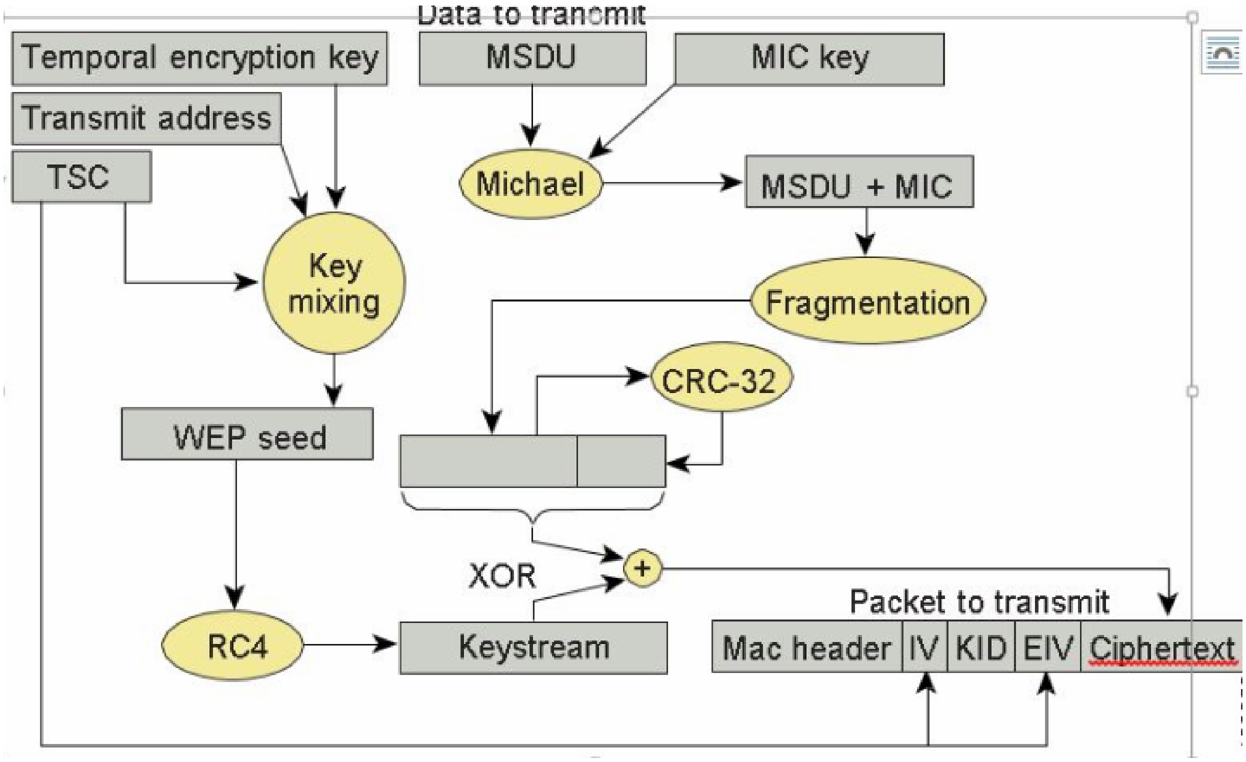
In WPA and WPA2, the encryption keys are derived during the four-way handshake discussed later in this section.

TKIP Encryption

Enterprise-level encryption mechanisms specified by 802.11i are certified as WPA/WPA2 and wIPS by the Wi-Fi Alliance: Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standard (AES). TKIP is the certified encryption method. It provides support for legacy WLAN equipment by addressing the original flaws associated with the 802.11 WEP encryption method. It does this by making use of the original RC4 core encryption algorithm.

The hardware refresh cycle of WLAN client devices is such that TKIP and AES is likely to be a common encryption option for a number of years to come. The AES encryption is the preferred method because it brings the WLAN encryption standards into alignment with broader IT industry standards and best practices. Figure 4-5 displays a basic TKIP flow chart.

Figure 4-5 TKIP Flow Chart



The two primary functions of TKIP are the generation of a per-packet key using RC4 encryption of the MAC service data unit (MSDU) and a message integrity check (MIC) in the encrypted packet. The per-packet key is a hash of the transmission address, the frame initialization vector (IV), and the encryption key. The IV changes with each frame transmission, so the key used for RC4 encryption is unique for each frame.

The MIC is generated using the Michael algorithm to combine a MIC key with user data. The use of the Michael algorithm is a trade-off because its low computational overhead is good for performance, but it can be susceptible to an active attack. To address this, WPA includes countermeasures to safeguard against these attacks that involve temporarily disconnecting the WLAN client and not allowing a new key negotiation for 60 seconds. Unfortunately, this behavior can itself become a type of DoS attack. Many WLAN implementations provide an option to disable this countermeasure feature.

Removal of TKIP from Wi-Fi® Devices

As per the Wi-Fi alliance and 802.11 WPA, wireless networks that use Temporal Key Integrity Protocol (TKIP), no longer provide sufficient security to protect consumer or enterprise Wi-Fi® networks. TKIP is an older security technology with known vulnerabilities to some cryptographic attacks.Wi-Fi® networks. TKIP is an older security technology with known vulnerabilities to some cryptographic attacks. TKIP and WEP use the same underlying cipher, and, consequently, they are vulnerable to a number of similar attacks. TKIP was designed as a transitional mechanism in 2004 for devices equipped with WEP and unable to support AES. Due to the known vulnerabilities of TKIP, networks utilizing it may be more susceptible to attack.

Recommendations:

- Network administrators should purchase or deploy equipment that supports WPA2.
- Network administrators should configure their APs to be WPA2 only.
- Equipment vendors should proactively transition away from TKIP support by discouraging its use to their customer base, and removing the functionality in product as internal research indicates when their market no longer needs it.

For equipment vendors, Wi-Fi Alliance recommends that they discourage the use of TKIP in the short term, and ultimately remove TKIP from all Wi-Fi devices when their market no longer needs it. At a minimum, vendors should remove TKIP and any "TKIP-only" mode configurations from the primary device interface. Access to the "TKIP-only" configuration mode via a secondary configuration interface is acceptable. The requirement to go to a secondary interface is a mechanism used to restrict TKIP usage to only those deployments with legacy devices; other deployments will typically use the primary configuration interface.

Transitional Exception:

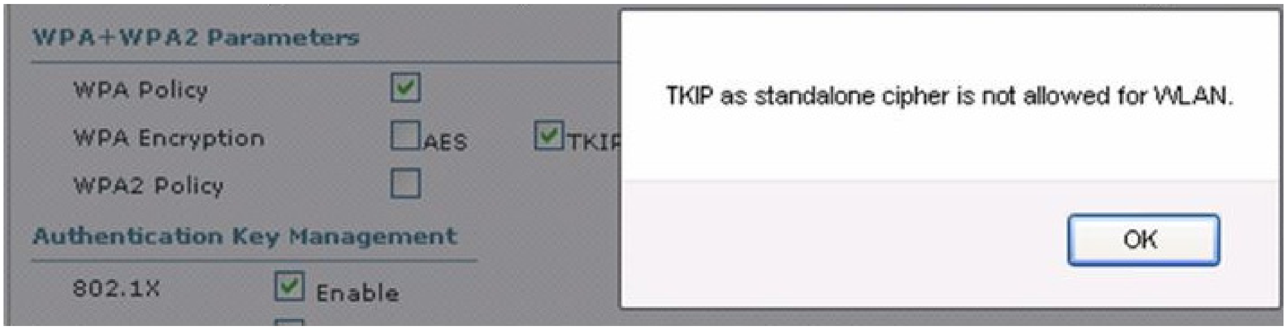
Vendors should remove TKIP and any "TKIP-only" mode configurations from the primary device interface. Access to the "TKIP-only" configuration mode via a secondary configuration interface is acceptable (CLI).

For more information, see Technical Note - Removal of TKIP from Wi-Fi Devices.

We developed a set of commands to configure TKIP from CLI mode only as was recommended by the Wi-Fi alliance:

```
(Cisco Controller) >config wlan security wpa wpa1 ciphers tkip <en/dis> <wlan#>
(Cisco Controller) >test wlan standalone-tkip <enable/disable> <wlan#>>
```

If the same configuration is attempted from the GUI interface the following will be displayed on the screen:



WPA+WPA2 Parameters

WPA Policy ☑

WPA Encryption ☐AES ☑TKIP

WPA2 Policy ☐

Authentication Key Management

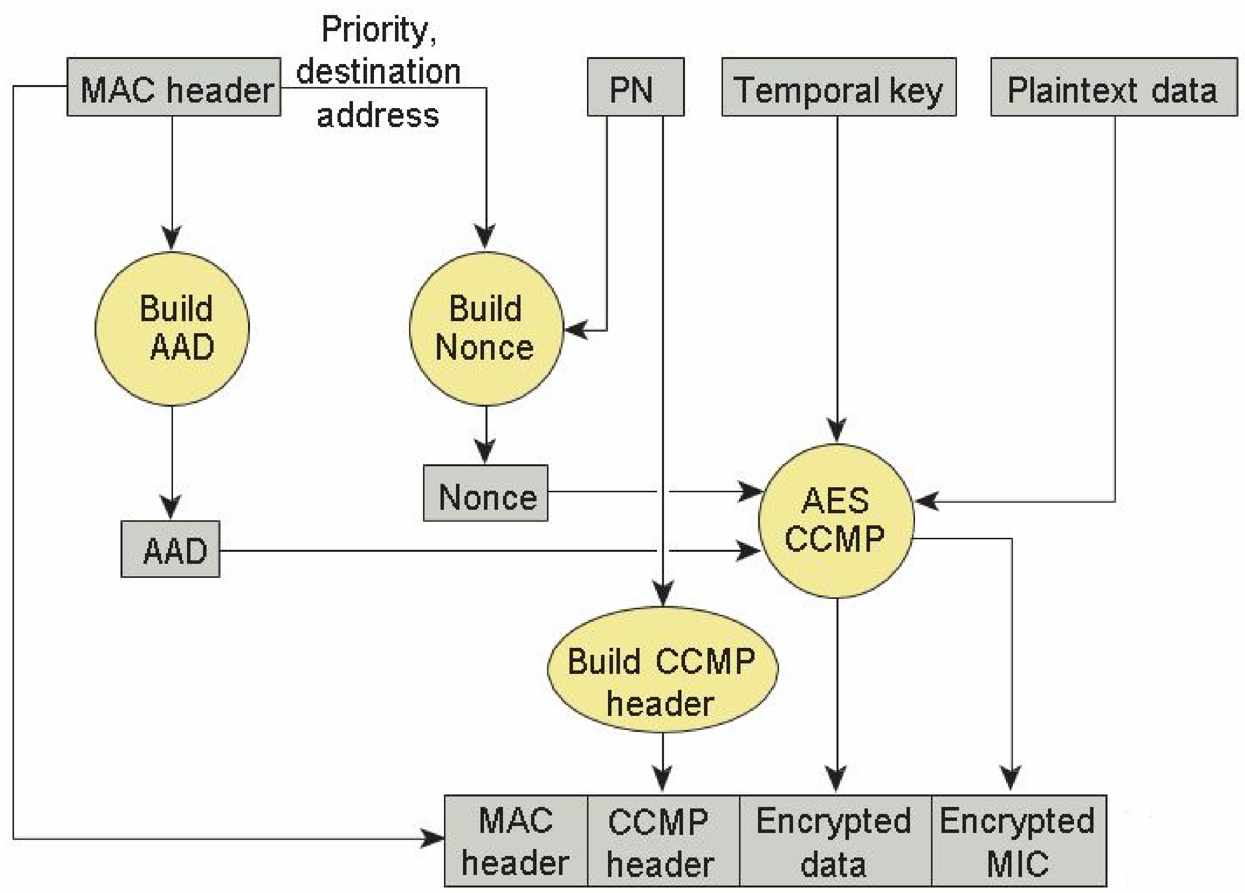
802.1X ☑ Enable

TKIP as standalone cipher is not allowed for WLAN.

AES Encryption

Figure 4-6 displays the basic AES counter mode/CBC MAC Protocol (CCMP) flow chart. CCMP is one of the AES encryption modes, where the counter mode provides confidentiality and CBC MAC provides message integrity.

Figure 4-6 WPA2 AES CCMP



In the CCMP procedure, additional authentication data (AAD) is taken from the MAC header and included in the CCM encryption process. This protects the frame against alteration of the non-encrypted portions of the frame.

To protect against replay attacks, a sequenced packet number (PN) is included in the CCMP header. The PN and portions of the MAC header are used to generate a nonce that is in turn used by the CCM encryption process.

Four-Way Handshake

The four-way handshake is the method used to derive the encryption keys to encrypt wireless data frames. Figure 4-7 graphically represents the frame exchanges used to generate the encryption keys. These keys are referred to as temporal keys.

The encryption keys are derived from the PMK that is mutually derived during the EAP authentication. This PMK is sent to the authenticator in the EAP success message, but is not forwarded to the supplicant because the supplicant has derived its own copy of the PMK.

1. The authenticator sends an EAPOL-Key frame containing an authenticator nonce (ANonce), which is a random number generated by the authenticator.

The supplicant derives a PTK from the ANonce and supplicant nonce (SNonce), which is a random number generated by the client/supplicant.

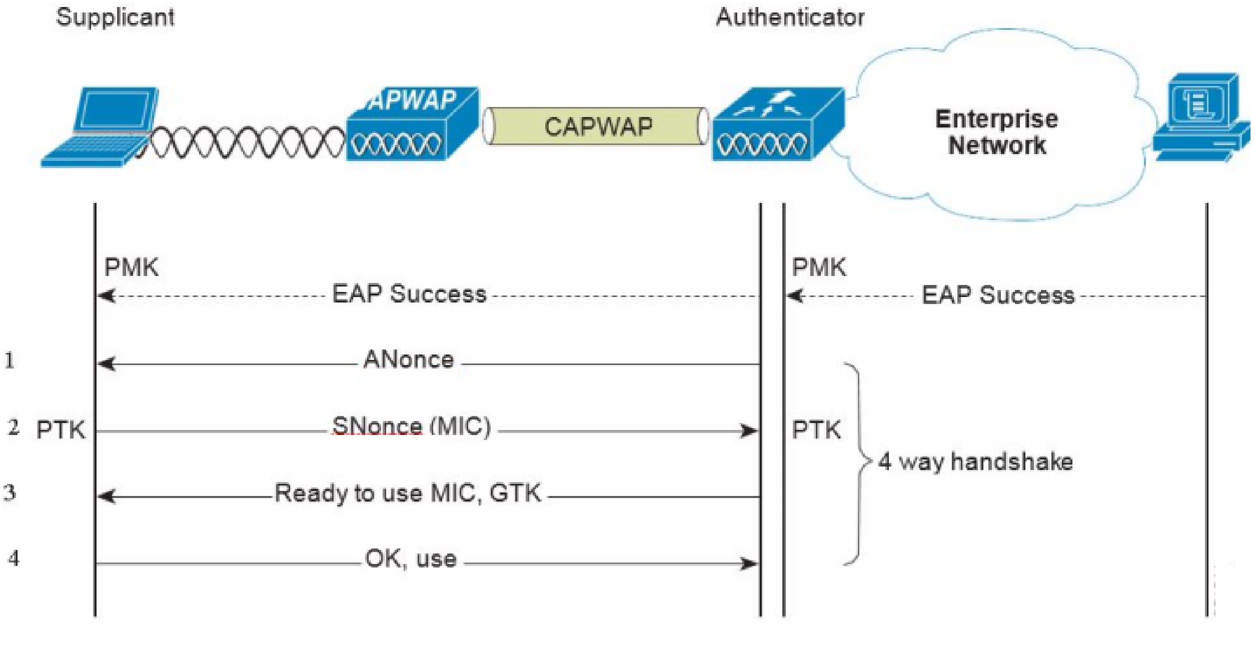
2. The supplicant sends an EAPOL-Key frame containing an SNonce, the RSN information element from the (re)association request frame, and an MIC.

   The authenticator derives a PTK from the ANonce and SNonce and validates the MIC in the EAPOL-Key frame.

3. The authenticator sends an EAPOL-Key frame containing the ANonce, the RSN information element from its beacon or probe response messages; the MIC, determining whether to install the temporal keys; and the encapsulated group temporal key (GTK), the multicast encryption key.

4. The supplicant sends an EAPOL-Key frame to confirm that the temporal keys are installed.

Figure 4-7 Four-Way Handshake

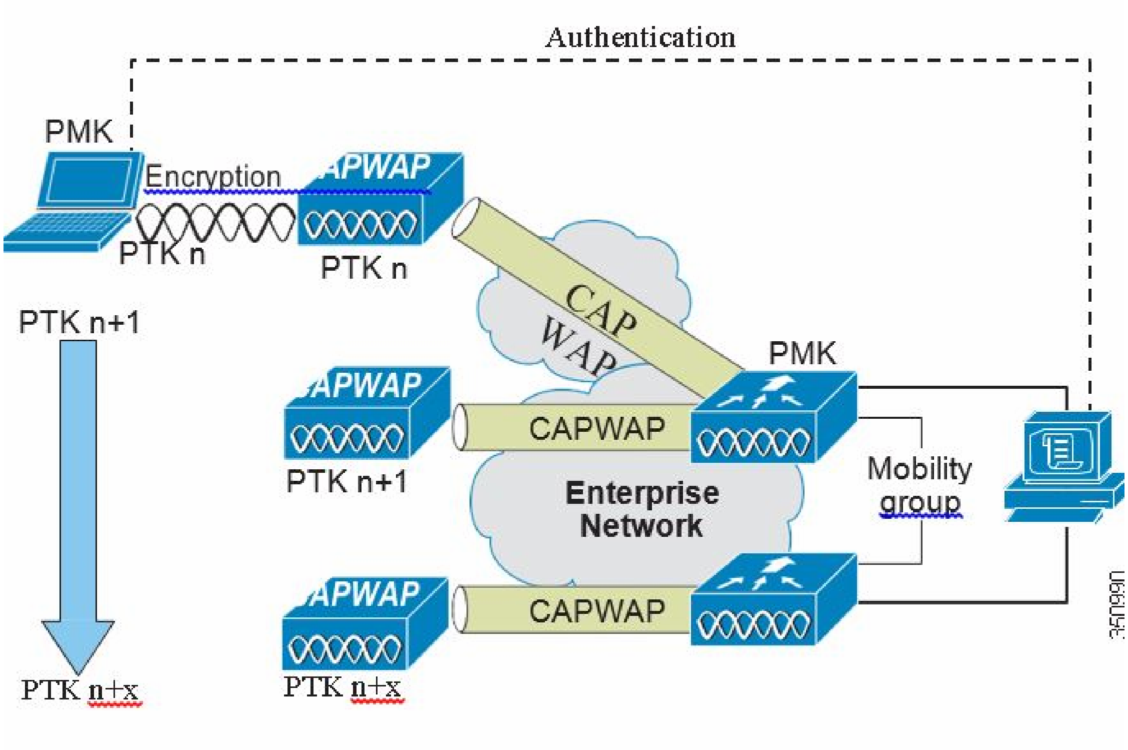


Proactive Key Caching (PKC) and CCKM

Proactive Key Caching (PKC) is an 802.11i extension that allows for the proactive caching (before the client roaming event) of the PMK that is derived during a client 802.1x/EAP authentication at the AP (see Figure 4-8). If a PMK (for a given WLAN client) is pre-cached at an AP, to which the client is about to roam, full 802.1x/EAP authentication is not required. Instead, the WLAN client can simply use the WPA four-way handshake process to securely derive a new session encryption key for communication with that AP.

The distribution of these cached PMKs to APs is greatly simplified in the Cisco Unified Wireless Network deployment. The PMK is simply cached in the controller(s) and made available to all APs that connect to it. The PMK is also shared with all other controllers that make up a mobility group with the anchor controller.

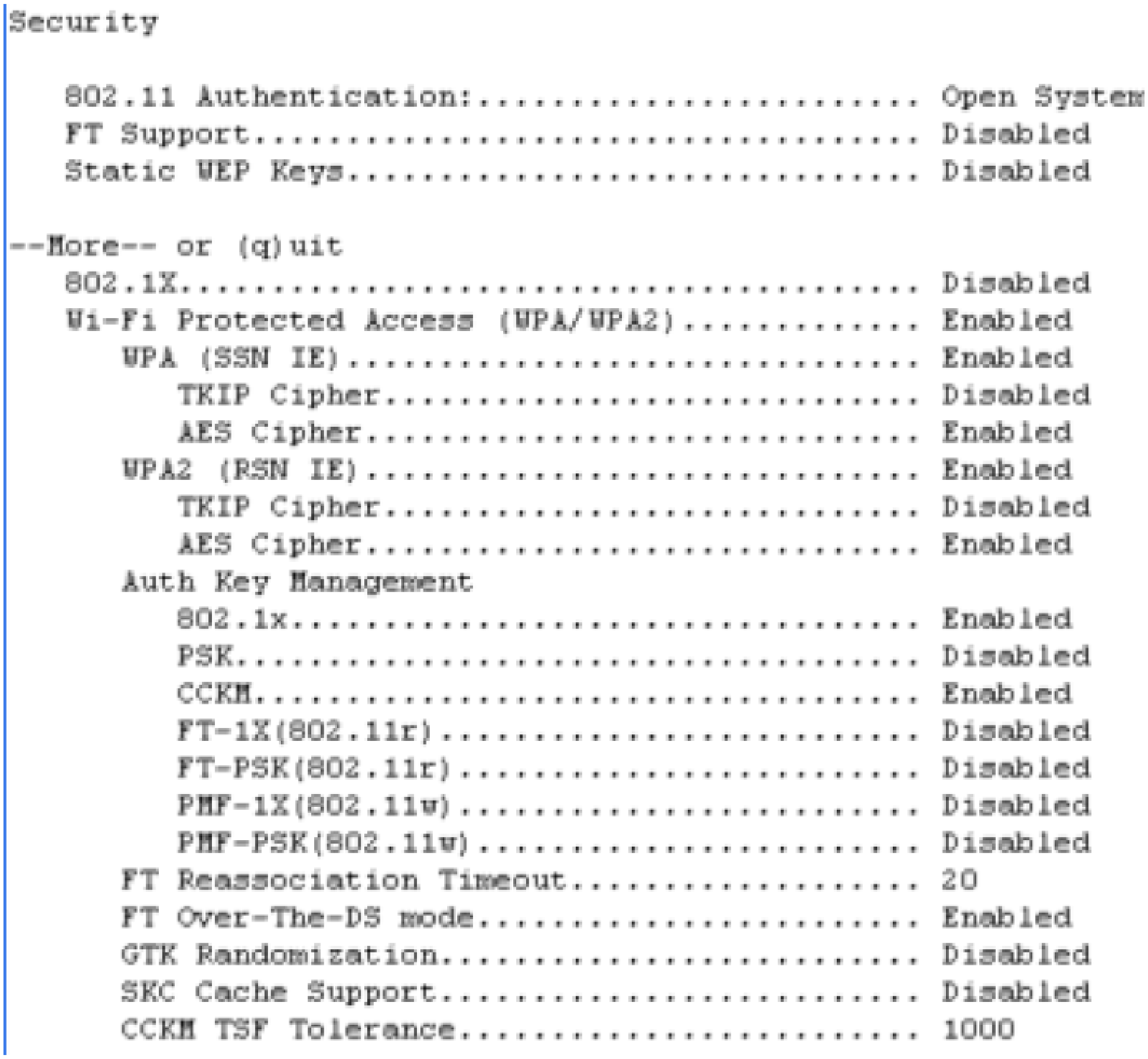
Figure 4-8 Proactive Key Caching Architecture



Cisco Centralized Key Management (CCKM) is a Cisco standard supported by Cisco Compatible Extensions clients to provide fast secure roaming (FSR). The principle mechanism for accelerating the roaming process is the same as PKC, which is to use a cached PMK. However, the implementation in CCKM is slightly different, which makes the two mechanisms incompatible with each other.

The state of the key cache for each WLAN client can be seen with the **show pmk-cache all** command. This identifies which clients are caching the keys, and which key caching mechanism is being used. The 802.11r workgroup is responsible for the standardization of an FSR mechanism for 802.11.

The WLC supports both CCKM and PKC on the same WLAN -802.1x+CCKM, as shown in the following example:



```
Security

   802.11 Authentication:........................ Open System
   FT Support.................................... Disabled
   Static WEP Keys............................... Disabled

--More-- or (q)uit
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
      WPA2 (RSN IE).............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
      Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Enabled
         FT-1X(802.11r).......................... Disabled
         FT-PSK(802.11r)......................... Disabled
         PMF-1X(802.11w)......................... Disabled
         PMF-PSK(802.11w)........................ Disabled
      FT Reassociation Timeout................... 20
      FT Over-The-DS mode........................ Enabled
      GTK Randomization.......................... Disabled
      SKC Cache Support.......................... Disabled
      CCKM TSF Tolerance......................... 1000
```

Cisco Unified Wireless Network Architecture

Figure 4-9 shows a high level topology of the Cisco Unified Wireless Network architecture that includes the CAPWAP APs, the mesh CAPWAPs, the management system (WCS/NCS/PI), and the wireless LAN controller (WLC).

The Cisco Access Control Server (ACS) or the Identity Services Engine (ISE) and their AAA features complete the solution by providing RADIUS services in support of wireless user authentication and authorization.

Figure 4-9 Cisco Unified Wireless Network Architecture

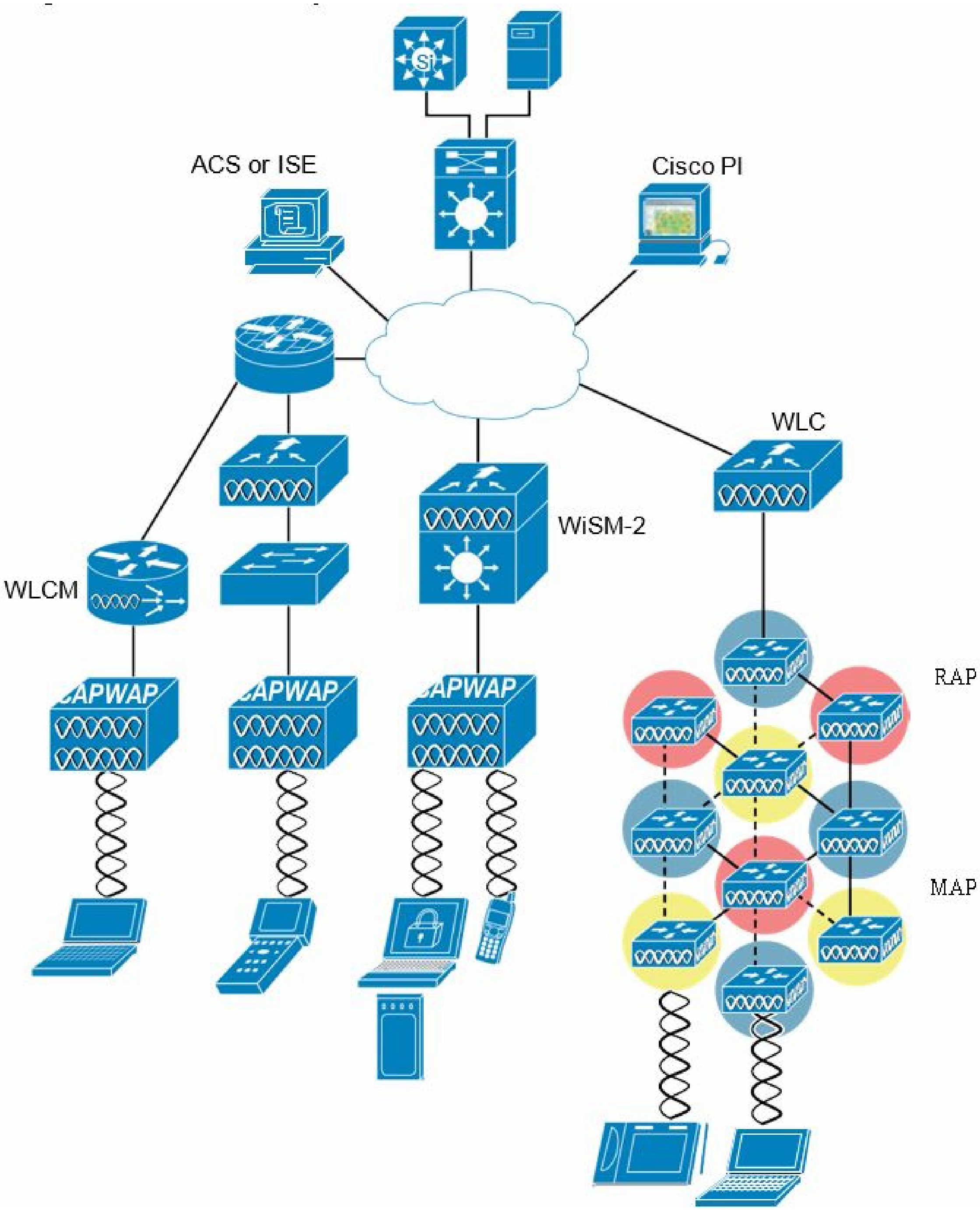
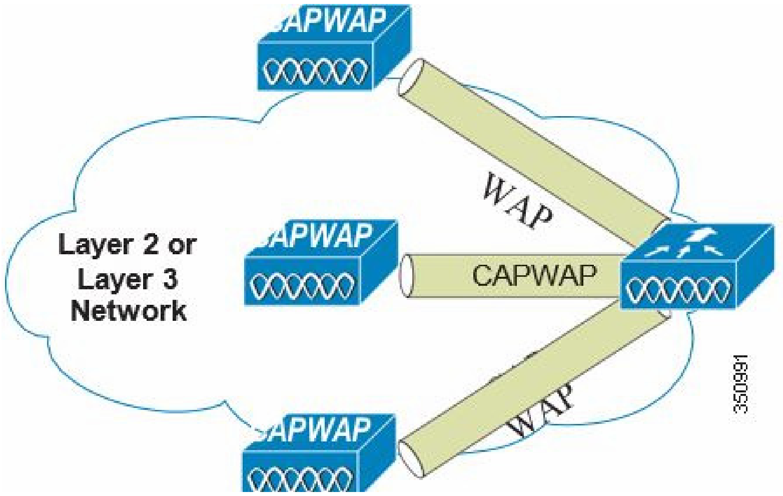


Figure 4-10 illustrates one of the primary features of the architecture: how APs use the CAPWAP protocol to communicate with and tunnel traffic to a WLC.

Figure 4-10 CAPWAP APs and WLC Connection



CAPWAP has three primary functions:

- Control and management of the AP
- Tunneling of WLAN client traffic to the WLC
- Collection of 802.11 data for the management of the Cisco Unified Wireless IPv6

Cisco Unified Wireless Network Security Features

The native 802.11 security features combined with the physical security and ease of deployment of the CAPWAP architecture serves to improve the overall security of WLAN deployments. In addition to the inherent security benefits offered by the CAPWAP protocol, the Cisco Unified Wireless Network solution also includes the following additional security features:

- Enhanced WLAN security options
- ACL and firewall features
- Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP) protection
- Peer-to-peer blocking
- Wireless intrusion protection system (wIPS)
  - Client exclusion
  - Rogue AP detection
- Management frame protection
- Dynamic RF management
- Architecture integration
- IDS integration

Enhanced WLAN Security Options

The Cisco Unified Wireless Network solution supports multiple concurrent WLAN security options. For example, multiple WLANs can be created on a WLC, each with its own WLAN security settings that can range from an open guest WLAN network and WEP networks for legacy platforms to the combinations of WPA and/or WPA2 security configurations.

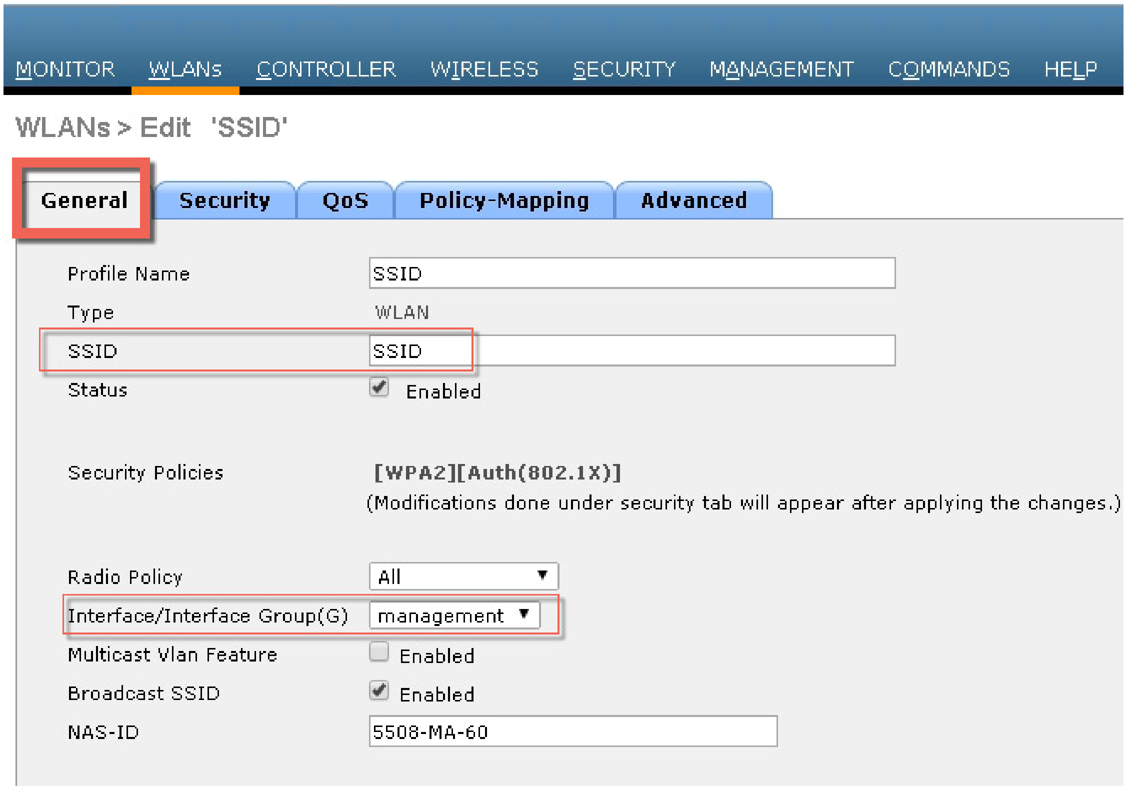
Each WLAN SSID can be mapped to either the same or different dot1q interface on the WLC, or Ethernet over IP (EoIP) tunneled to a different controller through a mobility anchor (Auto Anchor Mobility) connection.

If a WLAN client authenticates via 802.1x, a dot1q VLAN assignment can be controlled by way of RADIUS attributes passed to the WLC upon successful authentication.

Figure 4-11, Figure 4-12 and Figure 4-13 show a subset of the Unified Wireless Network WLAN configuration screen. The following four main configuration items appears:

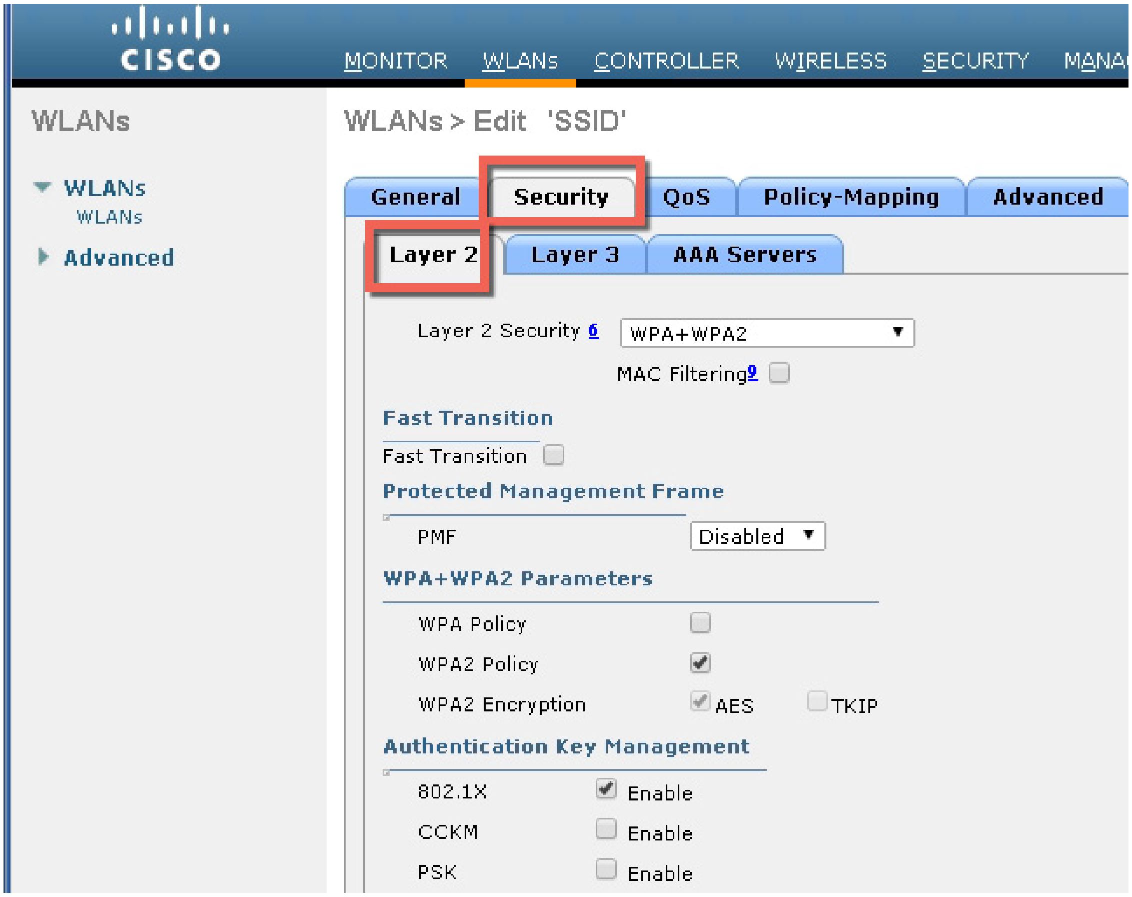
- The WLAN SSID
- The WLC interface to which the WLAN is mapped
- The Level 2security method (Figure 4-12)
- The Level 3 security method (Figure 4-13)

Figure 4-11 WLANs General Tab



Profile Name	SSID
Type	WLAN
SSID	SSID
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	☐ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	5508-MA-60

Figure 4-12 WLANs Layer 2 Security Tab



WLANs > Edit 'SSID'

Layer 2 Security 6 WPA+WPA2

MAC Filtering9 ☐

Fast Transition

Fast Transition ☐

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☑

WPA2 Encryption ☑ AES ☐ TKIP

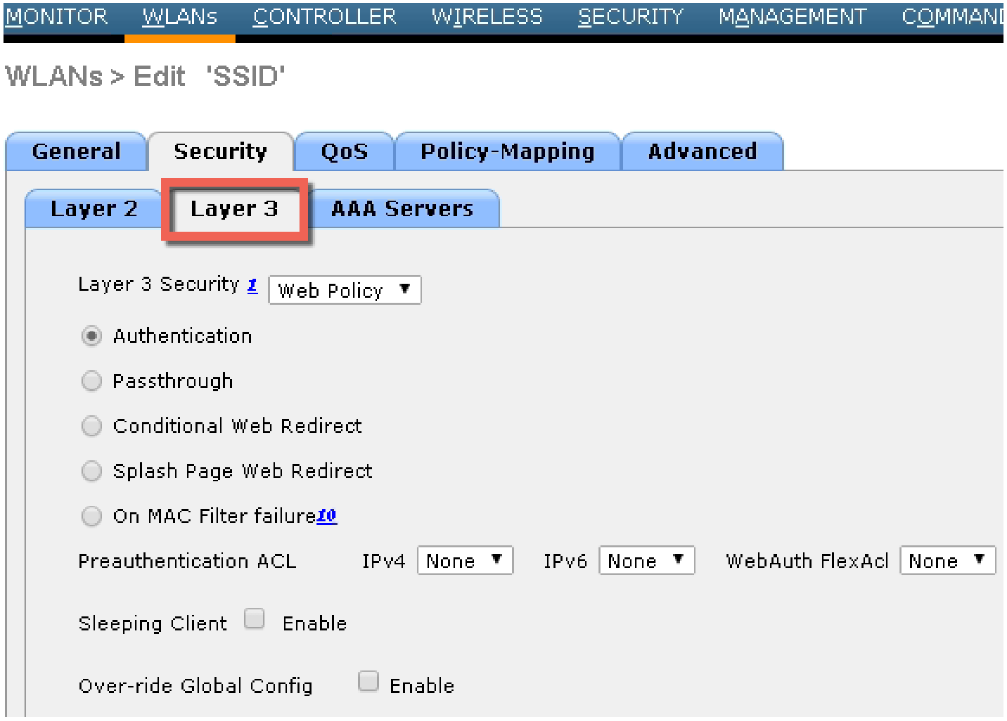
Authentication Key Management

802.1X ☑ Enable

CCKM ☐ Enable

PSK ☐ Enable

Figure 4-13 Wlan LAN security Layer 3



Layer 3 Security 1 Web Policy ▼

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure10

Preauthentication ACL IPv4 None ▼ IPv6 None ▼ WebAuth FlexAcl None ▼

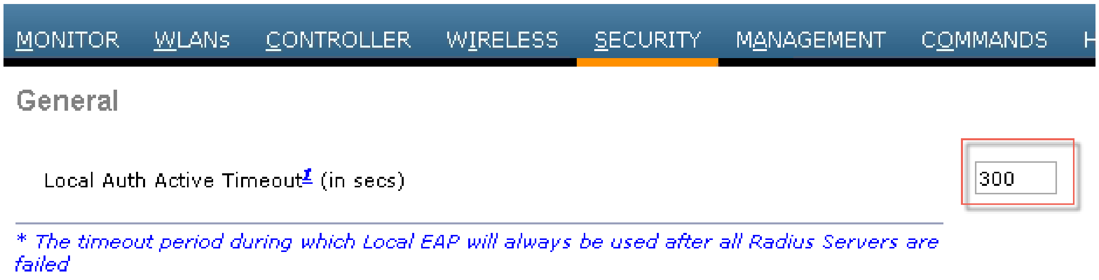
Sleeping Client ☐ Enable

Over-ride Global Config ☐ Enable

Local EAP Authentication

The WLC software provides local EAP authentication capability that can be used when an external RADIUS server is not available or becomes unavailable. The delay before switching to local authentication is configurable, as illustrated in Figure 4-14. When RADIUS server availability is restored, the WLC automatically switches back from local authentication to RADIUS server authentication.

Figure 4-14 Local Authentication Timeout



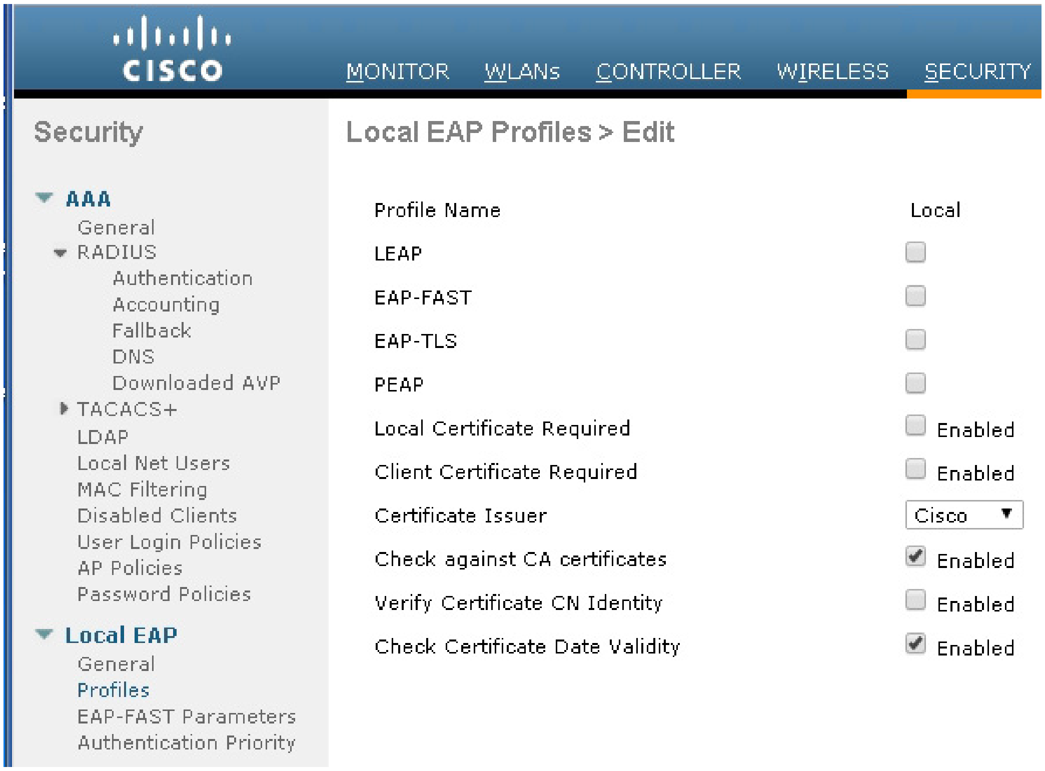
Local Auth Active Timeout1 (in secs) 300

* The timeout period during which Local EAP will always be used after all Radius Servers are failed

The EAP types supported locally on the WLC are LEAP, EAP-FAST, EAP-TLS, and PEAP.

Figure 4-15 displays the window where you can select the local EAP profiles.

Figure 4-15 Local EAP Profiles

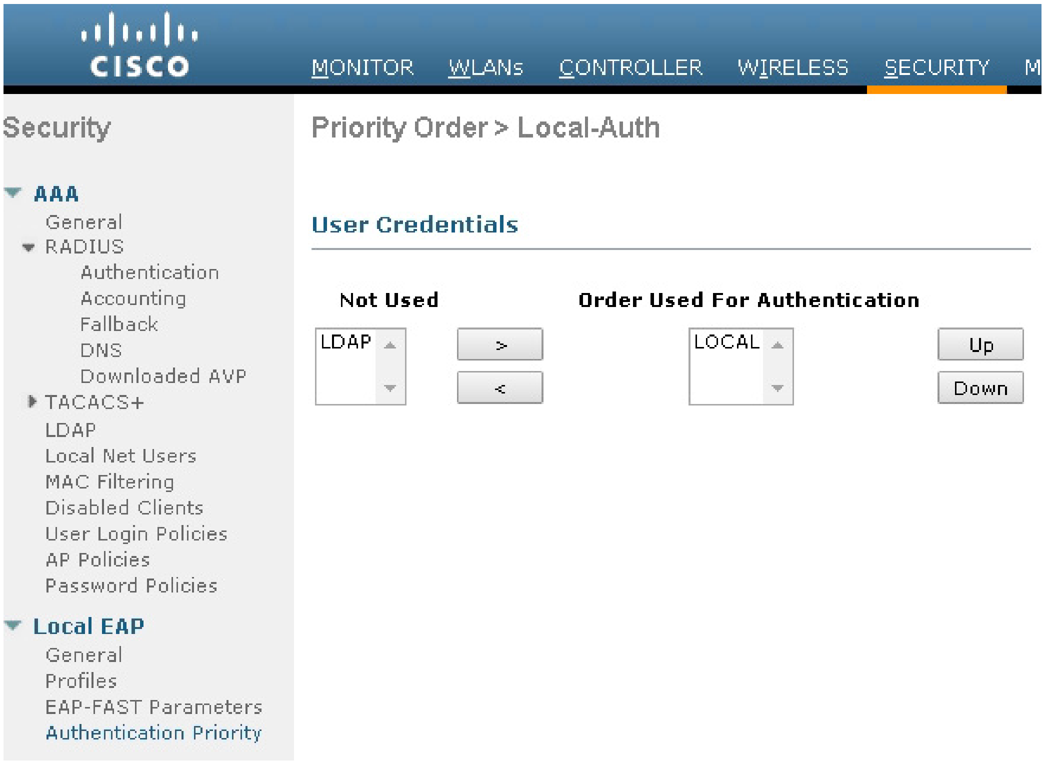


Local EAP Profiles > Edit

Profile Name	Local
LEAP	☐
EAP-FAST	☐
EAP-TLS	☐
PEAP	☐
Local Certificate Required	☐ Enabled
Client Certificate Required	☐ Enabled
Certificate Issuer	Cisco ▼
Check against CA certificates	☑ Enabled
Verify Certificate CN Identity	☐ Enabled
Check Certificate Date Validity	☑ Enabled

WLC can use its local database for authentication data, and it can also access an LDAP directory to provide data for EAP-FAST or EAP-TLS authentication. The user credential database priority (LDAP versus Local) is configurable, as shown in Figure 4-16.

Figure 4-16 Local EAP Priority



Priority Order > Local-Auth

User Credentials

Not Used: LDAP

Order Used For Authentication: LOCAL

ACL and Firewall Features

An Access Control List (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). After ACLs are configured on the controller, they can be applied to the management interface, the AP-manager interface, any of the dynamic interfaces, or a WLAN to control data traffic to and from wireless clients or to the controller CPU to control all traffic destined for the CPU.

You may also want to create a pre-authentication ACL for web authentication. Such an ACL could be used to allow certain types of traffic before authentication is complete.

Both IPv4 and IPv6 ACL are supported. IPv6 ACLs support the same options as IPv4 ACLs including source, destination, source and destination ports.

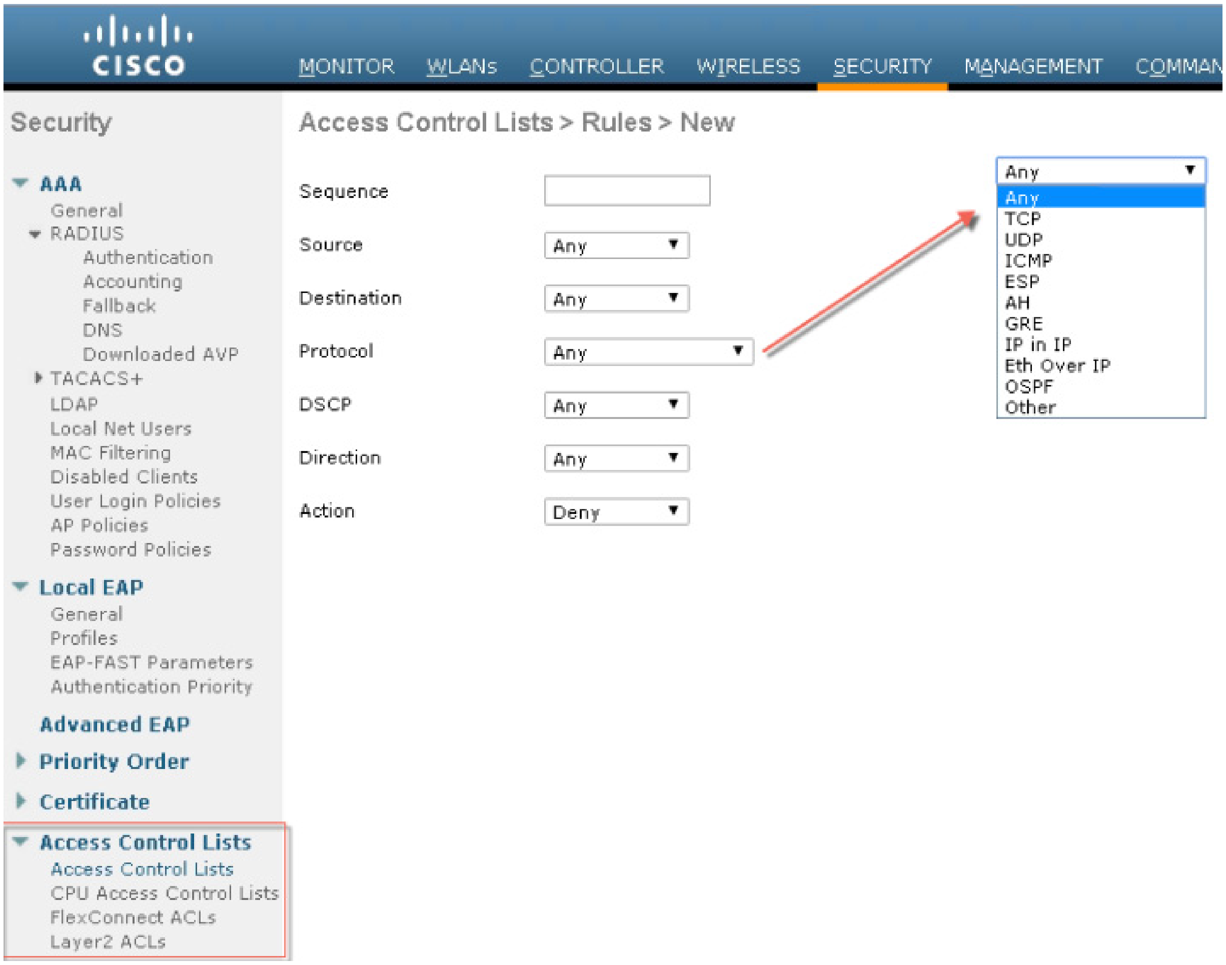
You can enable only IPv4 traffic in your network by blocking IPv6 traffic. That is, you can configure an IPv6 ACL to deny all IPv6 traffic and apply it on specific or all WLANs.

- You can define up to 64 ACLs, each with up to 64 rules (or filters) for both IPv4 and IPv6. Each rule has parameters that affect its action. When a packet matches all of the parameters for a rule, the action set for that rule is applied to the packet.
- When you apply CPU ACLs on a Cisco 5500 Series Controller or a Cisco WiSM2, you must permit traffic towards the virtual interface IP address for web authentication.
- All ACLs have an implicit “deny all rule” as the last rule. If a packet does not match any of the rules, it is dropped by the controller.

- If you are using an external web server with a Cisco 5500 Series Controller or a controller network module, you must configure a pre-authentication ACL on the WLAN for the external web server.
- If you apply an ACL to an interface or a WLAN, wireless throughput is degraded when downloading from a 1-GBps file server. To improve throughput, remove the ACL from the interface or WLAN, move the ACL to a neighboring wired device with a policy rate-limiting restriction, or connect the file server using 100 Mbps rather than 1 Gbps.
- Multicast traffic received from wired networks that is destined to wireless clients is not processed by WLC ACLs. Multicast traffic initiated from wireless clients, destined to wired networks or other wireless clients on the same controller, is processed by WLC ACLs.
- ACLs are configured on the controller directly or configured through templates. The ACL name must be unique.
- You can configure ACL per client (AAA overridden ACL) or on either an interface or a WLAN. The AAA overridden ACL has the highest priority. However, each interface, WLAN, or per client ACL configuration that you apply can override one another.
- If peer-to-peer blocking is enabled, traffic is blocked between peers even if the ACL allows traffic between them.
- Authentication traffic has to go through the Cisco WLC for this feature to be supported, even if DNS-based ACL is local to the AP.
- When you create an ACL, it is recommended to perform the two actions (create an ACL or ACL rule and apply the ACL or ACL rule) continuously either from CLI or GUI.

Figure 4-17 displays the ACL Configuration page. The ACL can specify source and destination address ranges, protocols, source and destination ports, DSCP, and direction in which the ACL is to be applied. An ACL can be created out of a sequence of various rules.

Figure 4-17 ACL Configuration Page



Access Control Lists > Rules > New

Sequence

Source Any

Destination Any

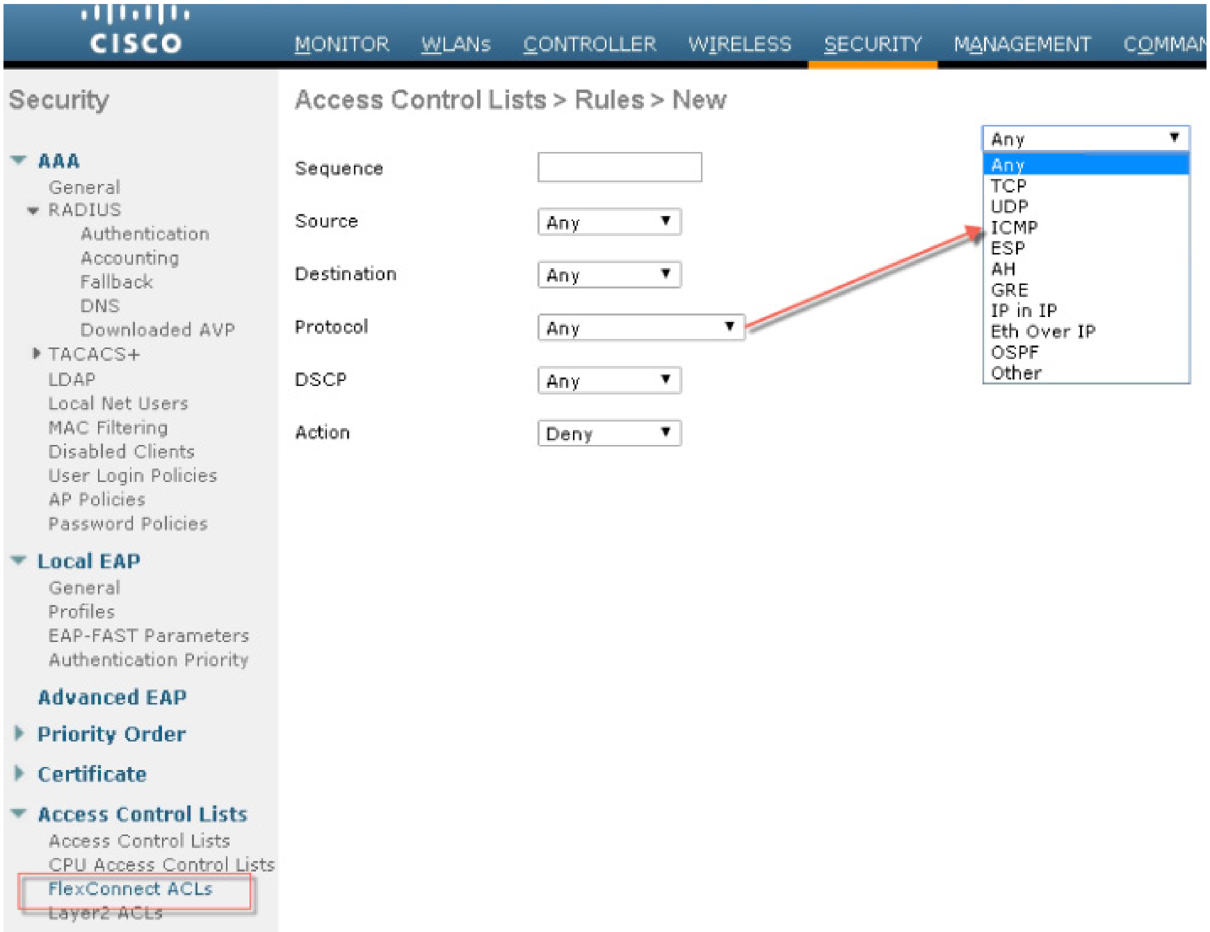
Protocol Any

DSCP Any

Direction Any

Action Deny

Figure 4-18 Illustration of Flex Connect ACL



Access Control Lists > Rules > New

Sequence

Source Any

Destination Any

Protocol Any

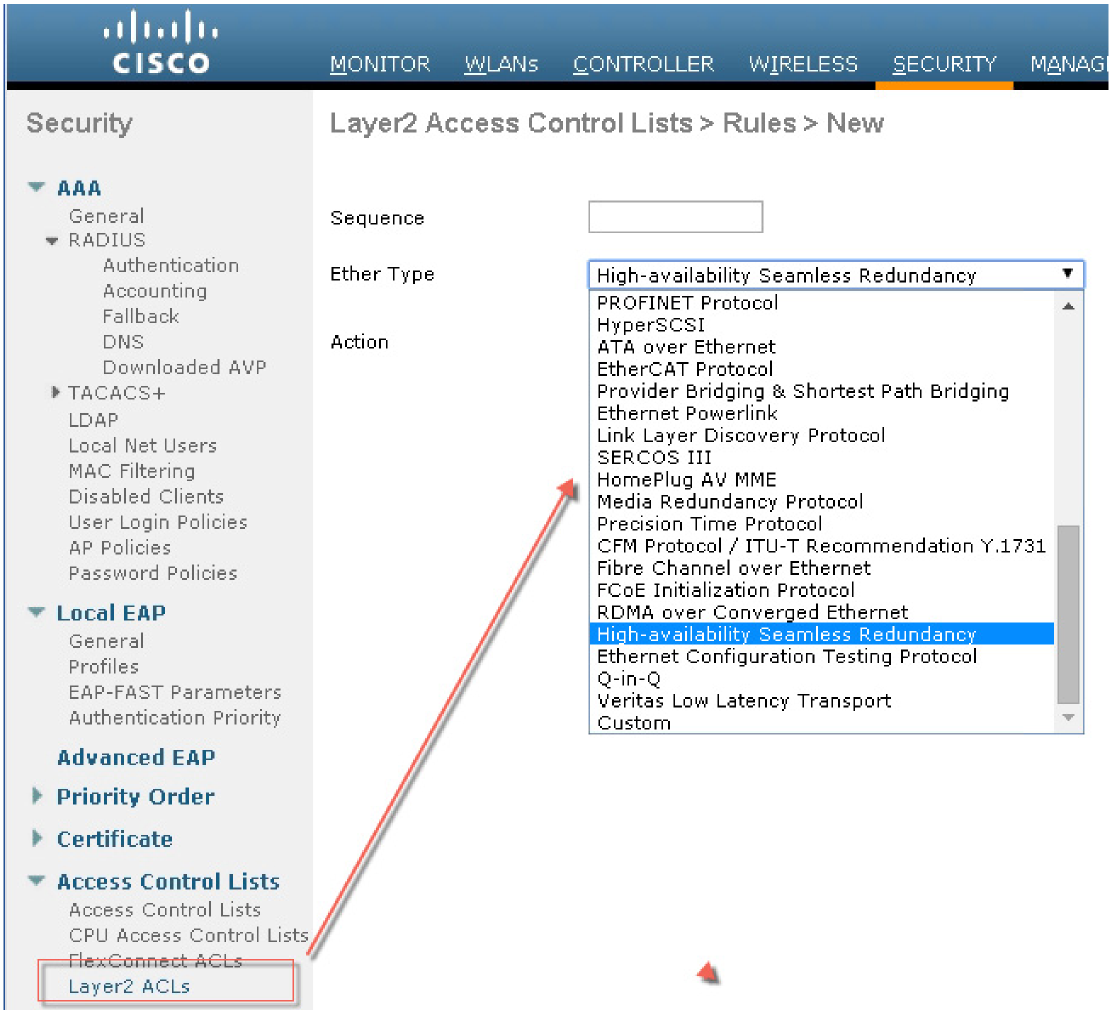
DSCP Any

Action Deny

Layer 2 Access Control Lists

You can configure rules for Layer 2 access control lists (ACLs) based on the Ethertype associated with the packets. Using this feature, if a WLAN with central switching is required to support only PPPoE clients, you can apply Layer 2 ACL rules on the WLAN to allow only PPPoE packets after the client is authenticated and the rest of the packets are dropped. Similarly, if the WLAN is required to support only IPv4 clients or only IPv6 clients, you can apply Layer 2 ACL rules on the WLAN to allow only IPv4 or IPv6 packets after the client is authenticated and the rest of the packets are dropped. For a locally-switched WLAN, you can apply the same Layer 2 ACL either for the WLAN or a FlexConnect AP. AP-specific Layer 2 ACLs can be configured only on FlexConnect APs. This is applicable only for locally-switched WLANs. The Layer 2 ACL that is applied to the FlexConnect AP takes precedence over the Layer 2 ACL that is applied to the WLAN.

Figure 4-19 Illustration of Layer 2 ACL available for configuration on the WLC



Layer2 Access Control Lists > Rules > New

Sequence

Ether Type: High-availability Seamless Redundancy

Action

DNS-based Access Control Lists

The DNS-based ACLs are used for client devices such as Apple and Android devices. When using these devices, you can set pre-authentication ACLs on the Cisco WLC to determine where devices have the right to go.

To enable DNS-based ACLs on the Cisco WLC, you need to configure the allowed URLs for the ACLs. The URLs need to be pre-configured on the ACL.

With DNS-based ACLs, the client when in registration phase is allowed to connect to the configured URLs.

The Cisco WLC is configured with the ACL name and that is returned by the AAA server for pre-authentication ACL to be applied. If the ACL name is returned by the AAA server, then the ACL is applied to the client for web-redirection.

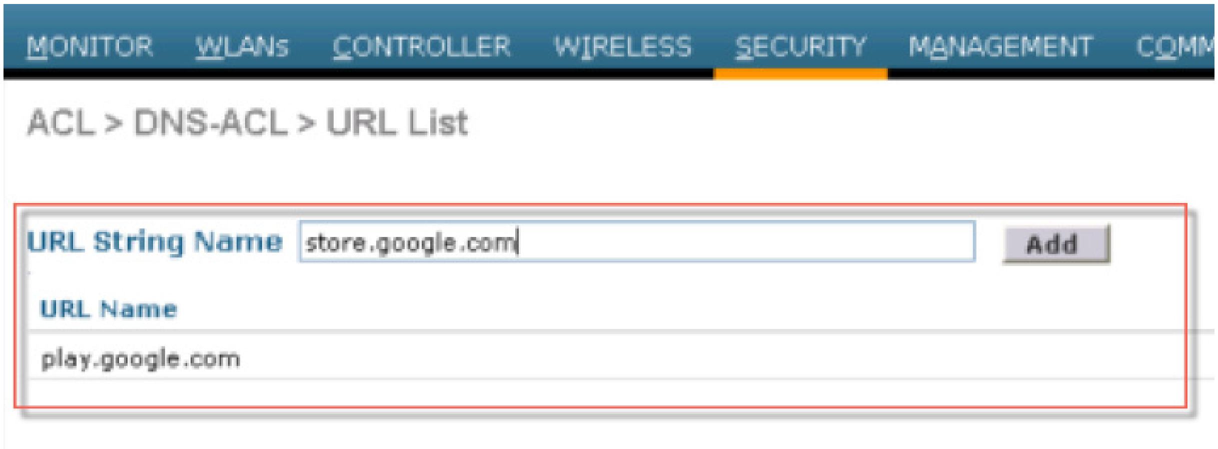
At the client authentication phase, the ISE server returns the pre-authentication ACL (url-redirect-acl). The DNS snooping is performed on the AP for each client until the registration is complete and the client is in SUPPLICANT PROVISIONING state. When the ACL configured with the URLs is received on the Cisco WLC, the CAPWAP payload is sent to the AP enabling DNS snooping on the client and the URLs to be snooped.

With URL snooping in place, the AP learns the IP address of the resolved domain name in the DNS response. If the domain name matches the configured URL, then the DNS response is parsed for the IP address, and the IP address is sent to the Cisco WLC as a CAPWAP payload. The Cisco WLC adds the IP address to the allowed list of IP addresses and thus the client can access the URLs configured.

Restrictions on DNS-based Access Control Lists

- Maximum of 10 URLs can be allowed for an access control list.
- For the Cisco WLC, 20 IP addresses are allowed for one client.
- Local authentication is not supported for FlexConnect APs.
- DNS-based ACLs are not supported on FlexConnect APs with Local Switching.
- DNS-based ACLs are not supported on Cisco 1130 and 1240 series access points.
- Authentication traffic has to go through the Cisco WLC to support this feature, even if DNS-based ACL is local to the AP.
- If a client is anchored, be it auto-anchor or after roaming, DNS-based ACLs do not work.
- DNS-based ACLs work only when RADIUS NAC (central web authentication or posture) are done on the SSID. DNS-based ACLs do not work with local web authentication or any other form of ACL other than a redirect-ACL used in the case of RADIUS NAC.

Figure 4-20 Illustration of DNS based ACL available for configuration on the WLC



URL String Name: store.google.com

URL Name
play.google.com

DHCP and ARP Protection

The WLC acts as a relay agent for WLAN client DHCP requests. In doing so, the WLC performs a number of checks to protect the DHCP infrastructure. The primary check is to verify that the MAC address included in the DHCP request matches the MAC address of the WLAN client sending the request. This protects against DHCP exhaustion attacks, by restricting a WLAN client to one DHCP request (IP address) for its own interface. The WLC by default does not forward broadcast messages from WLAN clients back out onto the WLAN, which prevents a WLAN client from acting as a DHCP server and spoofing incorrect DHCP information.

The WLC acts as an ARP proxy for WLAN clients by maintaining the MAC address-IP address associations. This allows the WLC to block duplicate IP address and ARP spoofing attacks. The WLC does not allow direct ARP communication between WLAN clients. This also prevents ARP spoofing attacks directed at WLAN client devices.

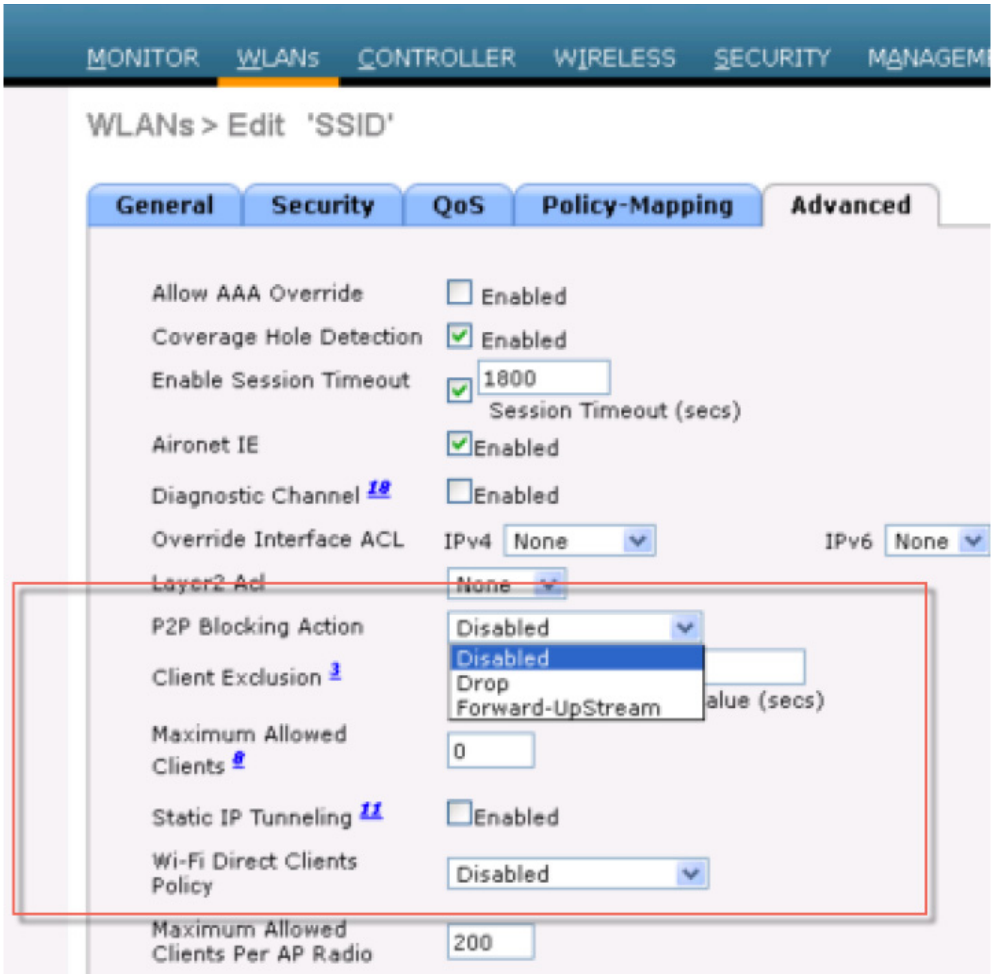
Peer-to-Peer Blocking

The WLC can be configured to block communication between clients on the same WLAN. This prevents potential attacks between clients on the same subnet by forcing communication through the router.

Figure 4-21 is the configuration screen for peer-to-peer blocking on the WLC.

Note This is a not a global setting on the WLC and applies to a specific WLANs in later releases.

Figure 4-21 Peer-to-Peer Blocking



WLANs > Edit 'SSID'

Allow AAA Override ☐ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel 18 ☐ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
P2P Blocking Action Disabled
- Disabled
- Drop
- Forward-UpStream

Client Exclusion 3 alue (secs)
Maximum Allowed Clients 8 0
Static IP Tunneling 11 ☐ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200

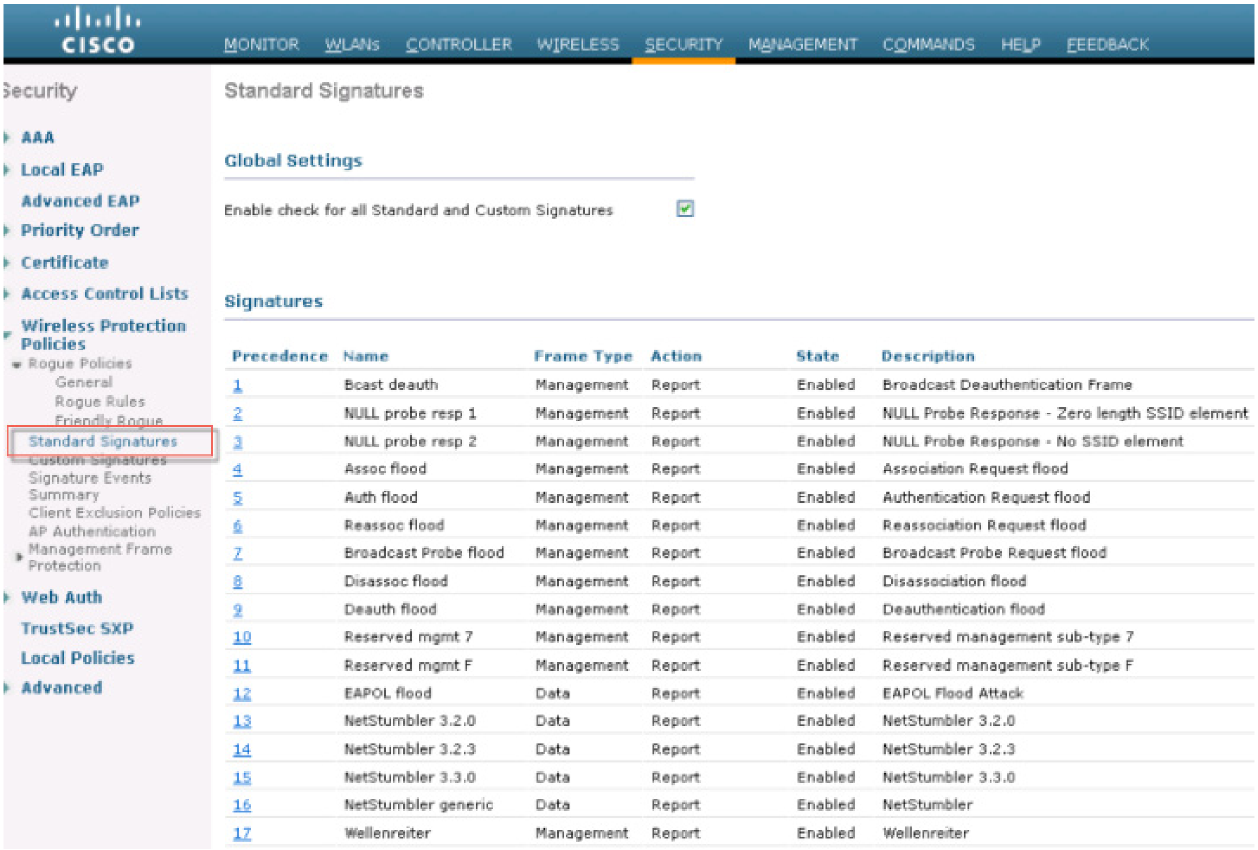
Wireless IDS

The WLC performs WLAN IDS analysis using information obtained from all of the connected APs, and reports detected attacks to WLC as well to the WCS. The Wireless IDS analysis is complementary to any analysis that can otherwise be performed by a wired network IDS system. The embedded Wireless IDS capability of the WLC analyzes 802.11and WLC-specific information that is not otherwise visible or available to a wired network IDS system.

The wireless IDS signature files used by the WLC are included in WLC software releases; however, they can be updated independently using a separate signature file. Custom signatures are displayed in the Custom Signatures window.

Figure 4-22 is the Standard Signatures window in the WLC.

Figure 4-22 Standard WLAN IDS Signatures



Standard Signatures

Global Settings

Enable check for all Standard and Custom Signatures ☑

Signatures

Precedence	Name	Frame Type	Action	State	Description
1	Bcast deauth	Management	Report	Enabled	Broadcast Deauthentication Frame
2	NULL probe resp 1	Management	Report	Enabled	NULL Probe Response - Zero length SSID element
3	NULL probe resp 2	Management	Report	Enabled	NULL Probe Response - No SSID element
4	Assoc flood	Management	Report	Enabled	Association Request flood
5	Auth flood	Management	Report	Enabled	Authentication Request flood
6	Reassoc flood	Management	Report	Enabled	Reassociation Request flood
7	Broadcast Probe flood	Management	Report	Enabled	Broadcast Probe Request flood
8	Disassoc flood	Management	Report	Enabled	Disassociation flood
9	Deauth flood	Management	Report	Enabled	Deauthentication flood
10	Reserved mgmt 7	Management	Report	Enabled	Reserved management sub-type 7
11	Reserved mgmt F	Management	Report	Enabled	Reserved management sub-type F
12	EAPOL flood	Data	Report	Enabled	EAPOL Flood Attack
13	NetStumbler 3.2.0	Data	Report	Enabled	NetStumbler 3.2.0
14	NetStumbler 3.2.3	Data	Report	Enabled	NetStumbler 3.2.3
15	NetStumbler 3.3.0	Data	Report	Enabled	NetStumbler 3.3.0
16	NetStumbler generic	Data	Report	Enabled	NetStumbler
17	Wellenreiter	Management	Report	Enabled	Wellenreiter

Cisco Adaptive Wireless Intrusion Prevention System

The Cisco Adaptive wireless Intrusion Prevention System (wIPS) is an advanced approach to wireless threat detection and performance management. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention. With a fully infrastructure-integrated solution, you can continually monitor wireless traffic on both the wired and wireless networks and use that network intelligence to analyze attacks from many sources to more accurately pinpoint and proactively prevent attacks rather than waiting until damage or exposure has occurred.

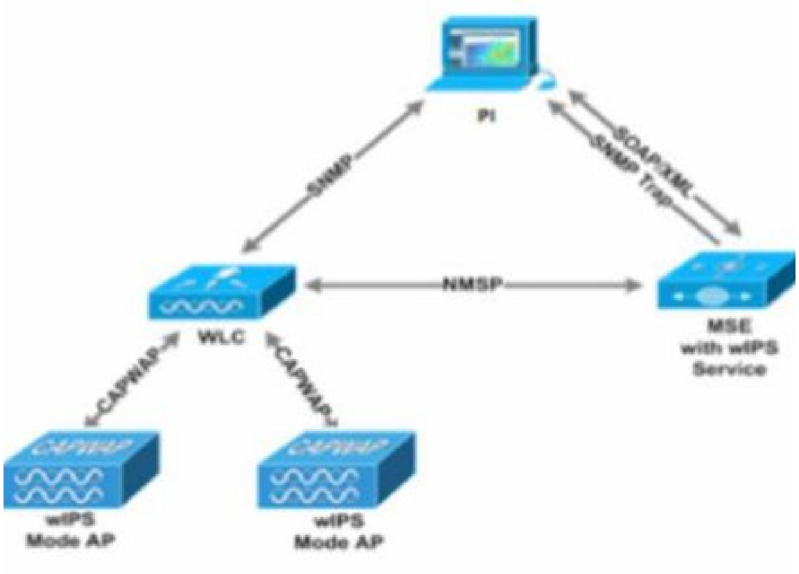
The Cisco Adaptive wIPS is enabled by the Cisco Mobility Services Engine (MSE), which centralizes the processing of intelligence collected by the continuous monitoring of Cisco Aironet access points. With Cisco Adaptive wIPS functionalities and Cisco Prime Infrastructure integration into the MSE, the wIPS service can configure, monitor, and report wIPS policies and alarms.

The Cisco Adaptive wIPS is not configured on the controller. Instead, the Prime Infrastructure forwards the profile configuration to the wIPS service, which forwards the profile to the controller. The profile is stored in flash memory on the controller and sent to access points when they join the controller. When an access point disassociates and joins another controller, it receives the wIPS profile from the new controller. Local mode or FlexConnect mode access points with a subset of wIPS capabilities is referred to as Enhanced Local Mode access point or ELM AP. You can configure an access point to work in wIPS mode if the access point is in any of the following modes described below.

wIPS Communication Protocols

To provide communication between each system component, a number of protocols are utilized:

- CAPWAP (Control and Provisioning of Wireless Access Points)—This protocol is utilized for communication between Access Points and controllers. It provides a bi-directional tunnel in which alarm information is shuttled to the controller and configuration information is pushed to the Access Point. CAPWAP control messages are DTLS encrypted and CAPWAP data has the option to be DTLS encrypted.
- NMSP (Network Mobility Services Protocol)—This protocol is used for communication between Wireless LAN Controllers and the Mobility Services Engine. In the case of a wIPS Deployment, this protocol provides a pathway for alarm information to be aggregated from controllers to the MSE and for wIPS configuration information to be pushed to the controller. This protocol is encrypted.
  - Controller TCP Port: 16113
- SOAP/XML (Simple Object Access Protocol)—This protocol is a method of communication between the MSE and PI. This protocol is used to distribute configuration parameters to the wIPS service running on the MSE.
  - oMSE TCP Port: 443
- SNMP (Simple Network Management Protocol)—This protocol is used to forward wIPS alarm information from the Mobility Services Engine to the Prime Infrastructure. It is also utilized to communicate rogue access point information from the Wireless LAN Controller to the Prime Infrastructure.



wIPS Deployment Modes

Beginning with the 7.4 Release, Cisco Adaptive Wireless IPS has three options for wIPS mode access points. To better understand the differences between the wIPS mode access points, lets discuss about each mode.

Local Mode with wIPS

Local Mode with wIPS provides wIPS detection “on-channel”, which means attackers will be detected on the channel that is serving clients. For all other channels, ELM provides best effort wIPS detection.

This means that every frame the radio would go “off-channel” for a short period of time. While "off-channel", if an attack occurs while that channel is scanned, the attack will be detected.

An example of Local Mode with wIPS on an AP3600, the 2.4 GHz radio is operating on channel 6. The AP will constantly monitor channel 6, any attacks on channel 6 will be detected and reported. If an attacker attacks channel 11, while the AP is scanning channel 11 “off-channel”, the attack will be detected.

The features of ELM are:

- Adds wIPS security scanning for 7x24 on channel scanning (2.4 GHz and 5 GHz), with best effort off channel support.
- The access point is additionally serving clients and with the G2 Series of Access Points enables CleanAir spectrum analysis on channel (2.4 GHz and 5 GHz).
- Adaptive wIPS scanning in data serving local and FlexConnect APs.
- Protection without requiring a separate overlay network.
- Supports PCI compliance for the wireless LANs.
- Full 802.11 and non-802.11 attack detection.
- Adds forensics and reporting capabilities.
- Flexibility to set integrated or dedicated MM APs.
- Pre-processing at APs minimize data backhaul (that is, works over very low bandwidth links).
- Low impact on the serving data.

Monitor Mode

Monitor Mode provides wIPS detection "off-channel", which means the access point will dwell on each channel for an extend period of time, this allows the AP to detect attacks on all channels. The 2.4GHz radio will scan all 2.4GHz channels, while the 5GHz channel scans all 5GHz channels. An additional access point would need to be installed for client access.

Some of the features of Monitor Mode are:

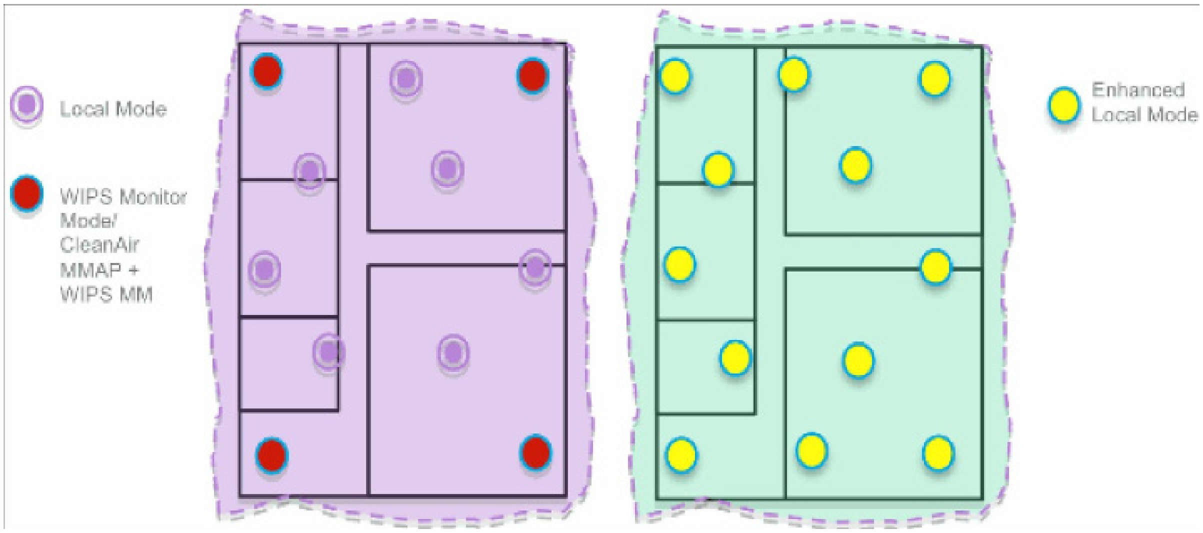
- The Monitor Mode Access Point (MMAP) is dedicated to operate in Monitor Mode and has the option to add wIPS security scanning of all channels (2.4GHz and 5GHz).
- The G2 Series of Access Points enable CleanAir spectrum analysis on all channels (2.4GHz and 5GHz).
- MMAPs do not serve clients.

Dedicated Monitor Mode versus ELM

Figure 4-23 illustrates a contrast between the standard deployments of wIPS monitor mode and APs with the ELM feature. The typical coverage range for both modes suggests:

- Dedicated wIPS monitor mode APs (shown in red in Figure 4-23) typically covers 15,000 to 35,000 square feet.
- APs with the ELM feature (shown in yellow in Figure 4-23) typically cover from 3,000 to 5,000 square feet.

Figure 4-23 Monitor Mode versus ELM



In the traditional wIPS deployment, a recommended ratio is 1 monitor mode AP to every 5 local mode APs (ratio can vary based on network design and expert guidance for best coverage). With ELM, you simply enable the ELM feature for all of the APs, effectively adding monitor mode wIPS operations to local data-serving mode AP while still maintaining performance.

AP 3600/3700 with Wireless Security Module (WSM): The Evolution of Wireless Security and Spectrum

A Cisco 3600 series Access point with the WSM module uses a combination of "on-channel" and "off-channel". This means that the AP3600 2.4 GHz and 5 GHz will scan the channel that they are serving clients and the WSM module would operate in monitor mode and scan all channels.

Some of the features of the WSM Module are:

- Industry's first Access Point enabling the ability to simultaneously Serve clients, wIPS security scan, and analyze the spectrum using CleanAir Technology.
- Dedicated 2.4 GHz and 5 GHz radio with its own antennas enabling 7x24 scanning of all wireless channels in the 2.4 GHz and 5 GHz bands.
- A single Ethernet infrastructure provides simplified operation with fewer devices to manage and optimized return on investment of the AP3600 wireless infrastructure and the Ethernet wired infrastructure.

On-Channel and Off-Channel Performance

When an AP visits a channel, the time the AP stays on that channel, to detect and classify an attack, is known as the dwell time. ELM primary feature operates effectively for on-channel attacks, without any compromise to the performance on data, voice and video clients, and services. In contrast, the local mode varies off-channel scanning providing minimal dwell time to detect and classify an attack.

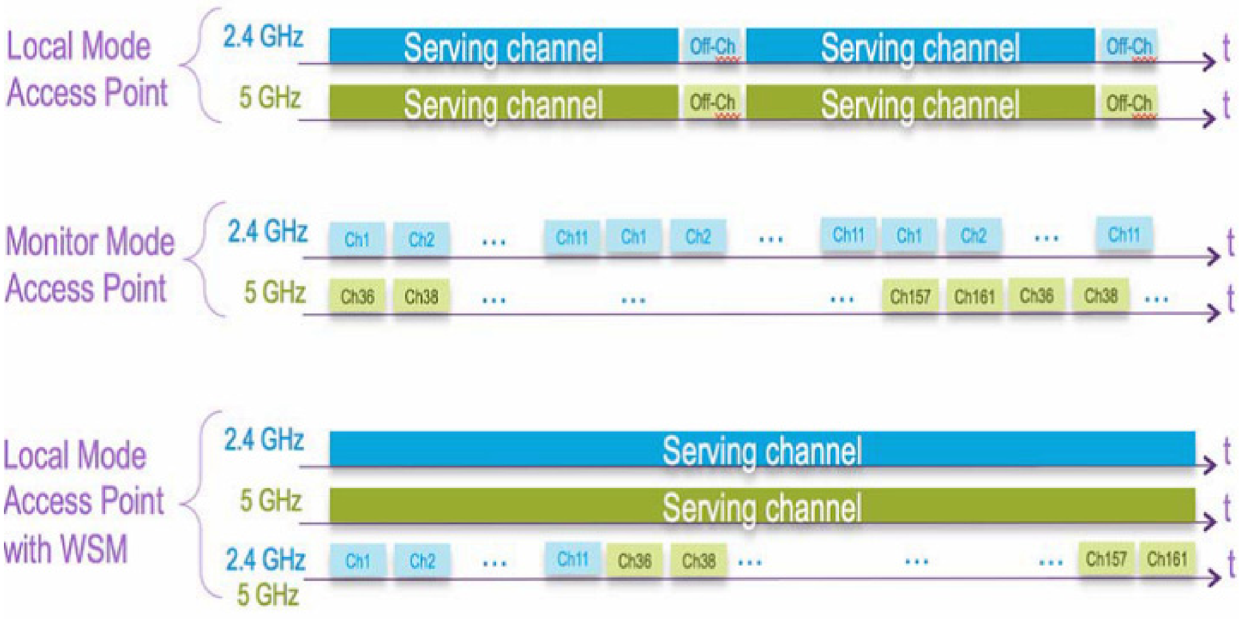
For example, due to radio resource management (RRM), when voice clients are associated to an AP scanning is deferred until the voice client is disassociated in order to ensure service is not affected. In this example, ELM detection during off-channel is considered best effort. Neighboring ELM APs operating on all/country/DCA channels increases effectiveness, hence the recommendation for enabling ELM on every local mode AP for maximum coverage protection. If your requirement is for dedicated scanning on all channels full-time, then we recommend deploying monitor mode APs.

Generally, the differences between local mode and monitor mode APs are:

- Local Mode AP—Serves WLAN clients with time slicing off-channel scanning, listens for 50 ms on each channel, and features configurable scanning for all/country/DCA channels.
- Monitor Mode AP—Does not serve WLAN clients, dedicated to scanning only, listens for 1.2 sec on each channel, and scans all channels.

The figure below explains the radio's behavior. When a radio is on its serving channel it is considered “on-channel”, when the radio is scanning other channels, it is considered "off-channel".

An AP in local mode is mostly "on-channel", making it difficult to detect attackers "off-channel". A monitor mode AP is always "off-channel", but cannot server clients, the WSM module provides a great combination of both.



ELM Across WAN Links

Cisco has optimized features in challenging topologies, such as deploying ELM APs across low bandwidth WAN links. The ELM feature involves pre-processing to determine attack signatures at the AP and is optimized to work over slower links. We recommend to test and measure the baseline to validate performance with ELM over WAN.

CleanAir Integration

Cisco CleanAir technology is a spectrum-aware, self-healing, and self-optimizing wireless network that mitigates the impact of wireless interference and offers performance protection for 802.11n networks.

The ELM feature compliments CleanAir operations with similar performance and benefits as monitor mode AP deployments, including these existing CleanAir spectrum-aware benefits:

- Dedicated silicon-level RF intelligence

- Spectrum-aware, self-healing, and self-optimizing
- Non-standard channel threat and interference detection and mitigation
- Non-Wi-Fi detection such as Bluetooth, microwave, cordless phones, and so forth
- Detect and locate RF layer DOS attacks such as RF jammers

ELM wIPS Alarm Flow

Attacks are only relevant when they occur on trusted APs. The ELM APs will detect an attack, then communicate, correlate, and report to the management system Cisco Prime Generally, the alarm flow process is:

1. Attack is launched against a trusted AP.
2. Detection on the AP with ELM feature communicates through CAPWAP to WLC.
3. Passed transparently to MSE via NMSP.
4. Log into wIPS database on MSE and send to the management system Cisco Prime by way of an SNMP trap.
5. Display at the management system Cisco Prime.

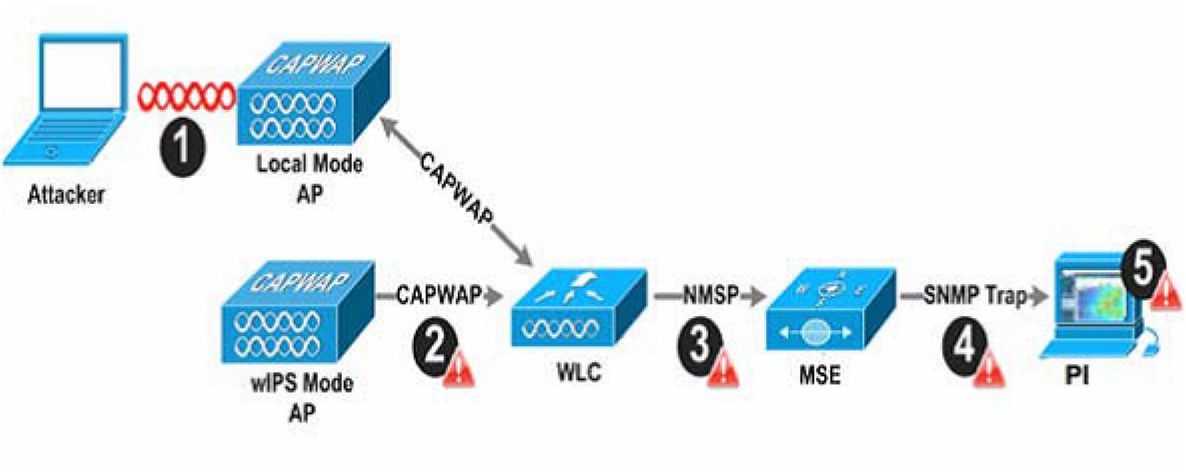
Cisco Adaptive wIPS Alarms

The controller supports five Cisco Adaptive wIPS alarms that serve as notifications for potential threats. You must enable these alarms based on your network topology using Cisco Prime Infrastructure. For more details on this, see the Cisco Prime Infrastructure User Guide.

- Device not protected by VPN—The controller generates an alarm when a wireless client and access point does not communicate over secure VPN, as all controller traffic must be routed through a VPN connection.
- WPA Dictionary Attack—The controller generates an alarm when a dictionary attack on the WPA security key occurs. The attack is detected before the initial handshake message between the client and the access point.
- WiFi Direct Session Detected—The controller generates an alarm when Wifi direct sessions of clients are detected with Wifi direct and prevents enterprise vulnerability.
- RSN Info Element Out-of-Bound Denial-of-Service—The controller generates an alarm when there are large values for RSN information element that results in an access point crash.
- DS Parameter Set DoS—The controller generates an alarm when confusion exists in the channel for the client while multiple channels overlap.

The Adaptive wIPS system follows a linear chain of communication to propagate attack information obtained from scanning the airwaves to the console of the Prime Infrastructure.

Figure 4-24 Threat Detection Alarm Flow



1. In order for an alarm to be triggered on the Cisco Adaptive wIPS system, an attack must be launched against a legitimate Access Point or Client. Legitimate Access Points and clients are discovered automatically in a Cisco Unified Wireless Network by 'trusting' devices broadcasting the same 'RF-Group' name. In this configuration, the system dynamically maintains a list of local-mode Access Points and their associated clients. The system can also be configured to 'trust' devices by SSID using the SSID Groups feature. Only attacks, which are considered harmful to the WLAN infrastructure, are propagated upwards to the rest of the system.
2. Once an attack has been identified by the wIPS Mode Access Point engine, an alarm update is sent to the Wireless LAN Controller and is encapsulated inside the CAPWAP control tunnel.
3. The Wireless LAN Controller will transparently forward the alarm update from the Access Point to the wIPS Service running on the Mobility Services Engine. The protocol used for this communication is NMSP.
4. Once received by the wIPS Service on the Mobility Services Engine, the alarm update will be added to the alarm database for archival and attack tracking. An SNMP trap is forwarded to the Prime Infrastructure containing the attack information. If multiple alarm updates are received referencing the same attack (for example, if multiple Access Points hear the same attack) only one SNMP trap will be sent to Prime Infrastructure.
5. The SNMP trap containing the alarm information is received and displayed by Prime Infrastructure.

Deployment Considerations - Required Components

The basic system components for a Cisco Adaptive wIPS system include:

- Access Points in wIPS Monitor Mode, in Local Mode with wIPS, or with a wireless security module
- Wireless LAN Controller(s)
- A Mobility Services Engine running the wIPS Service
- A Prime Infrastructure

The minimum code versions required for an Adaptive wIPS system:

- Available with Cisco Mobility Services Engine Software Release 5.2.xxx or later
- Requires Cisco Prime Infrastructure, version 1.3.
- Requires 7.2.xxx or later on Cisco Wireless LAN Controllers

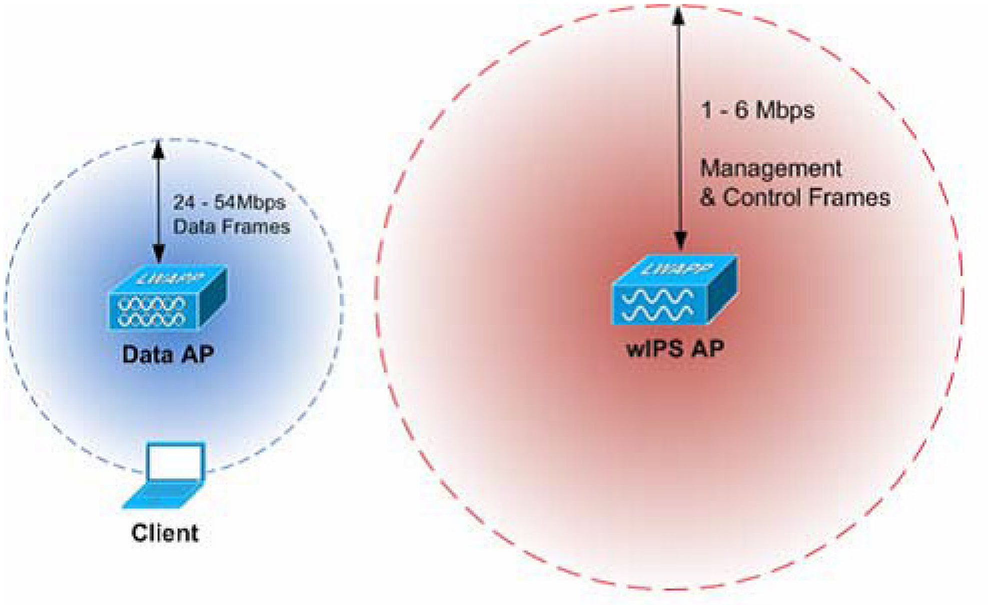
- Release 7.2 and later wireless IPS functionality requires monitor mode (that is, non-client-serving) access points
- Release 7.2.xxx and later wireless IPS functionality requires access points in local mode with wIPS (that is, client-serving)

The minimum code versions required for the Wireless Security Module (WSM):

- Wireless LAN Controller(s)—Version 7.4.XX or greater
- Cisco Prime Infrastructure—Version 1.3.XX or greater
- Mobility Services Engine—Version 7.4.XX or greater

How Many wIPS Access Points do I need?

Before deploying an Adaptive wIPS system, it is important to consider that the communications range of an access point's cell is less than the actual range at which frames may be received and decoded. The reason for this discrepancy is that an Access Point's communication range is limited by the weakest link - which in typical deployments is the WLAN client. Given that the output power of a WLAN client is intrinsically less than the Access Point's maximum, the range of the cell is restricted to the client's abilities. In addition, it is recommended practice to run Access Points at less than full power to build RF redundancy and load balancing into the wireless network. These aforementioned fact combined with the superior receive sensitivity of Cisco's Access Points allows the Adaptive wIPS system to be deployed with less access point density than the client serving infrastructure while still providing pervasive monitoring.



As depicted in the above diagram, a wIPS deployment is based on hearing 802.11 management and control frames which are used by a majority of attacks to cause harm. This is in contrast to a data Access Points deployment that is surveyed to provide higher throughput data rates anywhere from 24Mbps to 54Mbps.

There are numerous factors that go into deciding exactly the number of wIPS Access Points that are required for a specific environment. Given that each prospective deployment's security requirements and environmental conditions are different, there is no hard and fast rule that will address the needs of every deployment but a few generalized guidelines must be taken into account.

The main factors, which affect the number of wIPS Access Points required, are as follows.

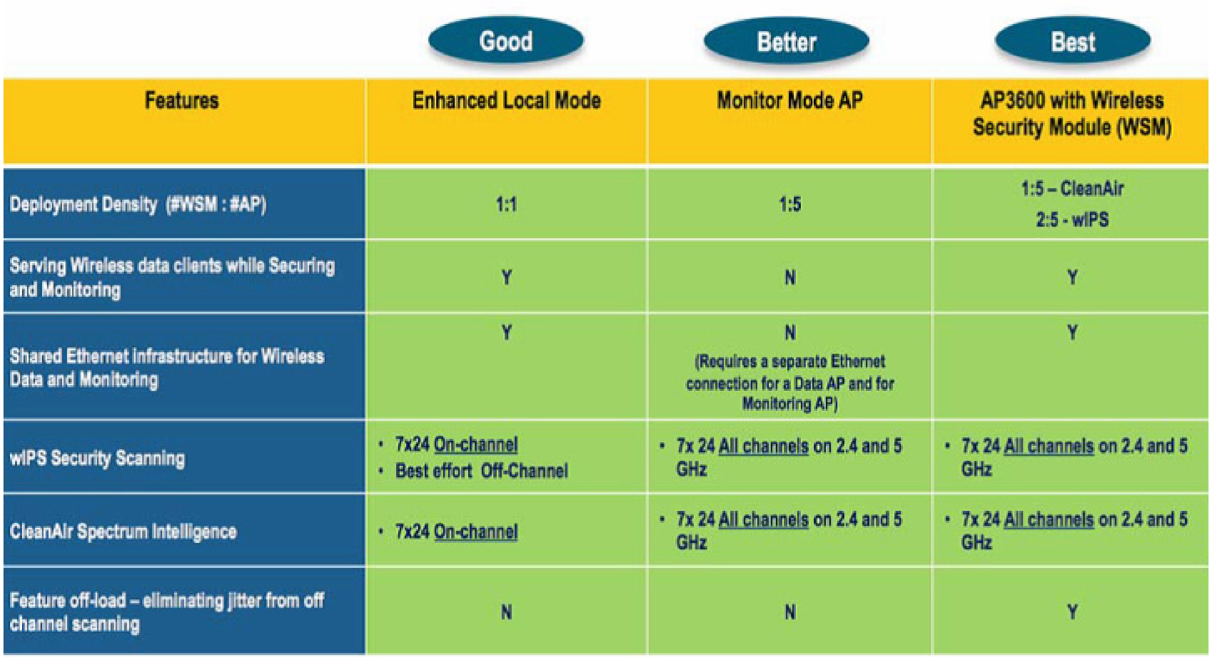
Access Point Density Recommendations

The square footage of access point coverage can be measured based on frequency and environment, but with the newer wIPS modes, other factors also contribute to wIPS access point density recommendations. All access point modes can monitor the same distance, but due to the reasons below, we recommend to deploy each mode with a different density.

Access Points in local mode with wIPS are geared towards serving clients. For local mode with wIPS deployments, it is recommended for every access point be put in local mode with wIPS.

For monitor mode access points, we recommend that a ratio of 1:5 local mode to monitor mode access points.

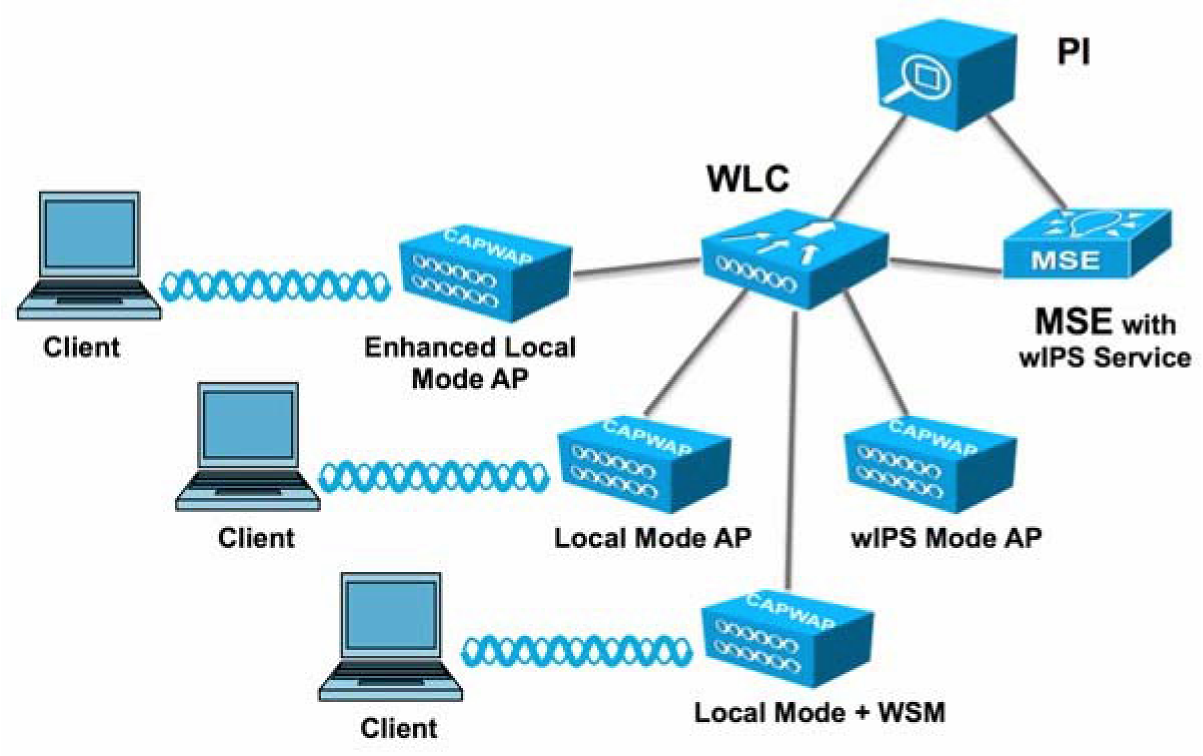
Finally for the WSM module, there is a single radio monitoring all channels on both the 2.4 GHz and 5 GHz band. Since radio has additional channels to scan, it is recommended that the WSM module be deployed with a 2:5 density to speed up detection time.



	Good	Better	Best
Features	**Enhanced Local Mode**	**Monitor Mode AP**	**AP3600 with Wireless Security Module (WSM)**
Deployment Density (#WSM : #AP)	1:1	1:5	1:5 – CleanAir 2:5 - wIPS
Serving Wireless data clients while Securing and Monitoring	Y	N	Y
Shared Ethernet infrastructure for Wireless Data and Monitoring	Y	N (Requires a separate Ethernet connection for a Data AP and for Monitoring AP)	Y
wIPS Security Scanning	• 7x24 On-channel • Best effort Off-Channel	• 7x 24 All channels on 2.4 and 5 GHz	• 7x 24 All channels on 2.4 and 5 GHz
CleanAir Spectrum Intelligence	• 7x24 On-channel	• 7x 24 All channels on 2.4 and 5 GHz	• 7x 24 All channels on 2.4 and 5 GHz
Feature off-load – eliminating jitter from off channel scanning	N	N	Y

wIPS Integrated in a Cisco Unified Wireless Network

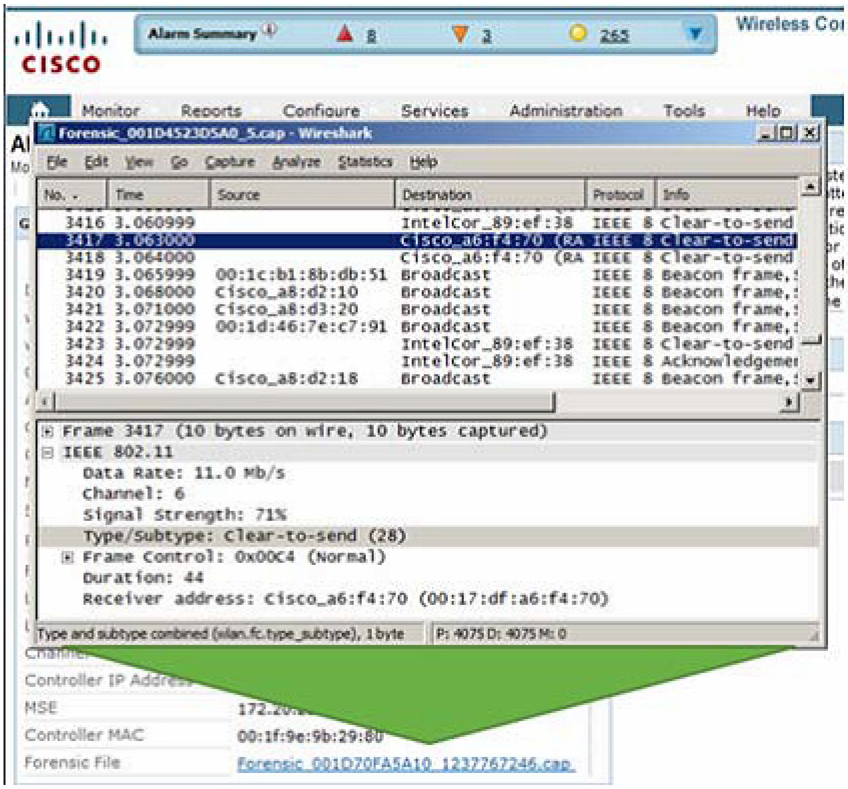
An integrated wIPS deployment is a system design in which non-wIPS Mode Access Points and wIPS Mode Access Points are intermixed on the same controller(s) and managed by the same Prime Infrastructure. This can be any combination of local mode, flex connect mode, local mode with wIPS, monitor mode, and 3600 series Access points with the WSM module. Overlaying wIPS protection and data shares many of the components including controllers and Prime Infrastructure thus reducing duplicate infrastructure costs.



Forensics

The Cisco Adaptive wIPS system provides the ability to capture attack forensics for further investigation and troubleshooting purposes. At a base level, the forensics capability is a toggle-based packet capture facility, which provides the ability to log and retrieve a set of wireless frames. This feature is enabled on a per attack basis from within the wIPS profile configuration of PI.

Once enabled, the forensics feature is triggered once a specific attack alarm is seen over the airwaves. The forensic file will be created based on the packets contained within the buffer of the wIPS Mode AP that triggered the original alarm. This file is transferred to the Wireless LAN Controller via CAPWAP, which then forwards the forensic file via NMSP to the wIPS Service running on the Mobility Services Engine. The file is stored within the forensic archive on the MSE until the user configured disk space limit for forensics is reached. By default this limit is 20 GB, which when reached will cause the oldest forensic files to be removed. Access to the forensic file can be obtained by opening the alarm on the Prime Infrastructure, which contains a hyperlink to the forensic file. The files are stored as a '.CAP' file format which can be opened by either WildPacket's Omnipeek, AirMagnet Wi-Fi Analyzer, Wireshark or any other packet capture program which supports this format. See Wireshark for detailed information.



```
No. -  Time       Source             Destination         Protocol Info
  3416 3.060999                      IntelCor_89:ef:38   IEEE 8 Clear-to-send
  3417 3.063000                      Cisco_a6:f4:70 (RA  IEEE 8 Clear-to-send
  3418 3.064000                      Cisco_a6:f4:70 (RA  IEEE 8 Clear-to-send
  3419 3.065999   00:1c:b1:8b:db:51  Broadcast           IEEE 8 Beacon frame,
  3420 3.068000   Cisco_a8:d2:10     Broadcast           IEEE 8 Beacon frame,
  3421 3.071000   Cisco_a8:d3:20     Broadcast           IEEE 8 Beacon frame,
  3422 3.072999   00:1d:46:7e:c7:91  Broadcast           IEEE 8 Beacon frame,
  3423 3.072999                      IntelCor_89:ef:38   IEEE 8 Clear-to-send
  3424 3.072999                      IntelCor_89:ef:38   IEEE 8 Acknowledgemen
  3425 3.076000   Cisco_a8:d2:18     Broadcast           IEEE 8 Beacon frame,

⊞ Frame 3417 (10 bytes on wire, 10 bytes captured)
⊟ IEEE 802.11
     Data Rate: 11.0 Mb/s
     Channel: 6
     Signal Strength: 71%
     Type/Subtype: Clear-to-send (28)
   ⊞ Frame Control: 0x00C4 (Normal)
     Duration: 44
     Receiver address: Cisco_a6:f4:70 (00:17:df:a6:f4:70)

Type and subtype combined (wlan.fc.type_subtype), 1 byte    P: 4075 D: 4075 M: 0
```

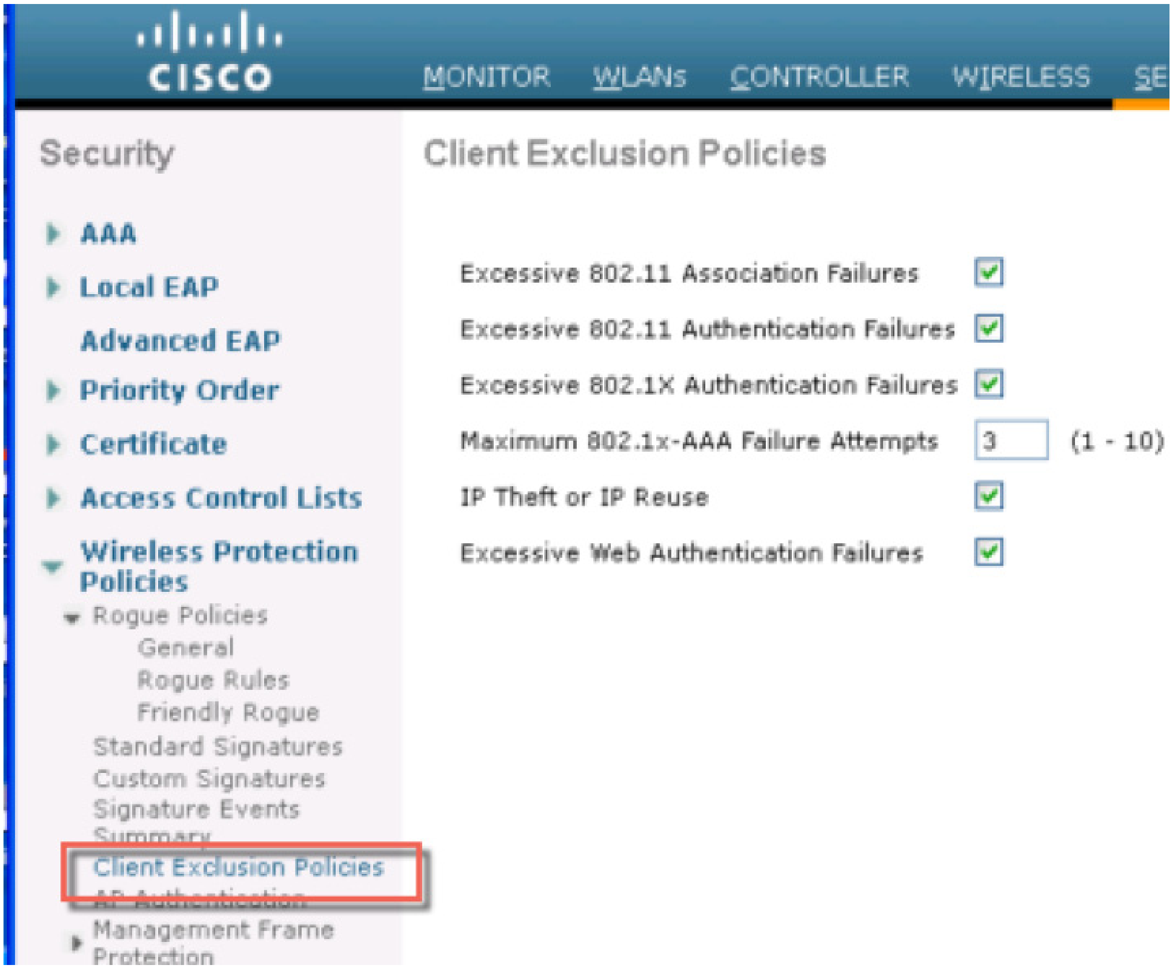
Controller IP Address
MSE 172.20.
Controller MAC 00:1f:9e:9b:29:80
Forensic File Forensic_001D70FA5A10_1237767246.cap

Client Exclusion

In addition to Wireless IDS, the WLC is able to take additional steps to protect the WLAN infrastructure and WLAN clients. The WLC is able to implement policies that exclude WLAN clients whose behavior is considered threatening or inappropriate. Figure 4-25 shows the Exclusion Policies window, containing the following currently supported client exclusion policies:

- Excessive 802.11 association failures—Possible faulty client or DoS attack
- Excessive 802.11 authentication failures—Possible faulty client or DoS attack
- Excessive 802.1X authentication failures—Possible faulty client or DoS attack
- Maximum 802.1X —AAA Failure Attempts (1-10)
- IP theft or IP reuse—Possible faulty client or DoS attack
- Excessive web authentication failures—Possible DoS or password-cracking attack

Figure 4-25 Client Exclusion Policies



Client Exclusion Policies

Excessive 802.11 Association Failures ☑
Excessive 802.11 Authentication Failures ☑
Excessive 802.1X Authentication Failures ☑
Maximum 802.1x-AAA Failure Attempts 3 (1 - 10)
IP Theft or IP Reuse ☑
Excessive Web Authentication Failures ☑

Managing Rogue Devices and Policies

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of Clear to Send (CTS) frames. This action mimics an access point, informing a particular client to transmit, and instructing all the other clients to wait, which results in legitimate clients being unable to access network resources. Wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Rogue Location Discovery Protocol

Cisco Rogue Location Discovery Protocol (RLDP) is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends de-authentication messages to all connected clients and then shuts down the radio interface. Then, it associates to the rogue AP as a client. The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature. RLDP has 100% accuracy in rouge AP detection. It detects Open APs and NAT APs.

Detecting Rogue Devices

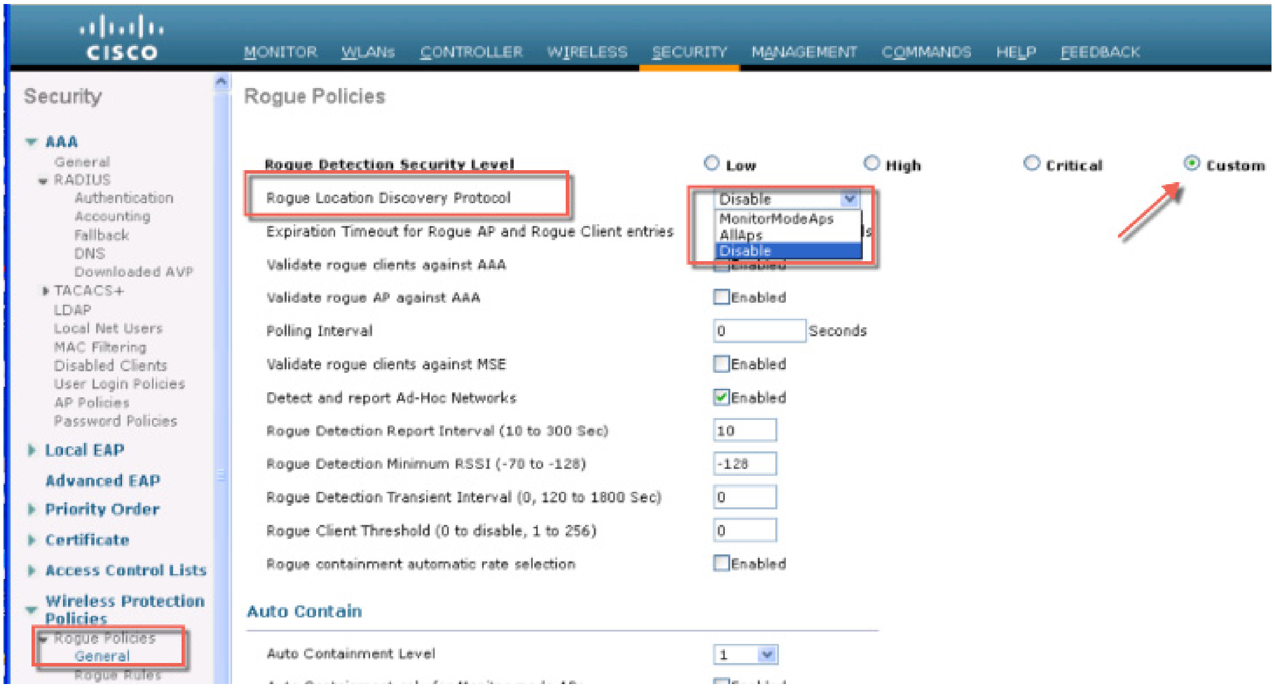
The controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) and the rogue detector mode access point is connected to determine if the rogue is attached to your network.

Controller initiates RLDP on rogue devices that have open authenticated and configured. If RLDP uses Flexconnect or local mode access points, then clients are disconnected for that moment. After the RLDP cycle, the clients are reconnected to the access points. As and when rogue access points are seen (auto-configuration), the RLDP process is initiated.

You can configure the controller to use RLDP on all the access points or only on the access points configured for the monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded radio frequency (RF) space, allowing monitoring without creating unnecessary interference and without affecting the regular data access point functionality. If you configure the controller to use RLDP on all the access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to contain the detected rogue either manually or automatically.

RLDP detects on wire presence of the rogue access points that are configured with open authentication only once, which is the default retry configuration.

Figure 4-26 Illustration of the RLDP configuration



Rogue Policies

Rogue Detection Security Level ○ Low ○ High ○ Critical ● Custom

Rogue Location Discovery Protocol: Disable (MonitorModeAps / AllAps / Disable)

Expiration Timeout for Rogue AP and Rogue Client entries

Validate rogue clients against AAA ☐ Enabled

Validate rogue AP against AAA ☐ Enabled

Polling Interval: 0 Seconds

Validate rogue clients against MSE ☐ Enabled

Detect and report Ad-Hoc Networks ☑ Enabled

Rogue Detection Report Interval (10 to 300 Sec): 10

Rogue Detection Minimum RSSI (-70 to -128): -128

Rogue Detection Transient Interval (0, 120 to 1800 Sec): 0

Rogue Client Threshold (0 to disable, 1 to 256): 0

Rogue containment automatic rate selection ☐ Enabled

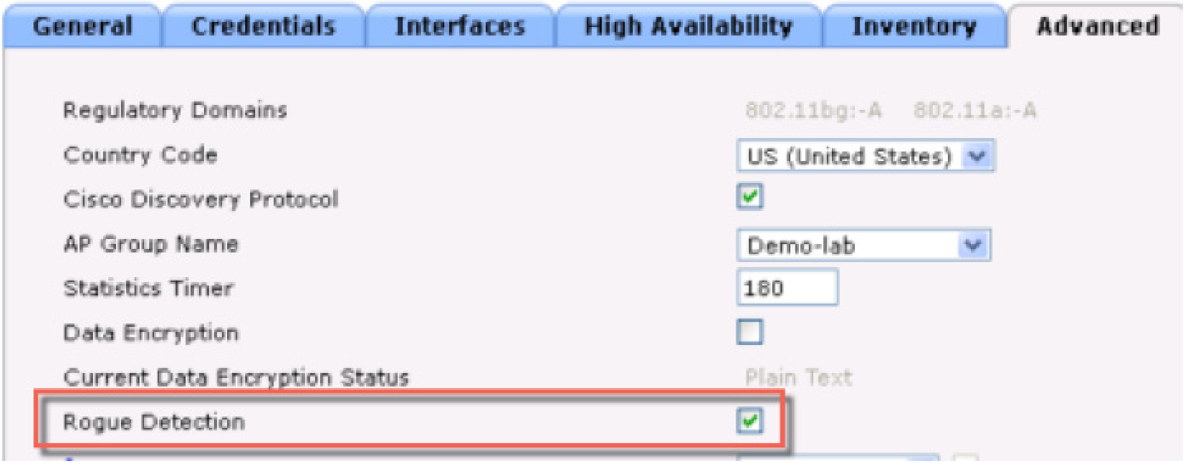
Auto Contain

Auto Containment Level: 1

A rogue access point is moved to a contained state either automatically or manually. The controller selects the best available access point for containment and pushes the information to the access point. The access point stores the list of containments per radio. For auto containment, you can configure the controller to use only the monitor mode access point.

Rogue Detection Policies Parameters

Make sure that rogue detection is enabled for the corresponding access points. Rogue detection is enabled by default for all access points joined to the controller (except for OfficeExtend access points).



Regulatory Domains 802.11bg:-A 802.11a:-A

Country Code US (United States)

Cisco Discovery Protocol ☑

AP Group Name Demo-lab

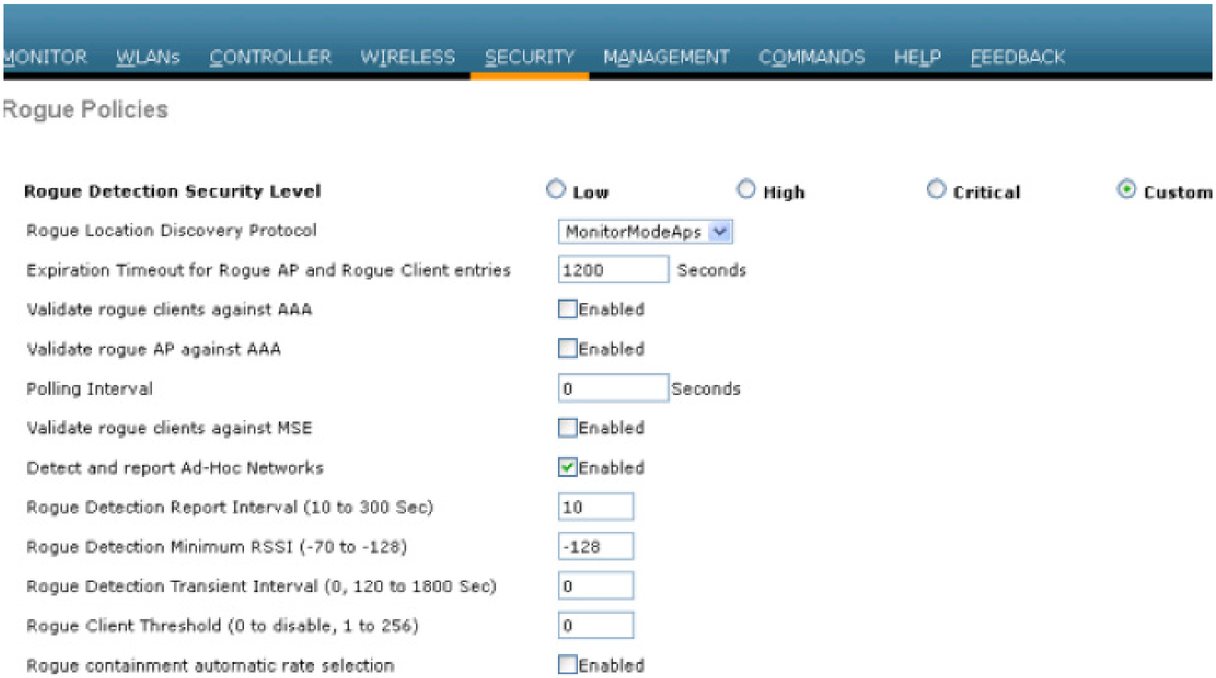
Statistics Timer 180

Data Encryption ☐

Current Data Encryption Status Plain Text

Rogue Detection ☑

1. **Rogue Detection Security Level** following options:
    - **Low**—Basic rogue detection for small-scale deployments.
    - **High**—Basic rogue detection with auto containment for medium-scale deployments.
    - **Critical**—Basic rogue detection with auto containment and RLDP for highly sensitive deployments.
    - **Custom**—For auto RLDP, the security level should be set to Custom mode. There should not be any scheduling for RLDP even in the Custom mode.
2. **Rogue Location Discovery Protocol** AP options:
    - **Disable**—Disables RLDP on all the access points. This is the default value.
    - **All APs**—Enables RLDP on all the access points.
    - **Monitor Mode APs**—Enables RLDP only on the access points in the monitor mode.



Rogue Policies

Rogue Detection Security Level ○ Low ○ High ○ Critical ● Custom

Rogue Location Discovery Protocol: MonitorModeAps

Expiration Timeout for Rogue AP and Rogue Client entries: 1200 Seconds

Validate rogue clients against AAA: ☐ Enabled

Validate rogue AP against AAA: ☐ Enabled

Polling Interval: 0 Seconds

Validate rogue clients against MSE: ☐ Enabled

Detect and report Ad-Hoc Networks: ☑ Enabled

Rogue Detection Report Interval (10 to 300 Sec): 10

Rogue Detection Minimum RSSI (-70 to -128): -128

Rogue Detection Transient Interval (0, 120 to 1800 Sec): 0

Rogue Client Threshold (0 to disable, 1 to 256): 0

Rogue containment automatic rate selection: ☐ Enabled

3. **Rogue Client Validation**—use the AAA, MSE server or local database to validate if rogue clients are valid clients, select the Validate Rogue Clients.

   MSE responds with information about whether the rogue client is a valid learned client or not. The controller can contain or consider the rogue client as a threat.

4. **Detect and Report Ad-Hoc Networks**—if necessary select ad hoc rogue detection and reporting.
5. **Rogue Detection Report Interval**—the time interval, in seconds, at which APs should send the rogue detection report to the controller. The valid range is 10 seconds to 300 seconds, and the default value is 10 seconds.
6. **Rogue Detection Minimum RSSI**—the minimum Received Signal Strength Indicator (RSSI) value that a rogue entry should have for APs to detect the rogue and for a rogue entry to be created in the controller. The valid range is -128 dBm to -0 dBm, and the default value is 0 dBm. This feature is applicable to all the AP modes. There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.
7. **Rogue Detection Transient Interval**—time interval at which a rogue should be scanned for by the AP after the first time the rogue is scanned. After the rogue is scanned for consistently, updates are sent periodically to the controller. Thus, the APs filter the transient rogues, which are active for a very short period and are then silent. The valid range is between 120 seconds to 1800 seconds, and the default value is 0. The rogue detection transient interval is applicable to the monitor mode APs only.

This feature has the following advantages:

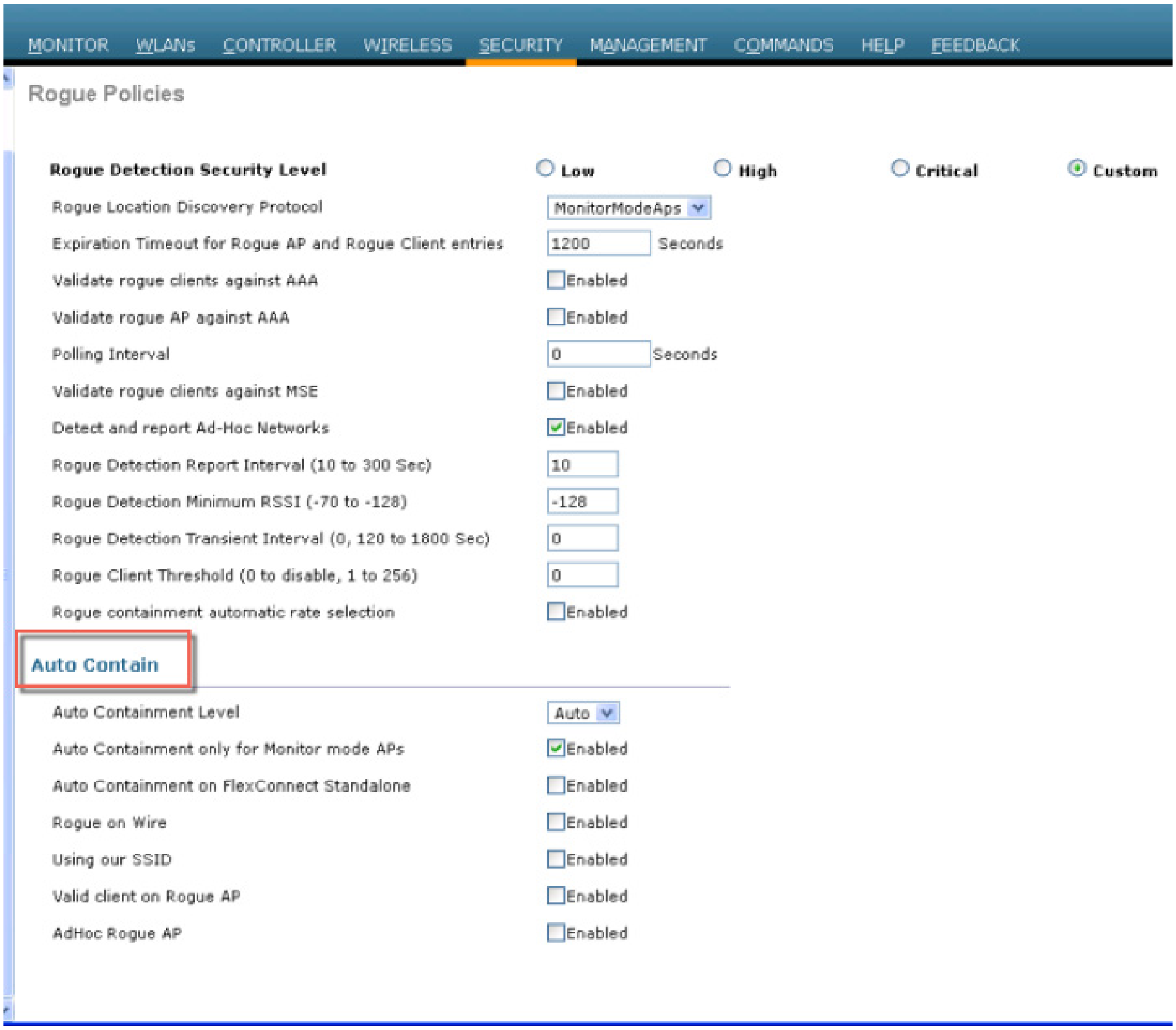
- Rogue reports from APs to the controller are shorter.
- Transient rogue entries are avoided in the controller.
- Unnecessary memory allocation for transient rogues are avoided.

8. **Rogue Client Threshold**—the threshold value. A value of 0 disables the rogue client threshold parameter.
9. **Rogue Containment Automatic Rate Selection**—Using this option, you can optimize the rate to use the best rate for the target rogue. The AP selects the best rate based on rogue RSSI.
10. **Containment**—If you want the controller to automatically contain certain rogue devices, enable the following parameters.
    - **Auto Containment Level**—Set the auto containment level. By default, the auto containment level is set to **1**. If you choose **Auto**, the controller dynamically chooses the number of APs required for effective containment.
    - **Auto Containment only for Monitor mode APs**—Configure the monitor mode access points for auto-containment.
    - **Auto Containment on FlexConnect Standalone**—Standalone StaFlexConnect Standalone mode access points for auto containment.
    - The auto-containment is continued if it was configured when the AP was in connected FlexConnect mode. After the standalone AP reassociates with the controller, auto containment is stopped and the future course of action is determined by the configuration on the controller that the AP is associated with. You can also configure auto containment on the ad hoc SSIDs and managed SSIDs on FlexConnect APs.
    - **Rogue on Wire**—Configure the auto containment of rogues that are detected on the wired network.
    - **Using Our SSID**—Configure the auto containment of rogues that are advertising your network's SSID. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.
    - **Valid Client on Rogue AP**—Valid Client on Rogue APed, the controller only generates an alarm when such a rogue associated. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.
    - **AdHoc Rogue AP**—Rogue APue AP this parameter unselected, the controller only generates an alarm when such this parameter unselected, the controller only generates an alarm when such a network is detected.

Caution When you select any of the Auto Contain parameters and click **Apply**, the following message is displayed:
"**Using this feature may have legal consequences. Do you want to continue?**"
The 2.4-GHz and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

Figure 4-27 Illustrates Rogue Policies configuration options; RLDP security levels and enablement on the Aps; also it shows the validation configuration against AAA or MSE.

Figure 4-27 Configuring Rogue Policies



Rogue Policies

Rogue Detection Security Level ○ Low ○ High ○ Critical ● Custom

Rogue Location Discovery Protocol: MonitorModeAps

Expiration Timeout for Rogue AP and Rogue Client entries: 1200 Seconds

Validate rogue clients against AAA: ☐ Enabled

Validate rogue AP against AAA: ☐ Enabled

Polling Interval: 0 Seconds

Validate rogue clients against MSE: ☐ Enabled

Detect and report Ad-Hoc Networks: ☑ Enabled

Rogue Detection Report Interval (10 to 300 Sec): 10

Rogue Detection Minimum RSSI (-70 to -128): -128

Rogue Detection Transient Interval (0, 120 to 1800 Sec): 0

Rogue Client Threshold (0 to disable, 1 to 256): 0

Rogue containment automatic rate selection: ☐ Enabled

Auto Contain

Auto Containment Level: Auto

Auto Containment only for Monitor mode APs: ☑ Enabled

Auto Containment on FlexConnect Standalone: ☐ Enabled

Rogue on Wire: ☐ Enabled

Using our SSID: ☐ Enabled

Valid client on Rogue AP: ☐ Enabled

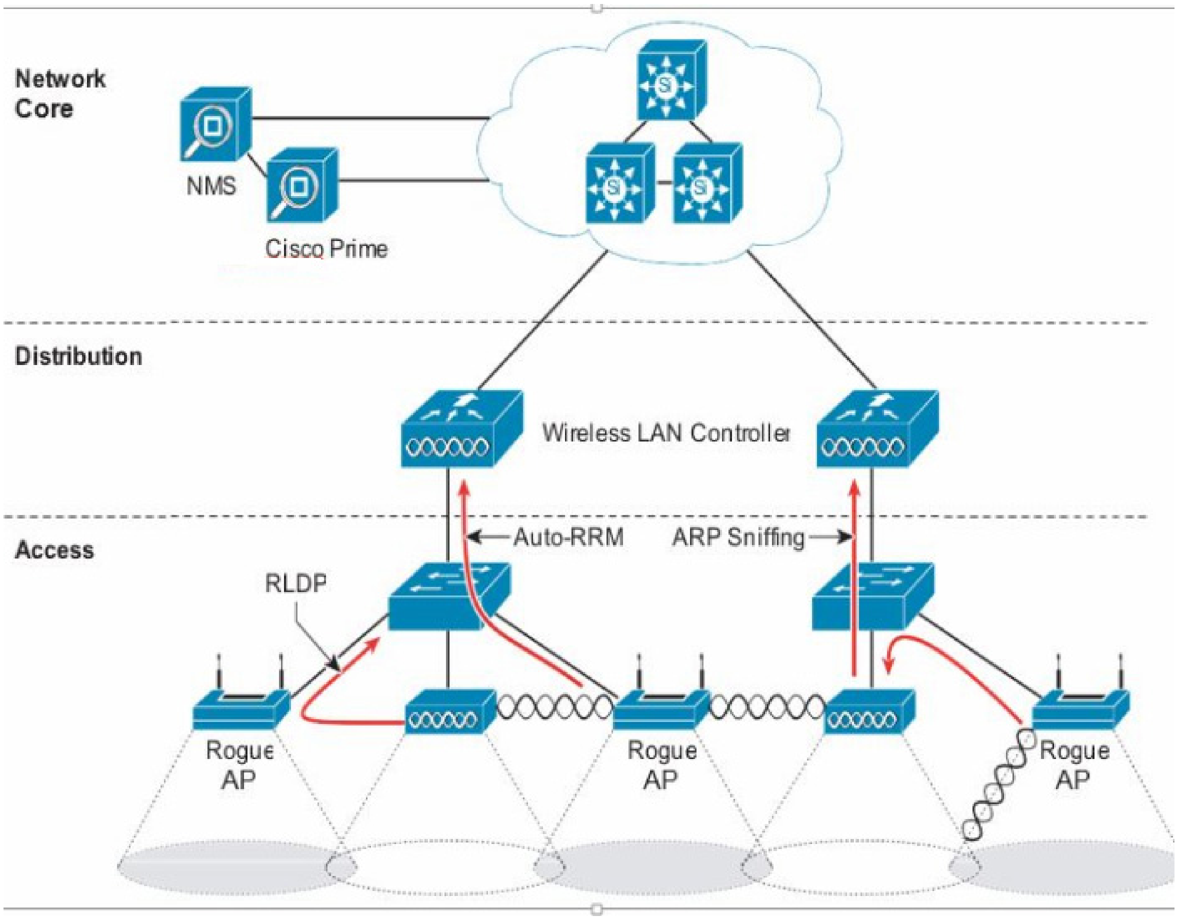
AdHoc Rogue AP: ☐ Enabled

Rogue AP

The Cisco Unified Wireless Networking solution, as shown in Figure 4-28, provides a complete solution for rogue APs. This solution provides:

- Air/RF detection—Detection of rogue devices by observing/sniffing beacons and 802.11 probe responses.
- Rogue AP location—Use of the detected RF characteristics and known properties of the managed RF network to locate the rogue device.
- Wire detection—A mechanism for tracking/correlating the rogue device to the wired network.
- Rogue AP isolation—A mechanism to prevent client connection to a rogue AP.

Figure 4-28 Unified Wireless Network Rogue AP Detection



Air/RF Detection

The two AP RF detection deployment models are:

- Standard AP deployment
- Monitor mode AP deployment

Both deployment models support RF detection and are not limited to rogue APs, but can also capture information upon detection of ad-hoc clients and rogue clients (the users of rogue APs). An AP that is configured for monitor mode is dedicated to scanning the RF channels and does not support client association or data transmission.

When searching for rogue APs, an AP goes off channel for 50 ms to listen for rogue clients, and to monitor noise and channel interference. The channels scanned are configured in the global WLAN network parameters for 802.11a and 802.11b/g.

Any detected prospective rogue client(s) and/or access points are sent to the controller to gather the following information:

- Rogue AP MAC address

- Rogue AP name
- Rogue connected client(s) MAC address
- Whether the frames are protected with WPA, WEP and WEP2
- The preamble
- Signal-to-noise ratio (SNR)
- Received signal strength indication (RSSI)
- Switchport tracing

The prospective rogue client/AP is not labeled a rogue until the WLC receives another report from a trusted AP or until the completion of a second detection cycle. The trusted AP moves to the same channel, as the prospective rogue, to monitor for rogue client/AP, noise, or interference. If the same client/AP is detected a second time, they are then labeled as rogue on the WLC.

Once labeled as a rogue, the WLC determines if this rogue is attached to the local network or is simply a neighboring AP. In either case, an AP that is not part of the managed Cisco Unified Wireless Network is considered a rogue.

In monitor mode, the trusted AP does not carry user traffic; it is dedicated to scanning channels. This mode of deployment is most common when a customer does not want to support WLAN services in a particular area, but wants to monitor that area for rogue APs and rogue clients.

Location

The location features of Cisco Prime Infrastructure can be used to provide a floor plan indicating the approximate location of a rogue AP. The floor plan displays the location of all legitimate APs, and highlights the location of a rogue AP with the skull-and-crossbones icon. For additional information on the Cisco Unified Wireless Network location features, see Cisco Wireless Location Appliance.

Wire Detection

Situations can exist where the Cisco Prime Infrastructure rogue location feature is not effective, such as in branch offices with only a few APs or where floor plan information might not be available. In these cases, the Cisco Unified Wireless Network solution offers two wire-based detection options:

- Rogue detector AP
- Rogue Location Discovery Protocol (RLDP)

If an AP is configured as a rogue detector, its radio is turned off and its role is to listen on the wired network for MAC addresses of clients associated to rogue APs; that is, *rogue clients*. The rogue detector listens for ARP packets that include rogue client MAC addresses. When it detects one of these ARPs, it reports this to the WLC, providing verification that the rogue AP is attached to the same network as the Cisco Unified Wireless Network.

To maximize the likelihood of capturing ARP information, the rogue AP detector is connected to all available broadcast domains using a Switched Port Analyzer (SPAN) port. Multiple rogue AP detector APs can be deployed to capture the various aggregated broadcast domains that exist on a typical network.

If a rogue client resides behind a wireless router (a common home WLAN device), its ARP requests are not seen on the wired network, so an alternative to the rogue detector AP method is needed. Additionally, rogue detector APs might not be practical for some deployments because of the large number of broadcast domains to be monitored (such as in the main campus network).

The RLDP option can aid in these situations. In this case, a standard AP, upon detecting a rogue AP, can attempt to associate with the rogue AP as a client and send a test packet to the controller, which requires the AP to stop behaving as a standard AP and temporarily go into client mode. This action confirms that the rogue AP in question is actually on the network, and provides IP address information that indicates its logical location in the network. Given the difficulties in deriving location information in branch offices coupled with the likelihood of a rogue being located in multi-tenant buildings, rogue AP detector and RLDP are useful tools that augment location-based rogue AP detection.

Switch Port Tracing

The Cisco Prime Infrastructure provides rogue access point detection by retrieving information from the controller. The rogue access point table is populated with any detected BSSID addresses from any frames that are not present in the *neighbor list*. A neighbor list contains the known BSSID addresses of validated APs or *neighbors*. At the end of a specified interval, the contents of the rogue table are sent to the controller in a CAPWAP Rogue AP Report message. With this method, the Cisco Prime Infrastructure simply gathers the information received from controllers. Additionally, you can also incorporate auto or manual switch port tracing (SPT) of wired rogue access point switch ports. The auto SPT is preferable for a large wireless network.

Auto SPT launches automatically when a rogue AP is reported to the Cisco Prime Infrastructure. The auto SPT provides a quicker scan based on the wired location association of the rogue AP. The Cisco Prime Infrastructure allows you to configure the criteria for auto SPT and auto containment so that you can run a trace and contain the detected rogue access points on the wire.

When the multiple controllers report that a rogue AP should be auto contained, the Cisco Prime Infrastructure finds the controller that reports the strongest RSSI and sends the containment request to the controller.

Rogue AP Containment

Rogue AP connected clients, or rogue ad-hoc connected clients, can be contained by sending 802.11 de-authentication packets from nearby APs. This should be done only after steps have been taken to ensure that the AP is truly a rogue AP, because it is illegal to do this to a legitimate AP in a neighboring WLAN. This is why the automatic rogue AP containment feature is removed from the solution.

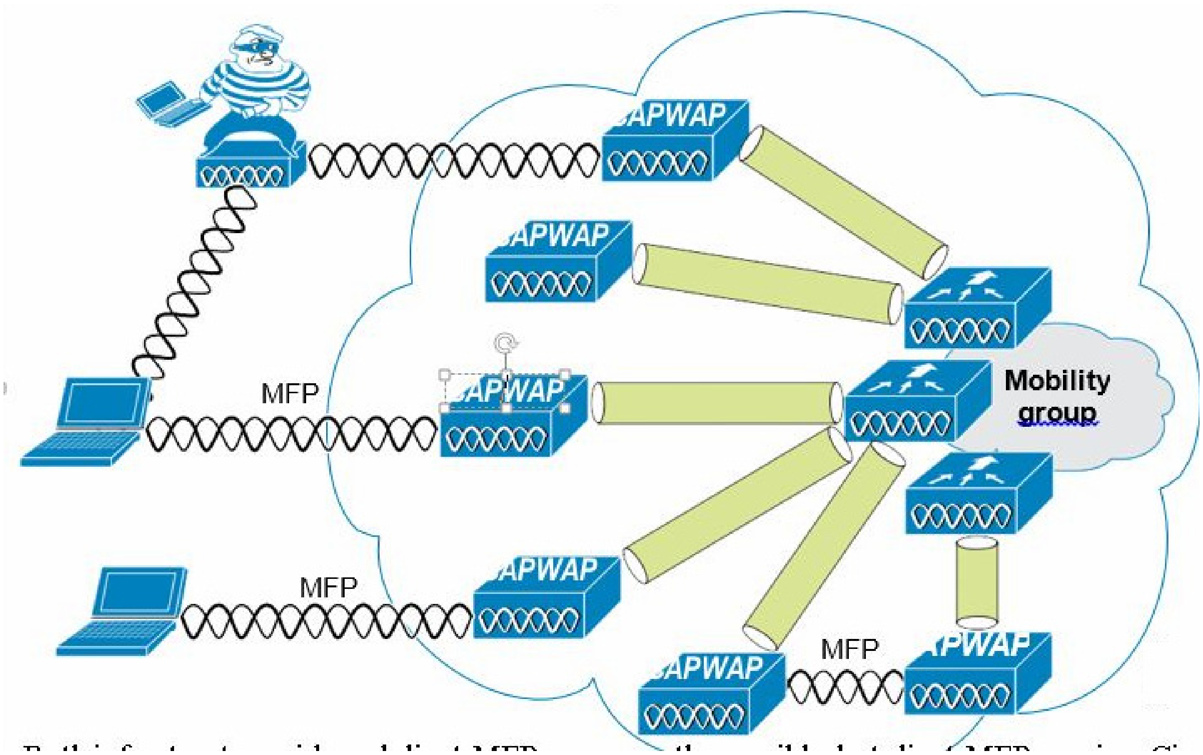
To determine whether rogue AP clients are also clients on the enterprise WLAN, the client MAC address can be compared with MAC addresses collected by the AAA during 802.1X authentication. This allows for the identification of potential WLAN clients that might have been compromised or users who are not following security policies.

Management Frame Protection

One of the challenges in 802.11 has been that management frames are sent in the clear with no encryption or message integrity checking and are therefore vulnerable to spoofing attacks. WLAN management frame spoofing can be used to attack a WLAN network. To address this, we created a digital signature mechanism to insert a message integrity check (MIC) into 802.11 management frames. This allows legitimate members of a WLAN deployment to be identified, as well as being able to identify rogue infrastructure devices, and spoofed frames through their lack of valid MICs.

The MIC used in management frame protection (MFP) is not a simple CRC hashing of the message, but also includes a digital signature component. The MIC component of MFP ensures that a frame has not been tampered with, and the digital signature component ensures that the MIC could have only been produced by a valid member of the WLAN domain. The digital signature key used in MFP is shared among all controllers in a mobility group; different mobility groups have different keys allowing validation of all WLAN management frames processed, by the WLCs, in that mobility group (Figure 4-29).

Figure 4-29 Management Frame Protection



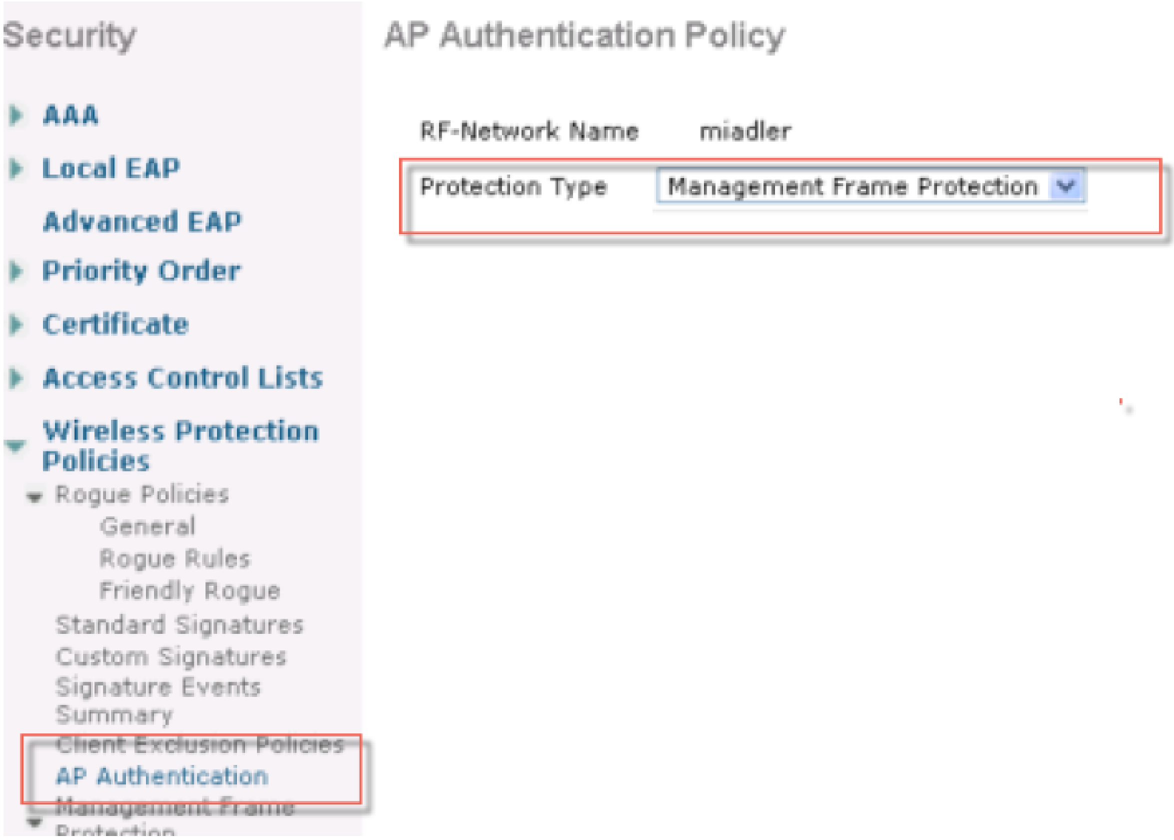
Both infrastructure-side and client MFP are currently possible, but client MFP requires Cisco Compatible Extensions v5 WLAN clients to learn the mobility group MFP key before they can detect and reject invalid frames.

MFP provides the following benefits:

- Authenticates 802.11 management frames generated by the WLAN network infrastructure.
- Allows detection of malicious rogues that spoof a valid AP MAC or SSID to avoid detection as a rogue AP, or as part of a man-in-the-middle attack.
- Increases the effectiveness of the rogue AP and WLAN IDS signature detection of the solution.
- Provides protection of client devices using Cisco Compatible Extensions v5.
- Supported by standalone AP.

Two steps are required to enable MFP: enabling it under the Security tab on the WLC (Figure 4-30) and enabling it on the WLANs in the mobility group (Figure 4-26).

Figure 4-30 Enabling MFP on the Controller



RF-Network Name miadler

Protection Type Management Frame Protection

Management System Security Features

Apart from providing location support for Rogue AP detection, the management system Cisco Prime provides two additional Unified Wireless Network security features: WLC configuration verification management and an alarm and reporting interface.

Configuration Verification

The management system Cisco Prime can provide on-demand or regularly-scheduled configuration audit reports, which compare the complete current running configuration of a WLC and its registered access points with that of a known valid configuration stored in the management system Cisco Prime databases. Any exceptions between the current running configuration and the stored database configuration are noted and brought to the attention of the network administrator via screen reports (Figure 4-30).

Alarms and Reports

Apart from the alarms that can be generated directly from a WLC and sent to an enterprise network management system Cisco Prime, where the management system can also send alarm notifications. The primary difference between alarm notification methods, apart from the type of alarm sent by the various components, is that the WLC uses Simple Network Management Protocol (SNMP) traps to send alarms (which can be interpreted only by an NMS system), whereas the management system Cisco Prime uses SMTP e-mail to send an alarm message to an administrator.

The management system Cisco Prime provides both real-time and scheduled reports, and can export or e-mail reports. The management system Cisco Prime provides reports on:

- Access points
- Audits
- Clients
- Inventory
- Mesh
- Performance
- Security

Cisco TrustSec SXP

The Cisco TrustSec enables organizations to secure their networks and services through identity-based access control to anyone, anywhere, anytime. The solution also offers data integrity and confidentiality services, policy-based governance, and centralized monitoring, troubleshooting, and reporting services. TrustSec can be combined with personalized, professional service offerings to simplify solution deployment and management, and is a foundational security component to Cisco Borderless Networks.

The Cisco TrustSec security architecture builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms. Cisco TrustSec uses the device and user credentials acquired during authentication for classifying the packets by security groups (SGs) as they enter the network. This packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be correctly identified to apply security and other policy criteria along the data path. The tag, called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic. Cisco TrustSec security group tag is applied only when you enable AAA override on a WLAN.

One of the components of Cisco TrustSec architecture is the security group-based access control. In the security group-based access control component, access policies in the Cisco TrustSec domain are topology-independent, based on the roles (as indicated by security group number) of source and destination devices rather than on network addresses. Individual packets are tagged with the security group number of the source.

Cisco devices use the SGT Exchange Protocol (SXP) to propagate SGTs across network devices that do not have hardware support for Cisco TrustSec. SXP is the software solution to avoid CTS hardware upgrade on all switches. WLC will be supporting SXP as part of TrustSec Architecture. The SXP sends SGT information to the CTS-enabled switches so that appropriate role-based access control lists (RBACLs) can be activated depending on the role information represented by the SGT. By default, the controller always works in the Speaker mode. To implement the SXP on a network, only the egress distribution switch needs to be CTS-enabled, and all the other switches can be non-CTS-capable switches.

The SXP runs between any access layer and distribution switch or between two distribution switches. The SXP uses TCP as the transport layer. CTS authentication is performed for any host (client) joining the network on the access layer switch similar to an access switch with CTS-enabled hardware. The access layer switch is not CTS hardware enabled. Therefore, data traffic is not encrypted or cryptographically authenticated when it passes through the access layer switch. The SXP is used to pass the IP address of the authenticated device, that is a wireless client, and the corresponding SGT up to the distribution switch. If the distribution switch is CTS hardware enabled, the switch inserts the SGT into the packet on behalf of the access layer switch. If the distribution switch is not CTS hardware enabled, the SXP on the distribution switch passes the IP-SGT mapping to all the distribution switches that have CTS hardware. On the egress side, the enforcement of the RBACL occurs at the egress L3 interface on the distribution switch.

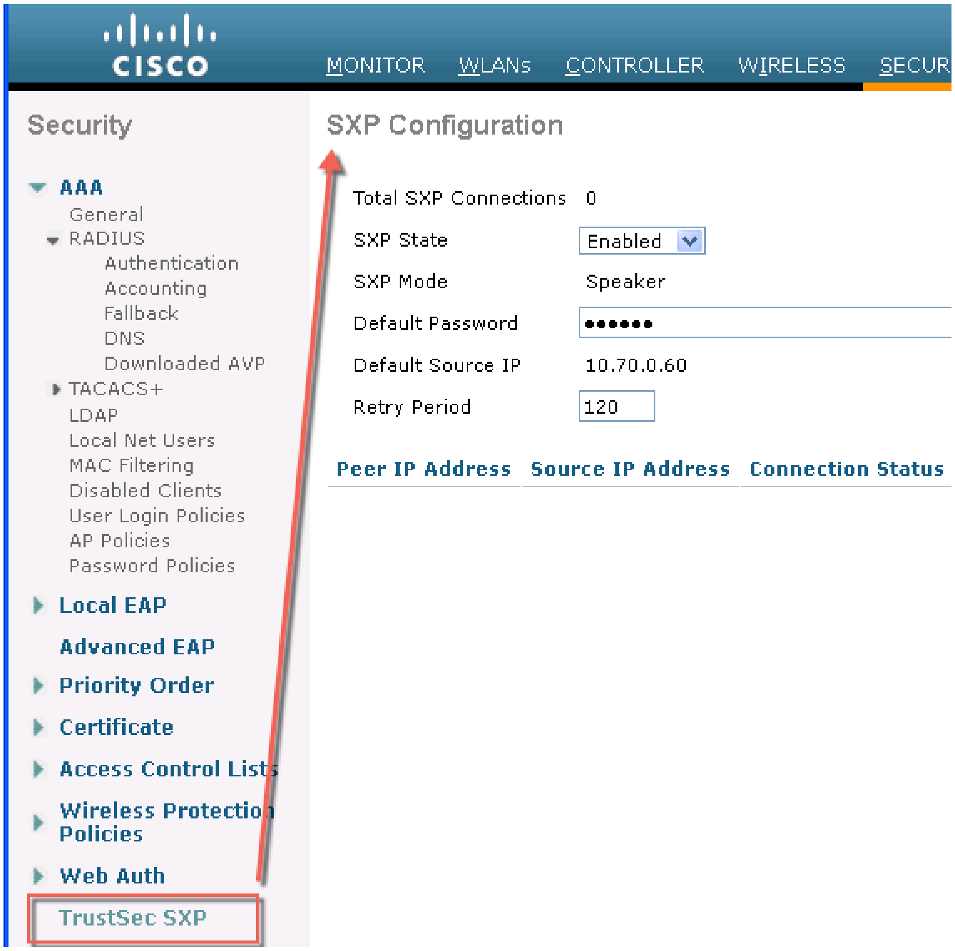
The following are some guidelines for Cisco TrustSec SXP:

- SSXP is supported on the following security policies only:
  - WPA2-dot1x
  - WPA-dot1x
  - 802.1x (Dynamic WEP)
  - MAC Filtering using RADIUS servers
  - Web authentication using RADIUS servers for user authentication
- SXP is supported for both IPv4 and IPv6 clients.
- Controller always operates in the Speaker mode.

For more information, see Cisco TrustSec.

Restrictions for Cisco TrustSec SXP

- SXP is not supported on FlexConnect access points.
- SXP is supported only in centrally switched networks that have central authentication.
- By default, SXP is supported for APs that work in local mode only.
- The configuration of the default password should be consistent for both controller and the switch.
- Fault tolerance is not supported because fault tolerance requires local switching on APs.
- Static IP-SGT mapping for local authentication of users is not supported.
- IP-SGT mapping requires authentication with external ACS servers.
- In auto-anchor/guest-anchor mobility the SGT information passed by the RADIUS server to foreign WLC can be communicated to the anchor WLC through the EoIP/CAPWAP mobility tunnel. The anchor WLC can then build the SGT-IP mapping and communicate it to another peer via SXP.



SXP Configuration

Total SXP Connections 0
SXP State Enabled
SXP Mode Speaker
Default Password ••••••
Default Source IP 10.70.0.60
Retry Period 120

Peer IP Address	Source IP Address	Connection Status

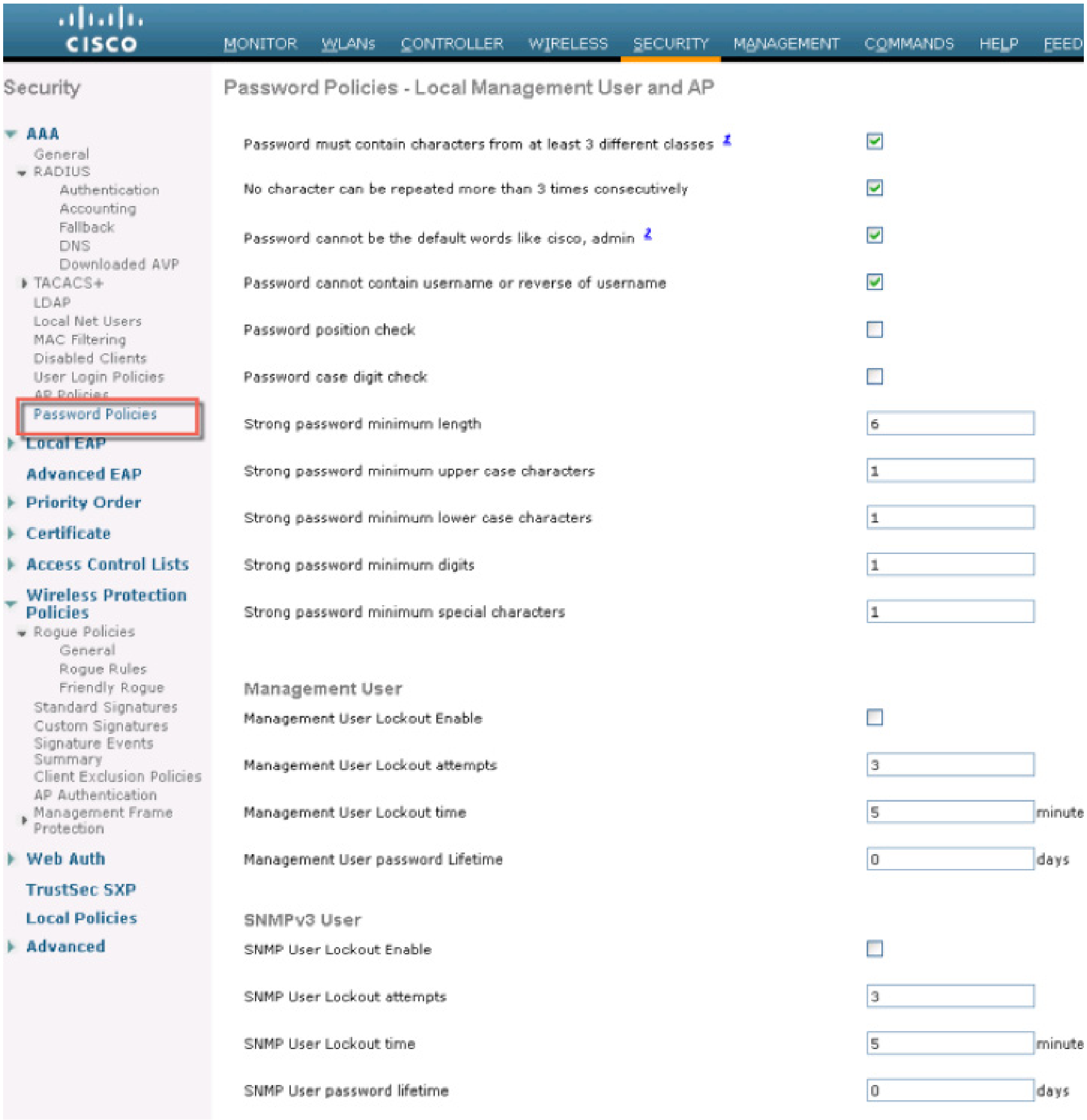
Password Policies

The password policies allows administrator to enforce strong password checks on newly created passwords for additional management users of controller and access point. The following are the requirements enforced on the new password:

- When the controller is upgraded from old version, all the old passwords are maintained as it is, even though the passwords are weak. After the system upgrade, if strong password checks are enabled, the same is enforced from that time and the strength of previously added passwords will not be checked or altered.
- Depending on the settings done in the Password Policy page, the local management, access point, management use and SNM3 user configuration is affected.

Figure 4-31 illustrates the password policies for Local Management User, AP, Management User and SNMPv3 user.

Figure 4-31 Password Policies - Local Management User and AP



Password Policies - Local Management User and AP

Password must contain characters from at least 3 different classes	☑
No character can be repeated more than 3 times consecutively	☑
Password cannot be the default words like cisco, admin	☑
Password cannot contain username or reverse of username	☑
Password position check	☐
Password case digit check	☐
Strong password minimum length	6
Strong password minimum upper case characters	1
Strong password minimum lower case characters	1
Strong password minimum digits	1
Strong password minimum special characters	1

Management User

Management User Lockout Enable	☐
Management User Lockout attempts	3
Management User Lockout time	5 minute
Management User password Lifetime	0 days

SNMPv3 User

SNMP User Lockout Enable	☐
SNMP User Lockout attempts	3
SNMP User Lockout time	5 minute
SNMP User password lifetime	0 days

CHAPTER 5

Cisco Unified Wireless QoS and AVC

This chapter describes quality of service (QoS) and Application Visibility and Control (AVC) in the context of WLAN implementations. This chapter describes WLAN QoS and AVC in general, but does not provide in-depth coverage on topics such as security, segmentation, and voice over WLAN (VoWLAN), although these topics have a QoS component.

This chapter is intended for those who are tasked with designing and implementing enterprise WLAN deployments using Cisco Unified Wireless Network technology.

QoS and AVC Overview

QoS refers to the capability of a network to provide differentiated service to selected network traffic over various network technologies. QoS technologies provide the following benefits:

- Provide building blocks for business multimedia and audio applications used in campus, WAN, and service provider networks
- Allow network managers to establish service-level agreements (SLAs) with network users
- Enable network resources to be shared more efficiently and expedite the handling of mission-critical applications
- Manage time-sensitive multimedia and audio application traffic to ensure that this traffic receives higher priority, greater bandwidth, and less delay than best-effort data traffic

With QoS, bandwidth can be managed more efficiently across WLANs, LANs and WANs. QoS provides enhanced and reliable network service by doing the following:

- Supporting dedicated bandwidth for critical users and applications
- Controlling jitter and latency (required by real-time traffic)
- Managing and minimizing network congestion
- Shaping network traffic to smooth the traffic flow
- Setting network traffic priorities

AVC provides application-aware control on a wireless network and enhances manageability and productivity. AVC is already supported on various ASR and WLC platforms. The support of AVC embedded within the FlexConnect AP extends as this is an end-to-end solution. This gives a complete visibility of applications in the network and allows the administrator to take some action on the application.

AVC has the following functionality and components:

- Next-generation Deep Packet Inspection (DPI) technology, called as Network Based Application Recognition (NBAR2), allows for identification and classification of applications. NBAR is a deep-packet inspection technology available on Cisco IOS based platforms, which supports stateful L4 – L7 classification. NBAR2 is based on NBAR and has extra requirements such as having a common flow table for all IOS features that use NBAR. NBAR2 recognizes application and passes this information to other features such as Quality of Service (QoS) and Access Control List (ACL), which can take action based on this classification.
- Ability to Apply Mark using QoS, Drop and Rate-limit applications.

The key use cases for NBAR AVC are capacity planning, network usage base lining, and better understanding of the applications that are consuming bandwidth. Trending of application usage helps the network administrator to plan for network infrastructure upgrade, improve quality of experience by protecting key applications from bandwidth-hungry applications when there is congestion on the network, capability to prioritize or de-prioritize, and drop certain application traffic.

AVC is supported on the 5520, 8540, 2500, 5508, 7500, 8500, and WiSM2 controllers on Local and FlexConnect modes (for WLANs configured for central switching only) since release 7.4. Release 8.1 introduces support for Application Visibility and Control (AVC) for locally switched WLANs on FlexConnect APs on 5508, 5500 series, 8500 series, 7500, WiSM2, and vWLC.

With AVC, applications can be viewed, managed, and controlled on the WLAN or per user. Network administrator can see, in GUI presentation, what application are being used on the wireless network and where and by whom the bandwidth being used. Administrator can view if the wireless network is being abused by a user browsing private or restricted sites, using very high bandwidth consuming applications such as Netflix or YouTube. With Network Based Application Recognition (NBAR2) engine running on the WLC, AVC provides application-aware control of over 1000 applications. Protocol Pack files that contain the algorithms to discover those applications come preloaded on the controller or can be upgraded to the latest versions dynamically.

Wireless QoS Deployment Schemes

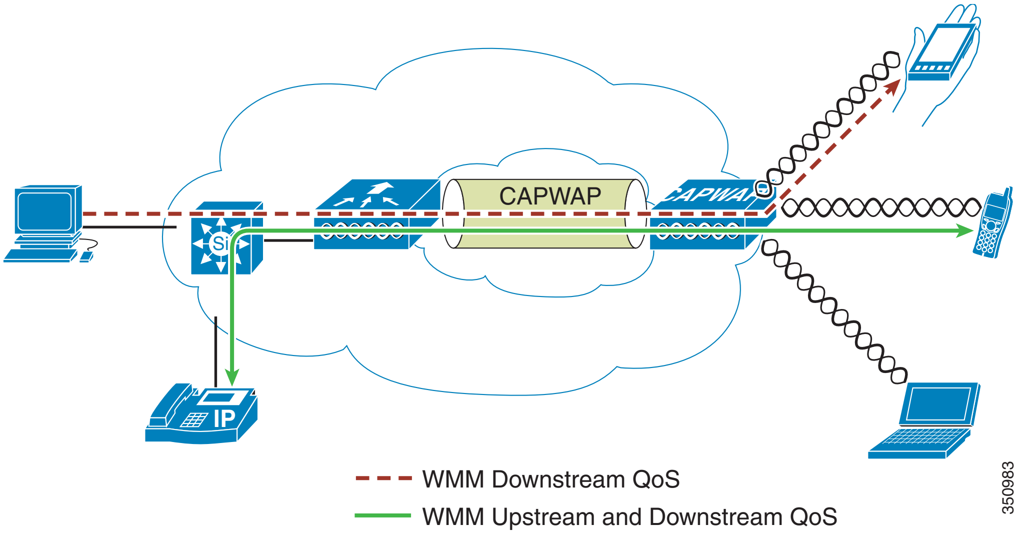
In the past, WLANs were mainly used to transport low-bandwidth, data-application traffic. Currently, with the expansion of WLANs into vertical (such as retail, finance, and education) and enterprise environments, WLANs are used to transport high-bandwidth data applications, in conjunction with time-sensitive multimedia applications. This requirement led to the necessity for wireless QoS.

Several vendors, including Cisco, support proprietary wireless QoS schemes for audio applications. To speed up the rate of QoS adoption and to support multi-vendor time-sensitive applications, a unified approach to wireless QoS is necessary. The IEEE 802.11e working group within the IEEE 802.11 standards committee has completed the standard definition, and adoption of the 802.11e standard is completed. As with many standards, there are many optional components. Just as occurred with 802.11 security in 802.11i, industry groups such as the Wi-Fi Alliance and industry leaders such as Cisco are defining the key requirements in WLAN QoS through their WMM and Cisco Compatible Extensions programs, ensuring the delivery of key features and interoperation through their certification programs.

Cisco Unified Wireless products support Wi-Fi MultiMedia (WMM), a QoS system based on IEEE 802.11e that has been published by the Wi-Fi Alliance and WMM Power Save, as well as Admission Control.

Figure 5-1 illustrates an example of the deployment of wireless QoS based on Cisco Unified Wireless technology features.

Figure 5-1 QoS Deployment Example



QoS Parameters

QoS is defined as the measure of performance for a transmission system that reflects its transmission quality and service availability. Service availability is a crucial component of QoS. Before QoS can be successfully implemented, the network infrastructure must be highly available.

Network transmission quality is determined by the elements of latency, jitter, and loss, as shown in Table 5-1.

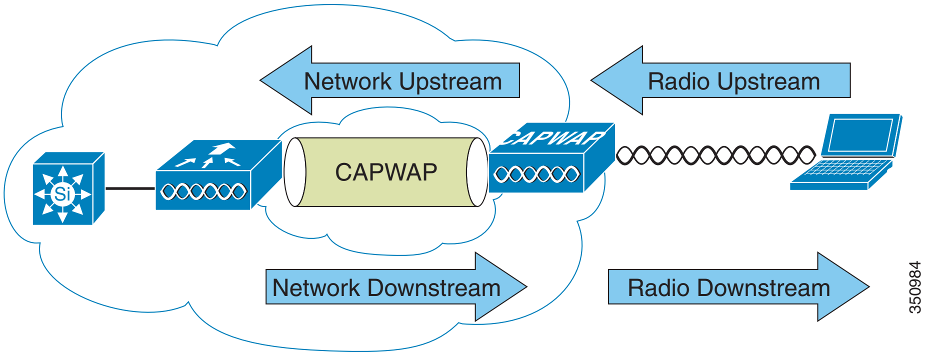
Table 5-1 QoS Transmission Quality

Element	Description
Latency	Latency (or delay) is the amount of time it takes for a packet to reach the receiving endpoint after being transmitted from the sending endpoint. This time period is called the end-to-end delay and can be divided into two areas: • Fixed network delay—Includes encoding and decoding time (for audio and video), and the finite amount of time required for the electrical or optical pulses to traverse the media en route to their destination. • Variable network delay—Generally refers to network conditions, such as queuing and congestion, that can affect the overall time required for transit.
Jitter	Jitter (or delay-variance) is the difference in the end-to-end latency between packets. For example, if one packet requires 100 ms to traverse the network from the source endpoint to the destination endpoint, and the next packet requires 125 ms to make the same trip, the jitter is calculated as 25 ms.
Loss	Loss (or packet loss) is a comparative measure of packets successfully transmitted and received to the total number that were transmitted. Loss is expressed as the percentage of packets that were dropped.

Radio Upstream and Downstream QoS

Figure 5-2 illustrates the concepts of *radio upstream* and *radio downstream* QoS.

Figure 5-2 Upstream and Downstream QoS



As illustrated in Figure 5-2:

- *Radio downstream* QoS—Traffic leaving the AP and traveling to the WLAN clients. Radio downstream QoS is the primary focus of this chapter, because this is still the most common deployment. The radio client upstream QoS depends on the client implementation.
- *Radio upstream* QoS—Traffic leaving the WLAN clients and traveling to the AP. WMM provides upstream QoS for WLAN clients supporting WMM.

- *Network downstream*—Traffic leaving the wireless LAN controller (WLC) traveling to the AP. QoS can be applied at this point to prioritize and rate-limit traffic to the AP

Note Configuration of *Ethernet downstream* QoS is not described in this guide.

- *Network upstream*—Traffic leaving the AP, traveling to the WLC. The AP classifies traffic from the AP to the upstream network according to the traffic classification rules of the AP.

QoS and Network Performance

The application of QoS features could be difficult to detect on a lightly loaded network. If latency, jitter, and loss are noticeable when the media is lightly loaded, it indicates either a system fault, poor network design, or that the latency, jitter, and loss requirements of the application are not a good match for the network. QoS features start to be applied to application performance as the load on the network increases. QoS works to keep latency, jitter, and loss for selected traffic types within acceptable boundaries. When providing only radio downstream QoS from the AP, radio upstream client traffic is treated as best-effort. A client must compete with other clients for upstream transmission as well as competing with best-effort transmission from the AP. Under certain load conditions, a client can experience upstream congestion, and the performance of QoS-sensitive applications might be unacceptable despite the QoS features on the AP. Ideally, upstream and downstream QoS can be operated either by using WMM on both the AP and WLAN client, or by using WMM and a client proprietary implementation.

Note WLAN client support for WMM does not mean that the client traffic automatically benefits from WMM. The applications looking for the benefits of WMM assign an appropriate priority classification to their traffic and the operating system needs to pass that classification to the WLAN interface. In purpose-built devices, such as VoWLAN handsets, this is done as part of the design. However, if implementing on a general purpose platform such as a PC, application traffic classification and OS support must be implemented before the WMM features can be used to good effect.

Even without WMM support on the WLAN client, the Cisco Unified Wireless Network solution is able to provide network prioritization in both network upstream and network downstream situations.

802.11 Distributed Coordination Function

Data frames in 802.11 are sent using the distributed coordination function (DCF), which is composed of the following main components:

- Interframe spaces (IFS including SIFS, PIFS, and DIFS, which are described below)
- Random backoff (contention window)

DCF is used in 802.11 networks to manage access to the RF medium. A baseline understanding of DCF is necessary to deploy 802.11e-based enhanced distributed channel access (EDCA). For more information on DCF, see the IEEE 802.11 specification at:

http://www.ieee802.org/11/

These 802.11 DCF components are discussed further in the following sections.

Interframe Spaces

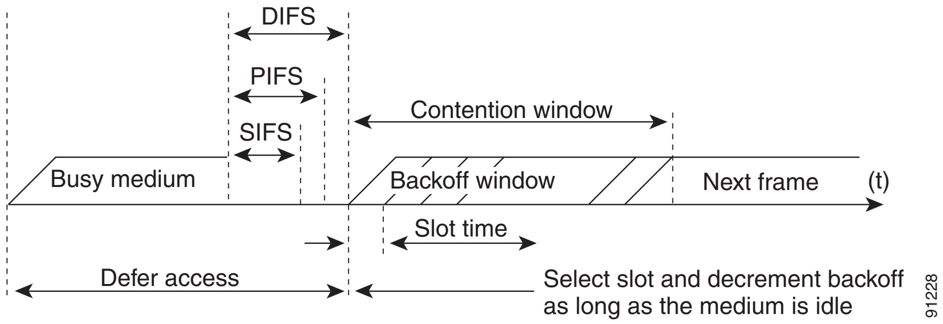
The 802.11 standard defines interframe spaces (IFS) as:

- Short interframe space (SIFS)—10 µs
- PCF interframe space (PIFS)—SIFS + 1 x slot time = 30 µs
- DCF interframe space (DIFS)—50 µs SIFS + 2 x slot time = 50 µs

Note The base timing used in the IFS example shown in Figure 5-3 is for 802.11b. The timing in 802.11g and 802.11a are different, but the principles applied are the same.

IFS allow 802.11 to control which traffic gets first access to the channel after carrier sense declares the channel to be free. Generally, 802.11 management frames and frames not expecting contention (a frame that is part of a sequence of frames) use SIFS, and data frames use DIFS, as shown in Figure 5-3.

Figure 5-3 Interframe Spaces



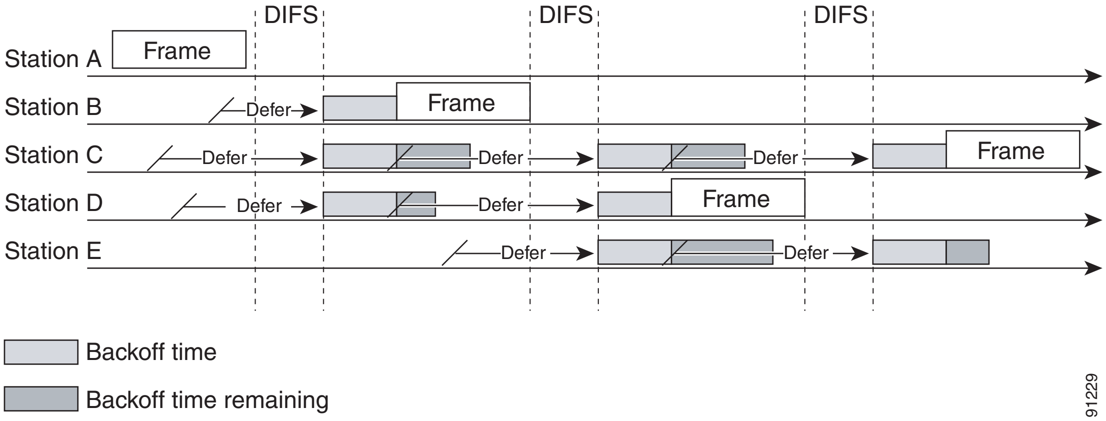
Random Backoff

When DCF has a data frame ready to be transmitted, the DCF goes through the following steps:

1. DCF generates a random backoff number between zero and a minimum contention window (see aCWmin, aCWmax, and Retries, page 5-7).
2. DCF waits until the channel is free for a DIFS interval.
3. If the channel is still free, DCF begins to decrement the random backoff number for every slot time (20 µs) that the channel remains free.
4. If the channel becomes busy (such as when a station gets to zero), DCF stops the decrement and steps 2 and 3 are repeated.
5. If the channel remains free until the random backoff number reaches zero, DCF allows the frame to be transmitted.

Figure 5-4 shows a simplified example of how the DCF process works. In this DCF process no acknowledgements are shown and no fragmentation occurs.

Figure 5-4 *Distributed Coordination Function Example*



The DCF steps illustrated in Figure 5-4 are:

1. Station A successfully transmits a frame. Three other stations want to transmit frames but must defer to Station A traffic.
2. After Station A completes the transmission, the stations must still defer to the DIFS.
3. When the DIFS completes, stations waiting to transmit a frame can begin to decrement their backoff counters, once for every slot time.
4. The backoff counter of Station B reaches zero before Stations C and D, and therefore Station B begins transmitting its frame.
5. When Station C and D detect that Station B is transmitting, they must stop decrementing their backoff counters and defer until the frame is transmitted and a DIFS has passed.
6. During the time that Station B is transmitting a frame, Station E receives a frame to transmit, but because Station B is transmitting a frame, it must defer in the same manner as Stations C and D.
7. When Station B completes transmission and the DIFS has passed, stations with frames to transmit begin to decrement their backoff counters. In this case, the Station D backoff counter reaches zero first and so Station D begins transmission of its frame.

The process continues as traffic arrives on the different stations.

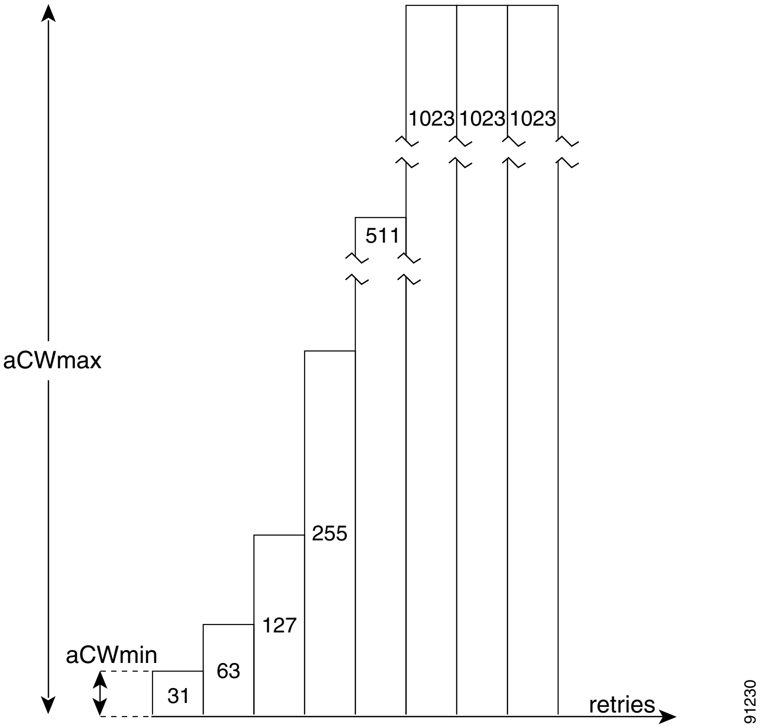
aCWmin, aCWmax, and Retries

DCF uses a contention window (CW) parameters to control the size of the random backoff. The CW is defined by the parameters:

- aCWmin—Minimum contention window
- aCWmax—Maximum contention window

The random number used in the random backoff is initially a number between 0 and aCWmin. If the initial random backoff expires without successfully transmitting the frame, the station or AP increments the retry counter and doubles the value random backoff window size. This doubling in size continues until the size equals aCWmax. The retries continue until the maximum retries or time to live (TTL) is reached. This process of doubling the backoff window is often referred to as a *binary exponential backoff,* and is illustrated in Figure 5-5 where the aCWmin if 2^5-1, and increases to 2^6-1, on the next backoff level, up to the aCWmax value of 2^{10}-1.

Figure 5-5 Growth in Random Backoff Range with Retries



Note These values are for 802.11b implementations. Values can be different for different physical layer implementations.

Wi-Fi Multimedia

This section describes three important Wi-Fi multimedia (WMM) topics:

- WMM Access
- WMM Classification
- WWM Queues

WMM Access

WMM is a Wi-Fi Alliance certification of support for a set of features from an 802.11e draft. This certification is for both clients and APs, and certifies the operation of WMM. WMM is primarily the implementation of the EDCA component of 802.11e. Additional Wi-Fi certifications are planned to address other components of the 802.11e.

WMM Classification

WMM uses the 802.1P classification scheme (part of the IEEE 802.1D MAC Bridges standard). This classification scheme has eight priorities that WMM maps to four access categories with WMM designations:

- AC_BK—Background
- AC_BE—Best effort
- AC_VI—Video
- AC_VO—Voice

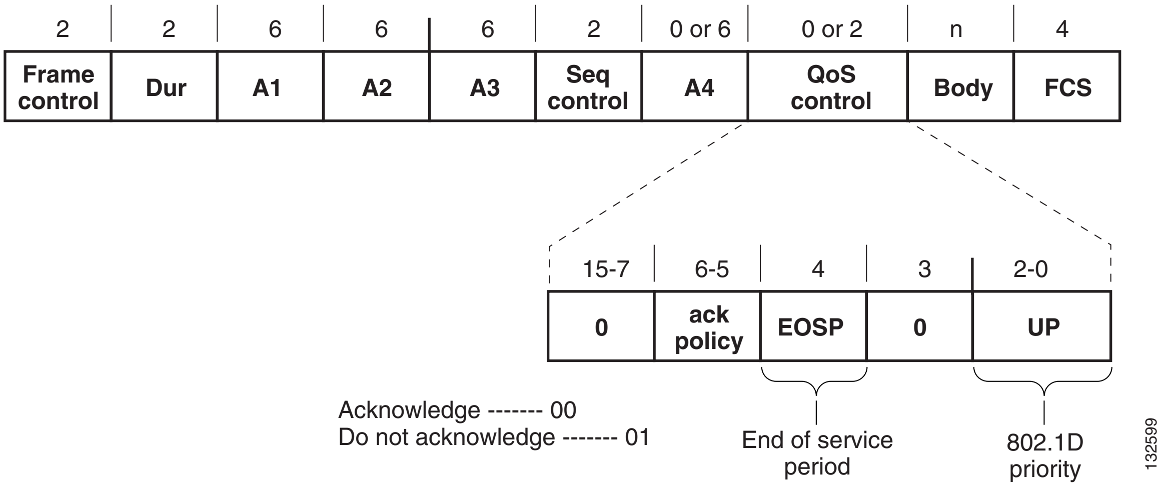
As shown in Table 5-2, these access categories map to the four queues (see WMM Queues, page 5-10) required by WMM devices.

Table 5-2 Table 2 802.1P and WMM Classification

Priority	802.1P Priority	802.1P Designation	Access Category_WMM Designation
Lowest	1	BK	AC_BK
	2	-	
	0	BE	AC_BE
	3	EE	
	4	CL	AC_VI
	5	VI	
	6	VO	AC_VO
Highest	7	NC	

Figure 5-6 shows the WMM data frame format. Note that even though WMM maps the eight 802.1P classifications to four access categories, the 802.11D classification is sent in the frame.

Figure 5-6 WMM Frame Format



The WMM and IEEE 802.11e classifications are different from the classifications recommended and used in the Cisco Unified Wireless Network, which are based on IETF recommendations. The primary difference in classification is the changing of audio and video traffic to 5 and 4 user priorities (UPs), respectively. This allows the 6 classification to be used for Layer 3 network control. To be compliant with both standards, the Cisco Unified Wireless Network solution performs a conversion between the various classification standards when the traffic crosses the wireless-wired boundary.

WMM Queues

Figure 5-7 shows the queuing performed on a WMM client or AP. There are four separate queues, one for each of the access categories. Each of these queues contends for the wireless channel in a similar manner to the DCF mechanism described above, with each of the queues using different IFS, aCWmin, and aCWmax values. If more than one frame from different access categories collide internally, the frame with the higher priority is sent and the lower priority frame adjusts its backoff parameters as though it had collided with a frame external to the queuing mechanism. This system is called enhanced distributed channel access (EDCA).

Figure 5-7 WMM Queues

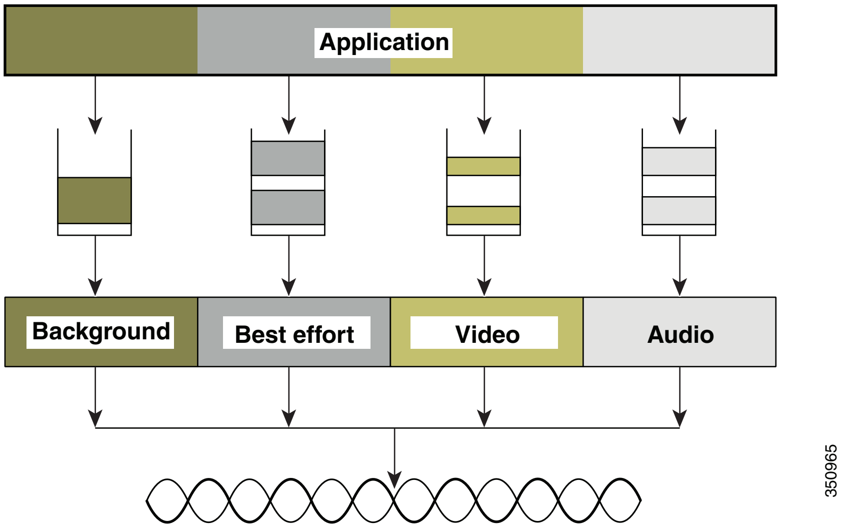
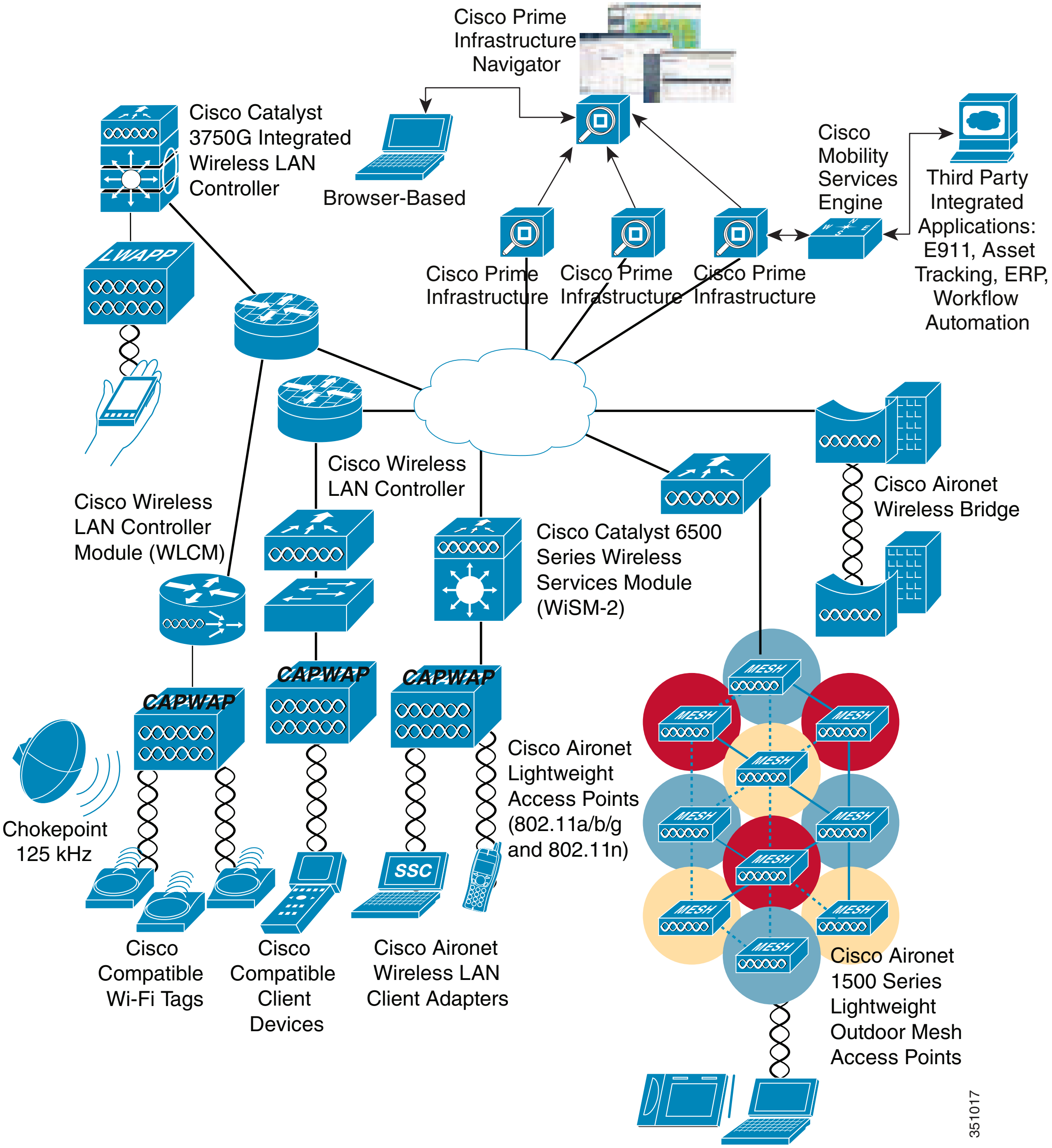


Figure 5-8 illustrates the principles behind EDCF, where different interframe spacing and aCWmin and aCWmax values (for clarity aCWmax is not shown) are applied per traffic classification. Different traffic types wait different IFS before counting down their random backoff. The aCW value used to generate the random backoff number also depends on the traffic classification. For example, the aCWmin[3] for Voice is 23-1, and aCWmin[5] for best-effort traffic is 25-1. High priority traffic has a small IFS and a small aCWmin value, giving a short random backoff, whereas best-effort traffic has a longer IFS and large aCWmin value that on average gives a large random backoff number.

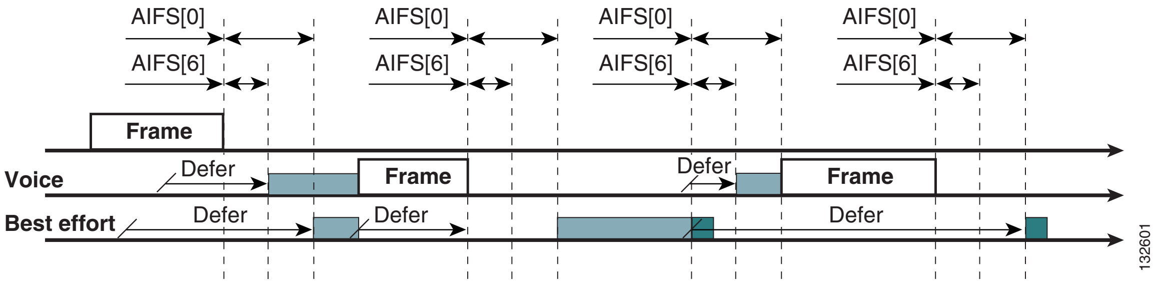
Figure 5-8 Access Category Timing



Enhanced Distributed Channel Access

Figure 5-9 illustrates an example of the enhanced distributed channel access (EDCA) process.

Figure 5-9 EDCA Example



The EDCA process follows the sequence:

1. While Station X is transmitting its frame, three other stations determine that they must transmit a frame. Each station defers because a frame was already being transmitted, and each station generates a random backoff.
2. Because the Voice station has a traffic classification of voice (audio), it has an *arbitrated interframe space* (AIFS) of two and uses an initial aCWmin of three. Therefore the station must defer the countdown of its random backoff for two slot times. It also has a short random backoff value.
3. The best-effort station has an AIFS of three and a longer random backoff time, because its aCWmin value is five.
4. The Voice station has the shortest random backoff time and therefore starts transmitting first. When Voice starts transmitting all other stations defer.
5. After the Voice station finishes transmitting, all stations wait their AIFS then begin to decrement their random backoff counters again.
6. The best-effort station then completes decrementing its random backoff counter and begins transmission. All other stations defer.

   This can happen even though there might be a Voice station waiting to transmit. This shows that best-effort traffic is not diminished by Voice traffic because the random backoff decrementing process eventually brings the best-effort backoff down to similar sizes as high priority traffic, and that the random process might, on occasion, generate a small random backoff number for best-effort traffic.
7. The process continues as other traffic enters the system.

The access category settings shown in Table 5-3 and Table 5-4 are, by default, the same for an 802.11a radio and are based on formulas defined in WMM.

Note Table 5-3 refers to the parameter settings on a client, which are slightly different from the settings for an AP. The AP has a larger AIFS[n] for audio and video admission controls (ACs).

Table 5-3 WMM Client Parameters

AC	**CWmin**	**aCWmax**	**AIFS[n]**	**TXOP Limit (802.11b)**	**TXOP Limit (802.11a/g)**
AC_BK	CWmin	aCWmax	7	0	0
AC_BE	CWmin	4*(aCQmin+1)-1	3	0	0
AC_VI	(CWmin+1)/2-1	CWmin	1	6.016 ms	3.008 ms
AC_VO	(CWmin+1)/4-1	(CWmin+1)/2-1	1	3.264 ms	1.504 ms

Table 5-4 WMM AP Parameters

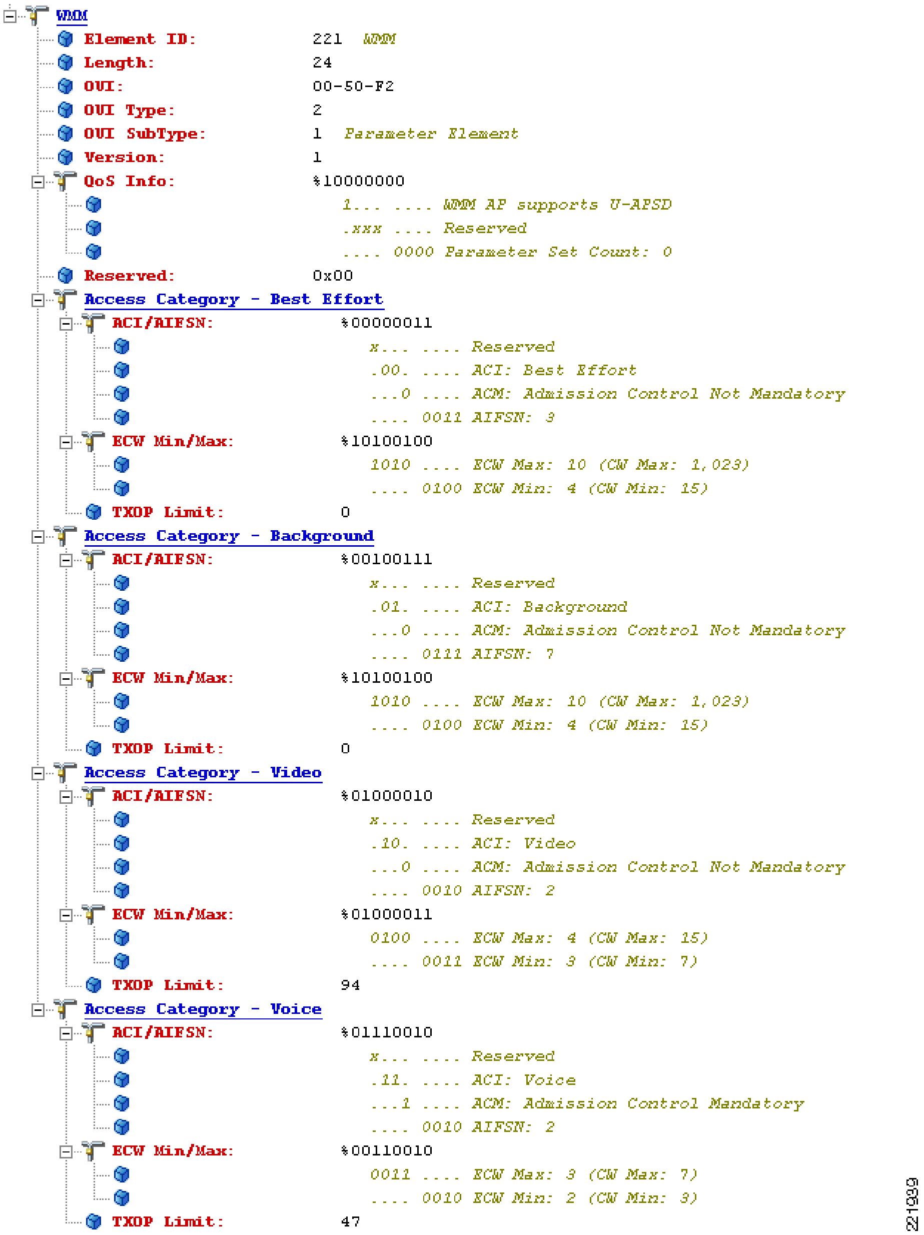
Access Category	**CWmin**	**aCWmax**	**AIFS[n]**	**TXOP Limit (802.11b**	**TXOP Limit (802.11a/g)**
AC_BK	CWmin	aCWmax	7	0	0
AC_BE	CWmin	4*(aCQmin+1)-1	3	0	0
AC_VI	(CWmin+1)/2-1	CWmin	2	6.016 ms	3.008 ms
AC_VO	(CWmin+1)/4-1	(CWmin+1)/2-1	2	3.264 ms	1.504 ms

The overall impact of the different AIFS, CWmin, and aCWmax values is difficult to illustrate in timing diagrams because their impact is more statistical in nature. It is easier to compare the AIFS and the size of the random backoff windows, as shown in Figure 5-8.

When comparing Voice and Background frames as examples, these traffic categories have CWmin values of 2^3-1 (7) and 2^5-1 (31), and AIFS of 2 and 7, respectively. This is an average delay of 5 (2+7/1) slot times before transmitting an audio frame, and an average of 22 slot (7+31/2) times for Background frame. Therefore, Voice frames are statistically much more likely to be sent before Background frames.

Figure 5-10 shows the WMM information in a probe response. Apart from the WMM access-category information contained in this element, the client also learns which WMM categories require admission control. As can be seen in this example, the Voice admission control (AC) is set to mandatory. This requires the client to transmit the request to the AP, and have the request accepted, before it can use this AC. Admission control is further discussed in different parts of this chapter.

Figure 5-10 Probe Response WMM Element Information



```
WMM
    Element ID:           221  WMM
    Length:               24
    OUI:                  00-50-F2
    OUI Type:             2
    OUI SubType:          1  Parameter Element
    Version:              1
    QoS Info:             %10000000
                             1... .... WMM AP supports U-APSD
                             .xxx .... Reserved
                             .... 0000 Parameter Set Count: 0
    Reserved:             0x00
    Access Category - Best Effort
        ACI/AIFSN:            %00000011
                                 x... .... Reserved
                                 .00. .... ACI: Best Effort
                                 ...0 .... ACM: Admission Control Not Mandatory
                                 .... 0011 AIFSN: 3
        ECW Min/Max:          %10100100
                                 1010 .... ECW Max: 10 (CW Max: 1,023)
                                 .... 0100 ECW Min: 4 (CW Min: 15)
        TXOP Limit:           0
    Access Category - Background
        ACI/AIFSN:            %00100111
                                 x... .... Reserved
                                 .01. .... ACI: Background
                                 ...0 .... ACM: Admission Control Not Mandatory
                                 .... 0111 AIFSN: 7
        ECW Min/Max:          %10100100
                                 1010 .... ECW Max: 10 (CW Max: 1,023)
                                 .... 0100 ECW Min: 4 (CW Min: 15)
        TXOP Limit:           0
    Access Category - Video
        ACI/AIFSN:            %01000010
                                 x... .... Reserved
                                 .10. .... ACI: Video
                                 ...0 .... ACM: Admission Control Not Mandatory
                                 .... 0010 AIFSN: 2
        ECW Min/Max:          %01000011
                                 0100 .... ECW Max: 4 (CW Max: 15)
                                 .... 0011 ECW Min: 3 (CW Min: 7)
        TXOP Limit:           94
    Access Category - Voice
        ACI/AIFSN:            %01110010
                                 x... .... Reserved
                                 .11. .... ACI: Voice
                                 ...1 .... ACM: Admission Control Mandatory
                                 .... 0010 AIFSN: 2
        ECW Min/Max:          %00110010
                                 0011 .... ECW Max: 3 (CW Max: 7)
                                 .... 0010 ECW Min: 2 (CW Min: 3)
        TXOP Limit:           47
```

Unscheduled-Automatic Power-save Delivery

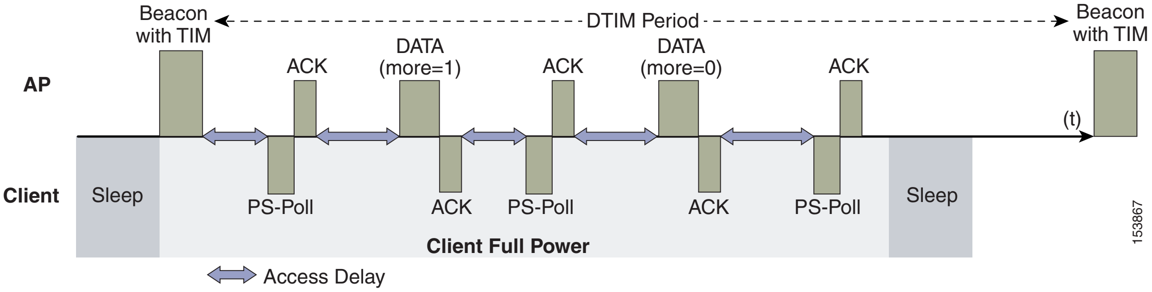
Unscheduled-automatic power-save delivery (U-APSD) is a feature of WMM that has two key benefits:

- The primary benefit of U-APSD is that it allows the audio client to synchronize the transmission and reception of audio frames with the AP, thereby allowing the client to go into power-save mode between the transmission/reception of each audio frame tuple. The WLAN client frame transmission in the access categories supporting U-APSD triggers the AP to transmit any data frames queued for that WLAN client in that access category. A U-APSD client continues listening to the AP until it receives a frame from the AP with an end-of-service period (EOSP) bit set. This tells the client that it can now go back into its power-save mode. This triggering mechanism is considered a more efficient use of client power than the regular listening for beacons method, at a period controlled by the delivery traffic indication message (DTIM) interval. This is because the latency and jitter requirements of audio are such that a wireless VoIP client would either not be in power-save mode during a call, resulting in reduced talk times, or would use a short DTIM interval that results in reduced standby times. The use of U-APSD allows the use of long DTIM intervals to maximize standby time without sacrificing call quality. The U-APSD feature can be applied individually across access categories, allowing U-APSD can be applied to the audio ACs in the AP, but the other ACs still use the standard power-save mode feature.

- The secondary benefit of this feature is increased call capacity. The coupling of transmission buffered data frames from the AP with the triggering data frame from the WLAN client allows the frames from the AP to be sent without the accompanying IFS and random backoff, thereby reducing the contention experience by call.

Figure 5-11 shows a sample frame exchange for the standard 802.11 power save delivery process.

Figure 5-11 Standard Client Power-Save

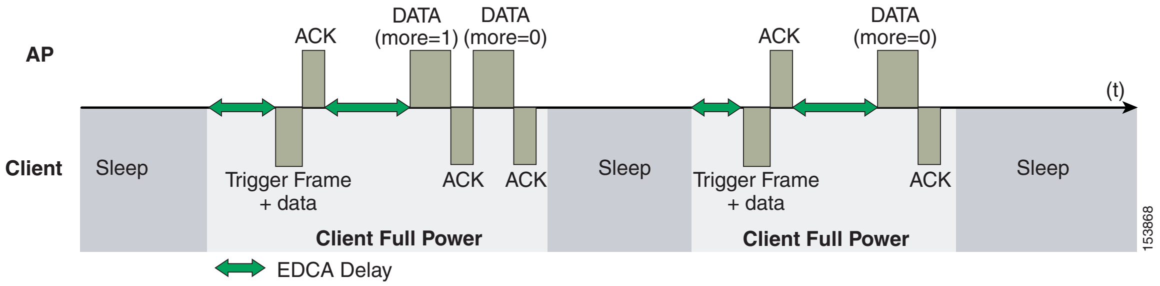


The client in power-save mode first detects that there is data waiting for it at the AP via the presence of the TIM in the AP beacon. The client must power-save poll (PS-Poll) the AP to retrieve that data. If the data sent to the client requires more than one frame to be sent, the AP indicates this in the sent data frame. This process requires the client to continue sending power-save polls to the AP until all the buffered data is retrieved by the client.

This presents two major problems. The first is that it is quite inefficient, requiring the PS-polls, as well as the normal data exchange, to go through the standard access delays associated with DCF. The second issue, being more critical to audio traffic, is that retrieving the buffered data is dependent on the DTIM, which is a multiple of the beacon interval. Standard beacon intervals are 100 ms, and the DTIM interval can be integer multiples of this. This introduces a level of jitter that is generally unacceptable for audio calls, and audio handsets switch from power-save mode to full transmit and receive operation when a audio call is in progress. This gives acceptable audio quality but reduces battery life. The Cisco 7921G Unified Wireless IP Phone addresses this issue by providing a PS-Poll feature that allows the 7921G to generate PS-Poll requests without waiting for a beacon TIM. This allows the 7921G to poll for frames when it has sent a frame, and then go back to power-save mode. This feature does not provide the same efficiency as U-APSD, but improves battery life for 7921G phones on WLANs without U-APSD.

Figure 5-12 shows an example of traffic flows with U-APSD. In this case, the trigger for retrieving traffic is the client sending traffic to the AP. The AP, when acknowledging the frame, tells the client that data is queued for it and that it should stay connected. The AP then sends data to the client, typically as a TXOP burst where only the first frame has the EDCF access delay. All subsequent frames are then sent directly after the acknowledgment frame. In a VoWLAN implementation there is likely to be only one frame queued at the AP. The VoWLAN client is able to go into sleep mode after receiving that frame from the AP.

Figure 5-12 U-APSD



This approach overcomes both the disadvantages of the previous scheme, in that it is much more efficient. The timing of the polling is controlled by way of the client traffic, which in the case of audio is symmetric, so if the client is transmitting a frame every 20 ms, it would be expecting to receive a frame every 20 ms as well. This would introduce a maximum jitter of 20 ms, rather than an `n * 100 ms` jitter.

TSpec Admission Control

Traffic Specification (TSpec) allows an 802.11e client to signal its traffic requirements to the AP. In the 802.11e MAC definition, two mechanisms provide prioritized access: the contention-based EDCA option and the controlled access option provided by the transmit opportunity (TXOP). When describing TSpec features where a client can specify its traffic characteristics, it is easy to assume that this would automatically result in the use of the controlled access mechanism, and have the client granted a specific TXOP to match the TSpec request. However, this does not have to be the case; a TSpec request can be used to control the use of the various access categories (ACs) in EDCA. Before a client can send traffic of a certain priority type, it must have requested to do so by way of the TSpec mechanism. For example, a WLAN client device wanting to use the audio access categories must first make a request for use of that AC. Whether or not AC use is controlled by TSpec requests is configurable with audio and audio ACs controlled by TSpec requests, and best-effort and background ACs can be open for use without a TSpec request. The use of EDCA ACs, rather than the 802.11e Hybrid Coordinated Channel Access (HCCA), to meet TSpec requests is possible in many cases because the traffic parameters are sufficiently simple to allow them to be met by allocating capacity, rather than creating a specific TXOP to meet the application requirements.

Add Traffic Stream

The Add Traffic Stream (ADDTS) function is used by WLAN client to send an *admission request* to an AP. Signaling its TSpec request to the AP, an admission request is in one of two forms:

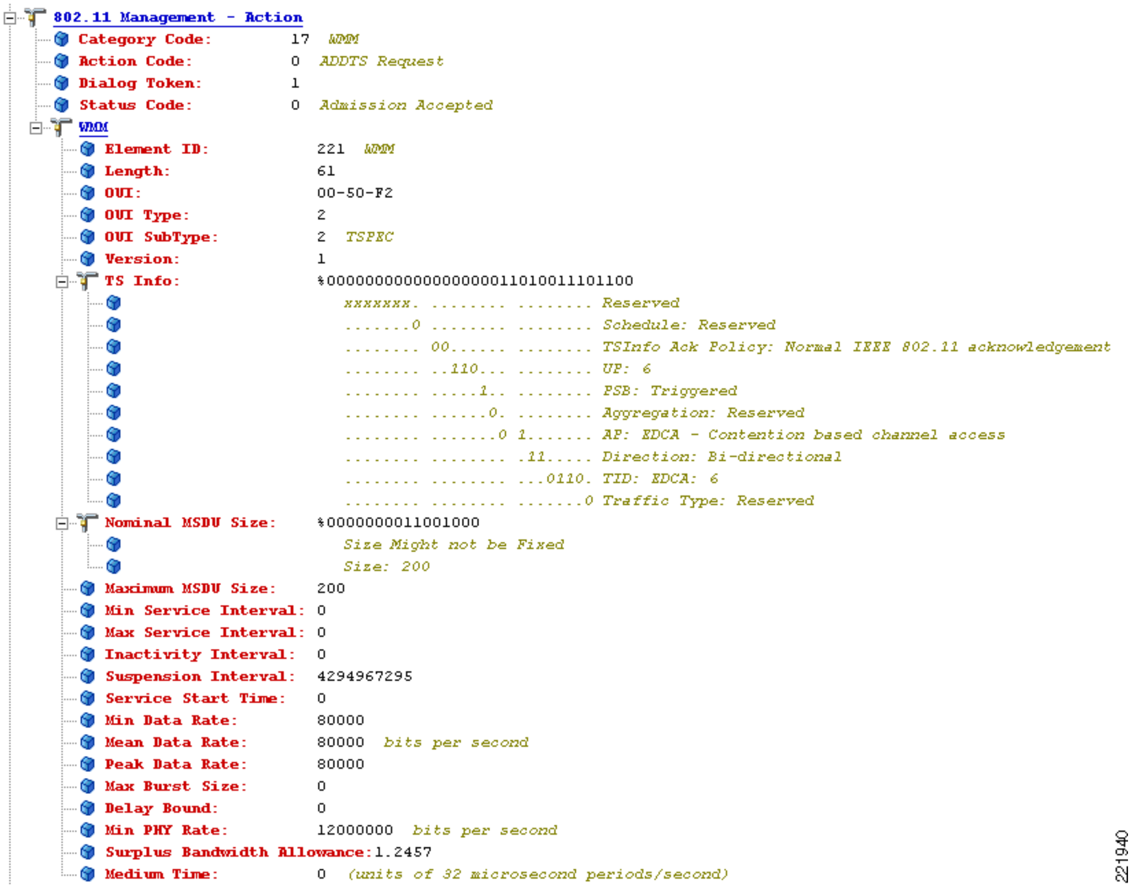
- ADDTS action frame—Created when a phone call is originated or terminated by a client associated to the AP. The ADDTS contains TSpec and could contain a traffic stream rate set (TSRS) information element (IE).
- Association and re-association message—The association message might contain one or more TSpecs and one TSRS IE if the station wants to establish the traffic stream as part of the association. The re-association message might contain one or more TSpecs and one TSRS IE if an station roams to another AP.

The ADDTS contains the TSpec element that describes the traffic request. See Figure 5-13 and Figure 5-14 for examples of an ADDTS request and response between a Cisco 7921 WLAN handset and a Cisco AP. Apart from key data describing the traffic requirements, such as data rates and frame sizes, the TSpec element also tells the AP the minimum physical rate that the client device will use. This allows the calculation of how much time that station can potentially consume in transmitting and receiving in this TSpec, and therefore allowing the AP to calculate whether it has the resources to meet the TSpec.

TSpec admission control is used by the WLAN client (target clients are VoIP handsets) when a call is initiated and during a roam request. During a roam, the TSpec request is appended to the re-association request.

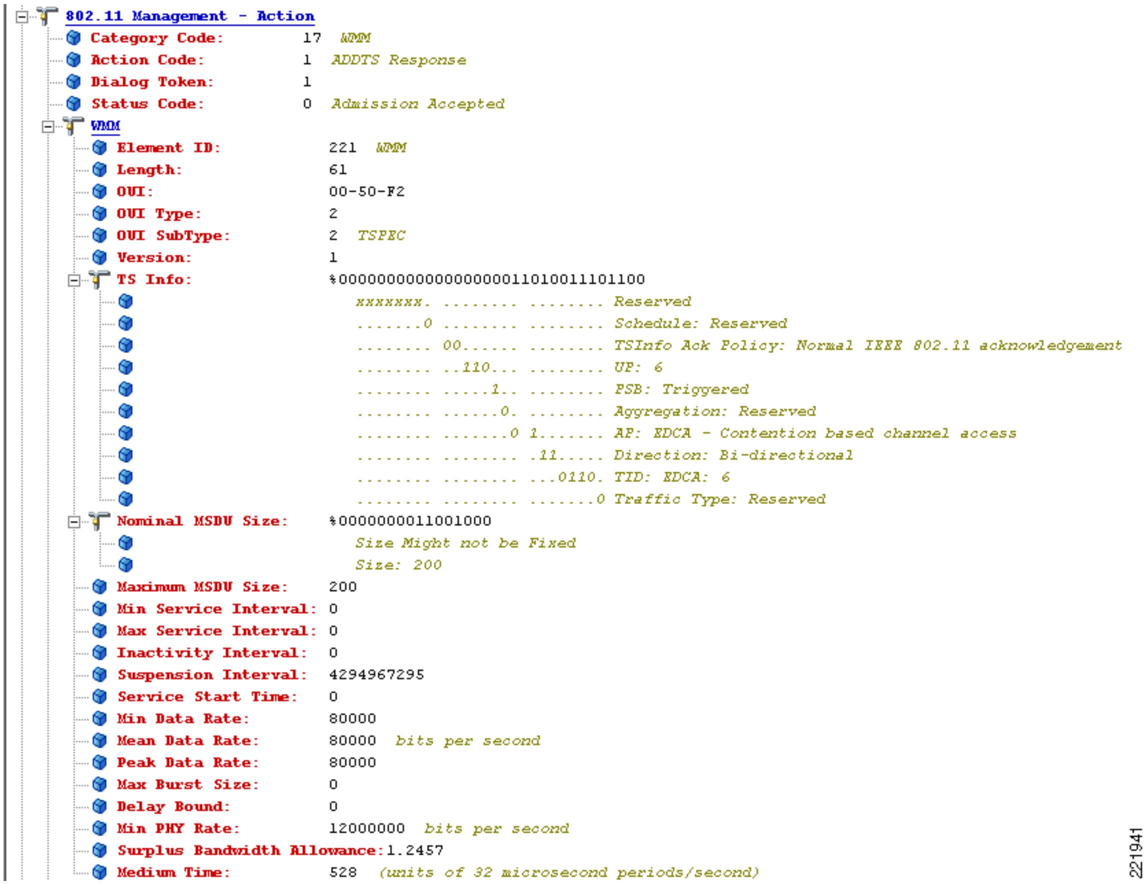
TSpec support is not required by clients. But when a WLAN is configured with call admission control (CAC) for either audio or video that client that is not in support of TSpec is must send the audio and video packets at a Best effort QoS level (see QoS Profiles, page 5-18). So, if the WLAN is set at QoS level of audio or video and CAC is enabled then the correct behavior for a client without ADDTS logic is to send the audio and video traffic with Best effort markings. If a TSpec capable clients has its ADDTS request reject be the Wi-Fi channel utilization is high than the configured CAC limit. That client per specification is supposed to mark the audio and video packets at Best effort.

Figure 5-13 ADDTS Request Decode



```
802.11 Management - Action
  Category Code:          17  WMM
  Action Code:            0   ADDTS Request
  Dialog Token:           1
  Status Code:            0   Admission Accepted
  WMM
    Element ID:              221  WMM
    Length:                  61
    OUI:                     00-50-F2
    OUI Type:                2
    OUI SubType:             2  TSPEC
    Version:                 1
    TS Info:                 %00000000000000000011010011101100
                               xxxxxxx. ........ ........ Reserved
                               .......0 ........ ........ Schedule: Reserved
                               ........ 00...... ........ TSInfo Ack Policy: Normal IEEE 802.11 acknowledgement
                               ........ ..110... ........ UP: 6
                               ........ .....1.. ........ PSB: Triggered
                               ........ ......0. ........ Aggregation: Reserved
                               ........ .......0 1....... AP: EDCA - Contention based channel access
                               ........ ........ .11..... Direction: Bi-directional
                               ........ ........ ...0110. TID: EDCA: 6
                               ........ ........ .......0 Traffic Type: Reserved
    Nominal MSDU Size:       %0000000011001000
                               Size Might not be Fixed
                               Size: 200
    Maximum MSDU Size:       200
    Min Service Interval:    0
    Max Service Interval:    0
    Inactivity Interval:     0
    Suspension Interval:     4294967295
    Service Start Time:      0
    Min Data Rate:           80000
    Mean Data Rate:          80000  bits per second
    Peak Data Rate:          80000
    Max Burst Size:          0
    Delay Bound:             0
    Min PHY Rate:            12000000  bits per second
    Surplus Bandwidth Allowance:1.2457
    Medium Time:             0  (units of 32 microsecond periods/second)
```

Figure 5-14 ADDTS Response Decode



```
802.11 Management - Action
    Category Code:          17  WMM
    Action Code:            1   ADDTS Response
    Dialog Token:           1
    Status Code:            0   Admission Accepted
    WMM
        Element ID:             221  WMM
        Length:                 61
        OUI:                    00-50-F2
        OUI Type:               2
        OUI SubType:            2  TSPEC
        Version:                1
        TS Info:                %000000000000000000110100111011OO
                                   xxxxxxx. ........ ........ Reserved
                                   .......0 ........ ........ Schedule: Reserved
                                   ........ 00...... ........ TSInfo Ack Policy: Normal IEEE 802.11 acknowledgement
                                   ........ ..110... ........ UP: 6
                                   ........ .....1.. ........ PSB: Triggered
                                   ........ ......0. ........ Aggregation: Reserved
                                   ........ .......0 1....... AP: EDCA - Contention based channel access
                                   ........ ........ .11..... Direction: Bi-directional
                                   ........ ........ ...0110. TID: EDCA: 6
                                   ........ ........ .......0 Traffic Type: Reserved
        Nominal MSDU Size:      %0000000011001000
                                   Size Might not be Fixed
                                   Size: 200
        Maximum MSDU Size:      200
        Min Service Interval:   0
        Max Service Interval:   0
        Inactivity Interval:    0
        Suspension Interval:    4294967295
        Service Start Time:     0
        Min Data Rate:          80000
        Mean Data Rate:         80000  bits per second
        Peak Data Rate:         80000
        Max Burst Size:         0
        Delay Bound:            0
        Min PHY Rate:           12000000  bits per second
        Surplus Bandwidth Allowance:1.2457
        Medium Time:            528  (units of 32 microsecond periods/second)
```

Advanced QoS Features for WLAN Infrastructure

In addition to the WMM support described above, the Cisco *Centralized WLAN Architecture* has a number of advanced QoS features. These features include:

- QoS Profiles
- WMM Policy
- Voice over IP Phones
- Admission Control Parameters

These features are described in the following sections.

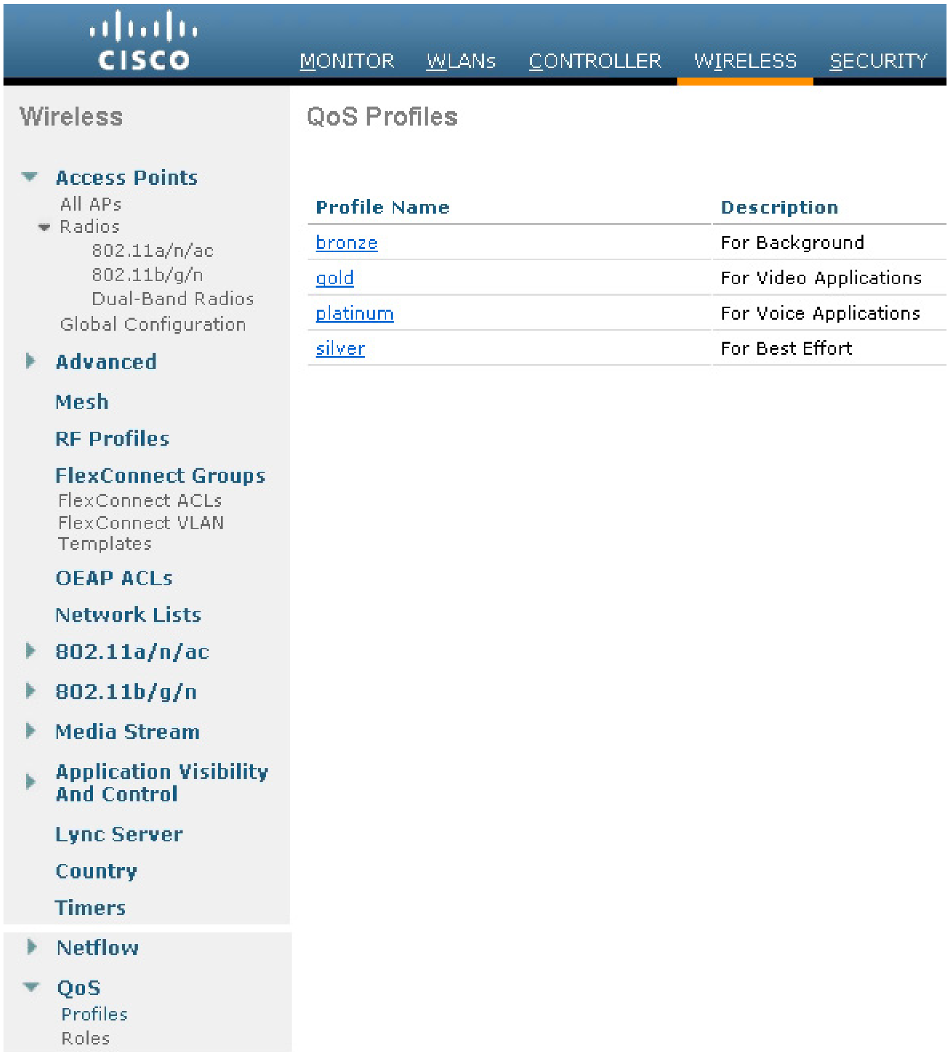
QoS Profiles

Primary among these are the QoS profiles used by the WLC. As shown in Figure 5-15, the QoS profiles can be configured as:

- Bronze—Background
- Gold—Video applications

- Platinum—Voice applications
- Silver—Best effort

Figure 5-15 QoS Profile Options



QoS Profiles

Profile Name	Description
bronze	For Background
gold	For Video Applications
platinum	For Voice Applications
silver	For Best Effort

Each of the profiles shown in Figure 5-15 allows the configuration of bandwidth contracts, RF usage control, and the maximum 802.1P classification allowed.

Note Cisco generally recommends that the Per-User Bandwidth Contracts settings be left at their default values and that the 802.11 WMM features be used to provide differentiated services.

For WLANs using a given profile, Voice or other profile classification in that profile controls two important class of service (CoS) behaviors:

- Determines what CoS value packets initiated from the WLC are marked with.

The value of the CoS parameter is used to mark the CoS of all CAPWAP (*Control And Provisioning of Wireless Access Points*) packets for the WLAN using that profile. So a WLAN with a platinum QoS profile, and the 802.1P mark of 6, will have its CAPWAP packets from the application manager interface of the controller marked with CoS of 5. The WLC adjusts the CoS to be compliant with Cisco QoS baseline recommendations. The reason why it is important to maintain the IEEE CoS marking in the configuration is below. If the WLAN is configured to trust CoS rather than DSCP at the network connection to the WLC, the CoS value is used for the DSCP of the CAPWAP packets received by the AP; and eventually the WMM classification and queuing for WLAN traffic. This is because the WLAN WMM classification of a frame is derived from the DSCP value of the CAPWAP packet carrying that frame.

- Determines the maximum CoS value that can be used by clients connected to that WLAN.

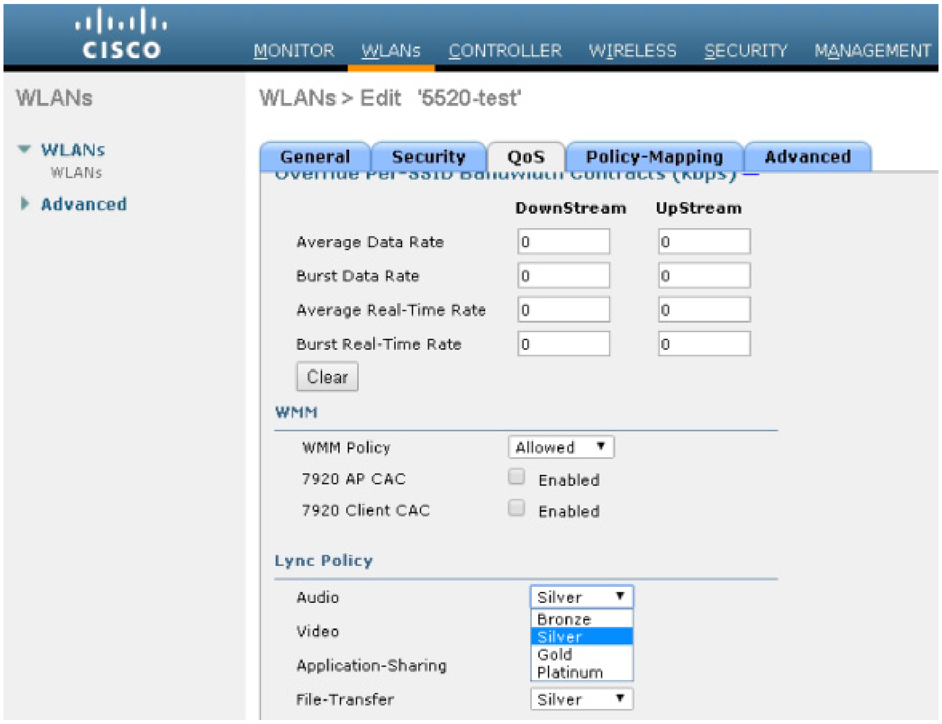
  The 802.1P classification sets the maximum CoS value that is admitted on a WLAN with that profile.

WMM audio traffic arrives with a CoS of 6 at the AP, and the AP automatically performs a CoS-to-DSCP mapping for this traffic based on a CoS of 6. If the CoS value in the WLC configuration is set to a value less than 6, this changed value is used by the WLAN QoS profile at the AP to set the maximum CoS marking used and therefore which WMM admission control (AC) to use.

The key point is that with the Cisco Unified Wireless Network, you should always think in terms of IEEE 802.11e classifications and allow the Unified Wireless Network Solution to take responsibility for converting between IEEE classification and the Cisco QoS baseline.

The WLAN can be configured with various default QoS profiles, as shown in Figure 5-16. Each of the QoS profiles are annotated with their typical use. In addition, clients can be assigned a QoS profile based on their identity, through authentication, authorization and accounting (AAA). For a typical enterprise, WLAN deployment parameters such as per-user bandwidth contracts and over-the-air QoS, should be left at their default values, and standard QoS mechanisms, such as WMM and wired QoS, should be used to provide optimum QoS to clients.

Figure 5-16 WLAN QoS Profile



WLANs > Edit '5520-test'

Override Per-SSID Bandwidth Contracts (kbps)

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WMM Policy: Allowed
7920 AP CAC: ☐ Enabled
7920 Client CAC: ☐ Enabled

Audio: Silver
Video:
Application-Sharing:
File-Transfer: Silver

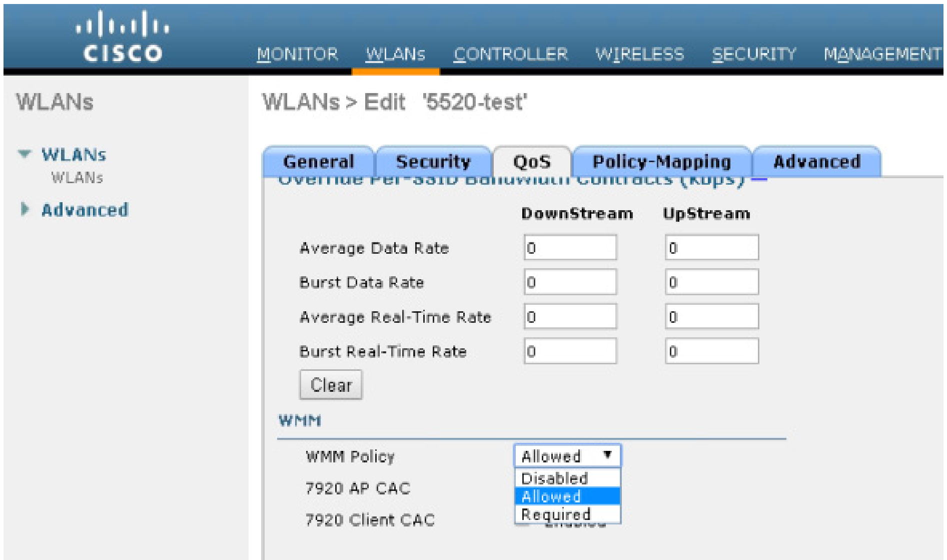
Bronze
Silver
Gold
Platinum

WMM Policy

In addition to QoS profiles, WMM Policy for the WLAN allows you to control additional WMM options, as shown in Figure 5-17. The WMM options are:

- Disabled—The WLAN does not advertise WMM capabilities nor allow WMM negotiations
- Allowed—The WLAN does allow WMM and non-WMM clients
- Required—Only WMM-enabled clients can be associated with this WLAN

Figure 5-17 WLAN WMM Policy



WLANs > Edit '5520-test'

Override Per-SSID Bandwidth Contracts (kbps)

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WMM Policy: Allowed (Disabled / Allowed / Required)

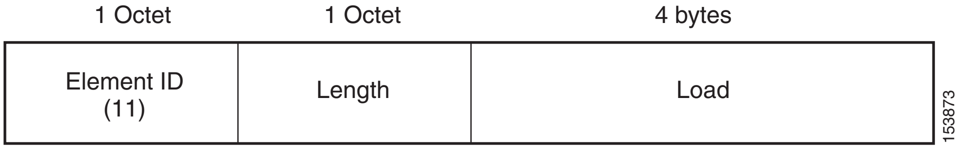
7920 AP CAC

7920 Client CAC

Voice over IP Phones

Figure 5-18 shows the basic QoS Enhanced Basis Service Set (QBSS) information element (IE) advertised by a Cisco AP. The Load field indicates the portion of available bandwidth currently used to transport data on that AP.

Figure 5-18 QBSS Information Element



1 Octet	1 Octet	4 bytes
Element ID (11)	Length	Load

There are actually three QBSS IEs that need to be supported in certain situations:

- Old QBSS—Draft 6 (pre-standard)
- New QBSS—Draft 13 802.11e (standard)
- New distributed CAC load IE—A Cisco information element

The QBSS used depends on the WMM and Cisco 792x VoIP phone settings on the WLAN.

792x phone support, as shown in Figure 5-19, is a component of the WLC WLAN configuration that enables the AP to include the appropriate QBSS element in its beacons. WLAN clients with QoS requirements, such as Cisco 792x phones, use these advertised QoS parameters to determine the best AP with which to associate.

The WLC provides 792x phone support through the client call admission control (CAC) limit. This support includes:

- Client CAC limit—The 7920 uses a call admission control setting that is set on the client. This supports legacy 7920 code-pre 2.01.

- AP CAC limit—The 7920 uses CAC settings learned from WLAN advertisement.

The various combinations of WMM, client CAC limit, and AP CAC limit settings result in different QBSS IEs being sent:

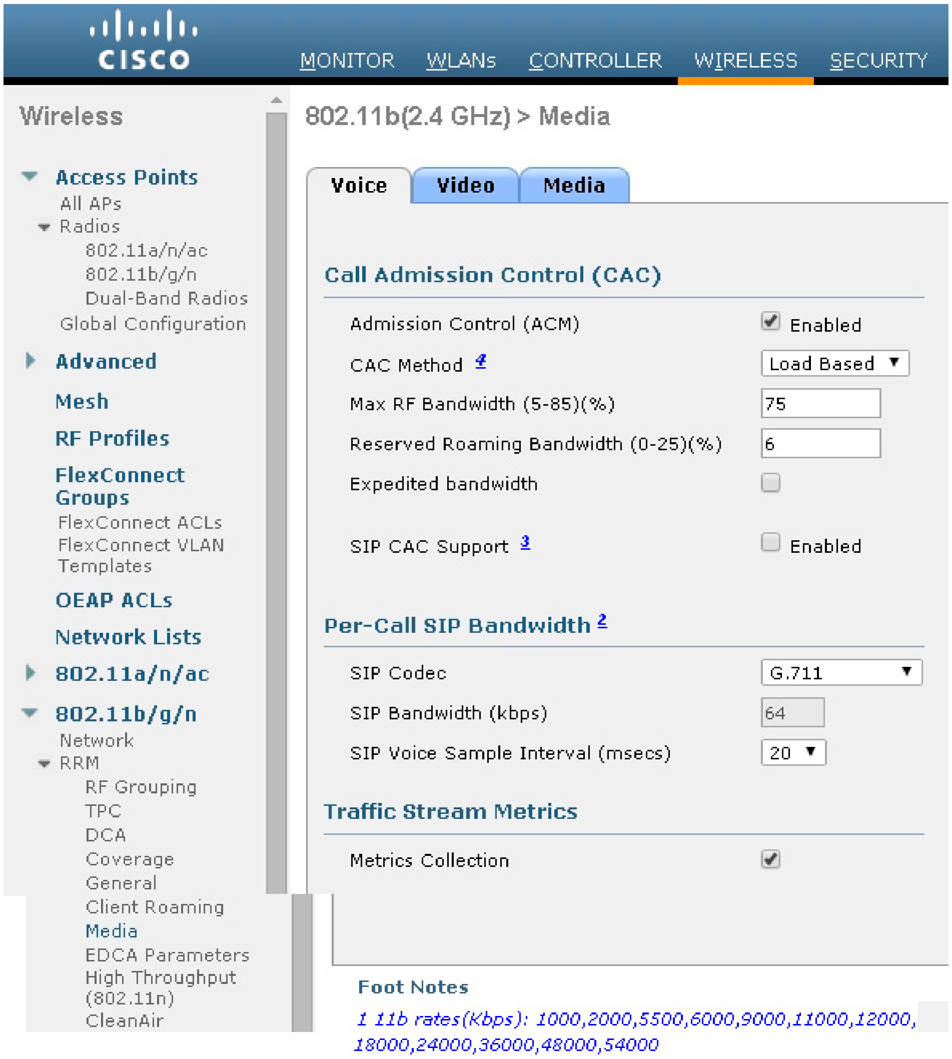
- If only WMM is enabled, IE number 2 (802.11e standard) QBSS Load IE is sent out in the beacons and probe responses.
- If 7920 client CAC limit is to be supported, IE number 1 (the pre-standard QBSS IE) is sent out in the beacons and probe responses on the 802.11b/g radios.
- If 7920 AP CAC limit is to be supported, the number 3 QBSS IE is sent in the beacons and probe responses for bg radios.

Note The various QBSS IEs use the same ID, and therefore the three QBSSs are mutually exclusive. For example, the beacons and probe responses can contain only one QBSS IE.

Admission Control Parameters

Figure 5-19 shows an example of the configuration window for setting the Voice, Video, and Media parameters on the controller.

Figure 5-19 Voice Parameter Setting



802.11b(2.4 GHz) > Media

Call Admission Control (CAC)

Admission Control (ACM) ☑ Enabled
CAC Method 4 Load Based
Max RF Bandwidth (5-85)(%) 75
Reserved Roaming Bandwidth (0-25)(%) 6
Expedited bandwidth ☐
SIP CAC Support 3 ☐ Enabled

Per-Call SIP Bandwidth 2

SIP Codec G.711
SIP Bandwidth (kbps) 64
SIP Voice Sample Interval (msecs) 20

Traffic Stream Metrics

Metrics Collection ☑

Foot Notes

1 11b rates(Kbps): 1000,2000,5500,6000,9000,11000,12000,18000,24000,36000,48000,54000

The CAC parameters include the *Max RF Bandwidth (%)* that a radio can be using and still accept the initiation of a VoWLAN call through a normal ADDTS request. The range of that value is 5 to 85 percent of the channel bandwidth.

The *Reserved Roaming Bandwidth* (%) parameter specifies how much capacity is reserved to be able to respond to ADDTS requests during association or re-association, and which are VoWLAN clients with calls in progress that are trying to roam to that AP.

To enable AC based upon these parameters, select the *Admission Control (ACM)* check box. This enables AC based upon the capacity of the AP but it does not take into account the possible *channel loading* impact of other APs in the area. To include this channel loading in capacity calculations, select the both *Load-Based AC* and *Admission Control (ACM)* check boxes.

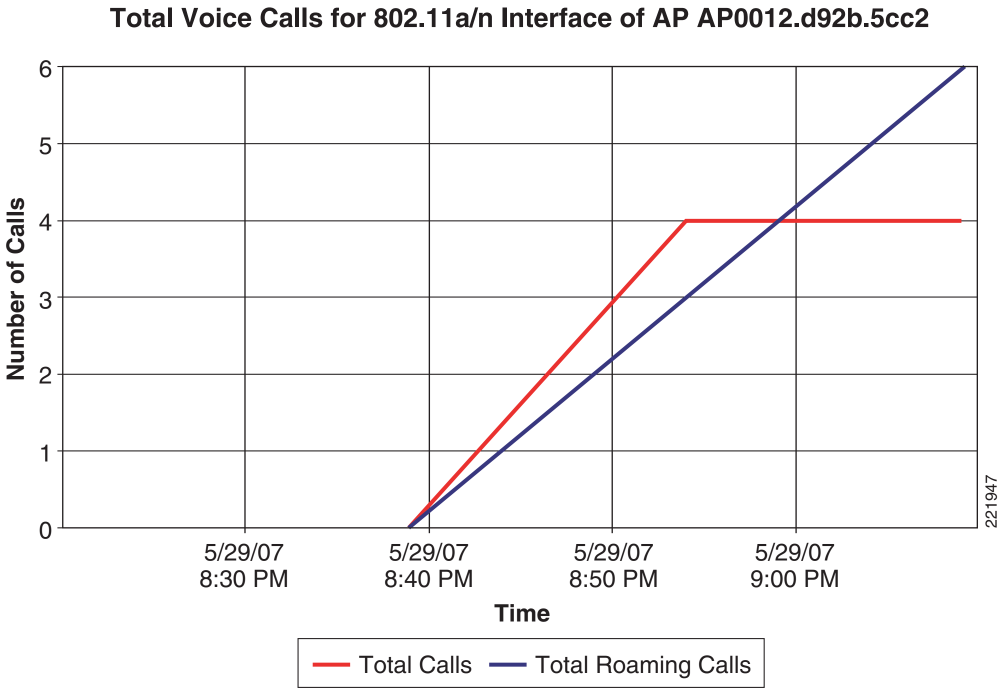
Note Voice and video load-based CAC applies to non-mesh APs. For mesh APs, only static CAC is applicable.

SIP CAC support requires either static or load-based CAC. If you are using *Static* CAC then SIP CAC support allows the configuration of the of the number of calls on the AP. Generally the dynamic the load-balanced approach is the better way of managing quantity of calls to prevent the quality from suffering from over subscription of calls on the Wi-Fi channel.

In the Voice Parameters window (Figure 5-19), the *Metrics Collection* option specifies whether data is collected on audio or video calls for use by Cisco Prime Infrastructure.

Figure 5-20 shows an example of one of the audio statistics reports available with Cisco Prime Infrastructure. The example shows the calls established on the radio of one AP and the number of calls that roamed to that AP. This report and other audio statistics can be scheduled or performed on request (ad-hoc) and either displayed graphically in Cisco Prime Infrastructure or written to a file.

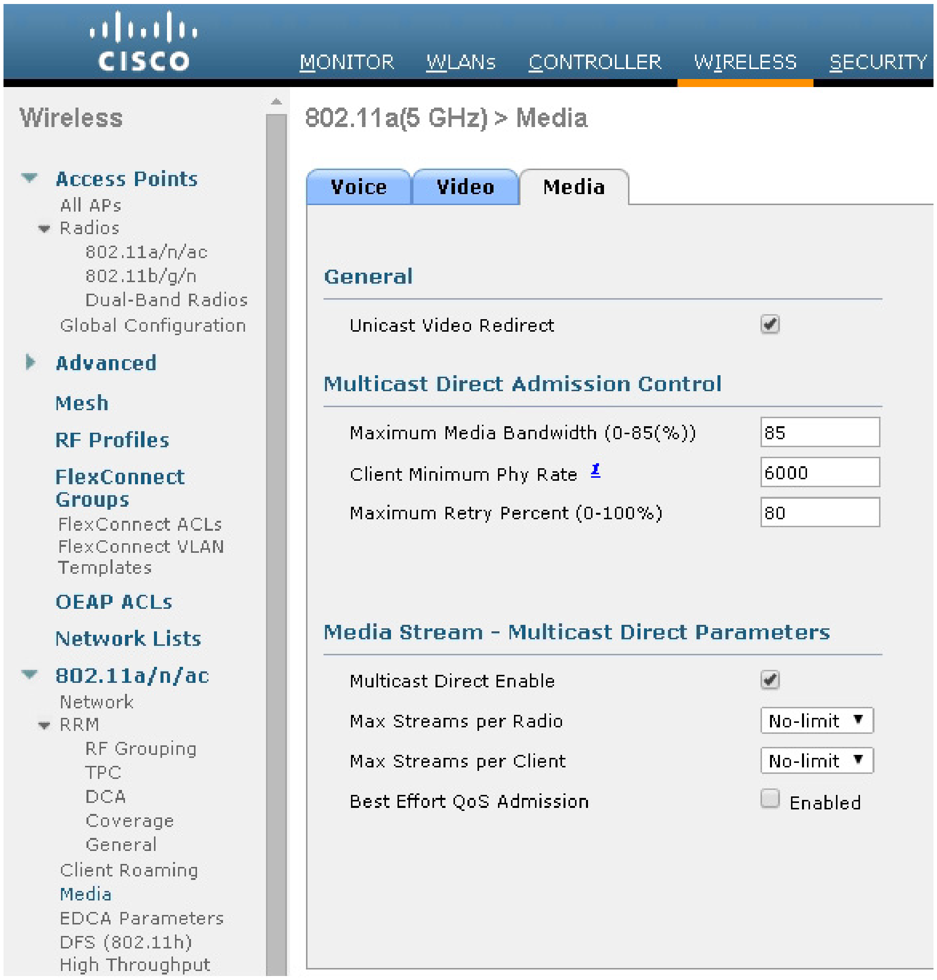
Figure 5-20 Voice Statistics from Cisco Prime Infrastructure



Note CAC is performed only for voice and video QoS profiles.

Figure 5-20 shows the effect of having a low percent of bandwidth set aside for audio CAC calls. Only enough bandwidth was reserved for four calls, but the calls were able to roam to other Wi-Fi channels. Figure 5-21 shows CAC options for media streaming. *Max RF Bandwidth* is shared between the audio, video and media streaming. The Voice, Video, and Media tabs each have their own *Max RF Bandwidth* that are added together for an aggregated total of the complete bandwidth reservation for media on a Wi-Fi channel. While each tab shows a maximum value of 85 percent for the field, the overall Max RF Bandwidth value is actually the sum of all three fields. If Max RF Bandwidth in the Voice tab is set to 85 percent then in video tab and media tabs the Max RF Bandwidth fields must be set to zero percent. If you wanted some bandwidth with CAC behavior on audio, video and data, then you could set the value to 25 percent in the fields of each tab. This would have a channel bandwidth limit for media of 75 percent. With each media type getting one quarter of the bandwidth and with data getting one fourth (1/4) of the bandwidth.

Figure 5-21 WLC 802.11a(5 GHz) Media Window



802.11a(5 GHz) > Media

General

Unicast Video Redirect ☑

Multicast Direct Admission Control

Maximum Media Bandwidth (0-85(%)) 85

Client Minimum Phy Rate 1 6000

Maximum Retry Percent (0-100%) 80

Media Stream - Multicast Direct Parameters

Multicast Direct Enable ☑

Max Streams per Radio No-limit

Max Streams per Client No-limit

Best Effort QoS Admission ☐ Enabled

CAC for video behaves like audio CAC. The purpose of CAC for video is to limit the amount of video calling so that the quality of active video calls is not negatively impacted by additional video being added to the Wi-Fi channel.

Note See the WLC configuration guide for more details on these and the other configuration options.

Impact of TSpec Admission Control

The purpose of TSpec admission control is to protect the high priority resources and not to deny clients access to the WLAN. Therefore, a client that has not used TSpec admission control does not have its traffic blocked; it simply has its traffic re-classified if it tries to transmit (which it should not do if the client is transmitting WMM-compliant traffic in a protected admission control).

Table 5-5 and Table 5-6 describe the impact on classification if admission control is enabled or not and whether or not a traffic stream has been established.

Table 5-5 Upstream Traffic

AC Enabled	Traffic Stream Established	No Traffic Stream
No	No change in behavior; the packets go into the network as they do today-user priority (UP) is limited to max= WLAN QoS setting.	No change in behavior; the packets go into the network as they do today-UP is limited to max= WLAN QoS setting.
Yes	No change in behavior; the packets go into the network as they do today-UP is limited to max= WLAN QoS setting.	Packets are remarked to BE (both CoS and DSCP) before they enter the network for WMM clients. For non-WMM clients, packets are sent with WLAN QoS.

Table 5-6 Downstream Traffic

AC Enabled	Traffic Stream Established	No Traffic Stream
No	No change	No change
Yes	No change	Remark UP to BE for WMM client. For non-WMM clients, use WLAN QoS.

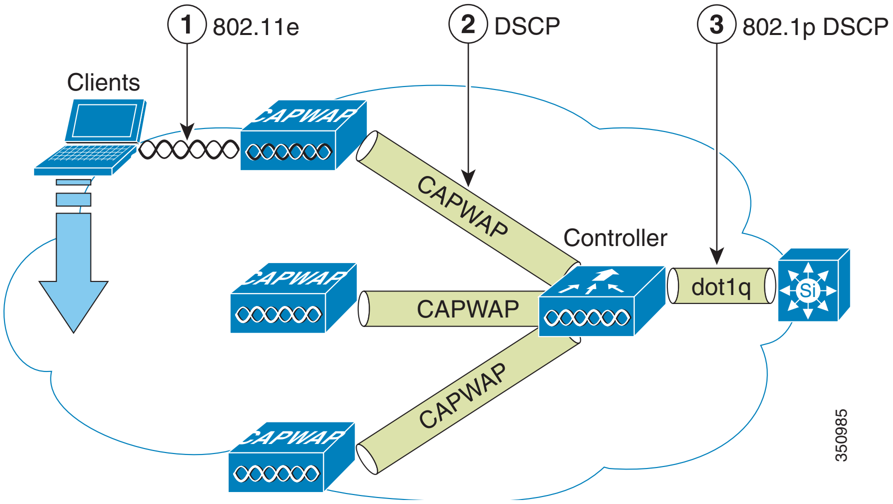
802.11e, 802.1P and DSCP Mapping

WLAN data in a Unified Wireless Network is tunneled by way of CAPWAP (IP UDP packets). To maintain the QoS classification that has been applied to WLAN frames, the WLC uses a process of mapping classifications to and from DSCP and CoS. For example, when WMM classified traffic is sent by a WLAN client, it has an 802.1P classification in its frame. The AP needs to translate this classification into a DSCP value for the CAPWAP packet carrying the frame to ensure that the packet is treated with the appropriate priority on its way to the WLC. A similar process must occur on the WLC for CAPWAP packets going to the AP.

A mechanism to classify traffic from non-WMM clients is also required so that their CAPWAP packets can also be given an appropriate DSCP classification (see Classification Considerations, page 5-33) by the AP and the WLC.

Figure 5-22 shows the various classification mechanisms in the CAPWAP WLAN network.

Figure 5-22 WMM and 802.1P Relationship



Multiple classification mechanisms and client capabilities require multiple strategies. These strategies include:

- CAPWAP control frames require prioritization so they are marked with a DSCP classification of CS6 (an IP routing class).
- WMM-enabled clients have the classification of their frames mapped to a corresponding DSCP classification for CAPWAP packets to the WLC. This mapping follows the standard IEEE CoS-to-DSCP mapping, with the exception of the changes necessary for QoS baseline compliance. This DSCP value is translated at the WLC to a CoS value on 802.1Q frames leaving the WLC interfaces.
- Non-WMM clients have the DSCP of their CAPWAP tunnel set to match the default QoS profile for that WLAN. For example, the QoS profile for a WLAN supporting 792x phones would be set to platinum, resulting in a DSCP classification of EF for data frames packets from that AP WLAN.
- CAPWAP data packets from the WLC have a DSCP classification that is determined by the DSCP of the wired data packets sent to the WLC. The 80211.e classification used when transmitting frames from the AP to a WMM client is determined by the AP table converting DSCP to WMM classifications.

Note The WMM classification used for traffic from the AP to the WLAN client is based on the DSCP value of the CAPWAP packet, and not the DSCP value of the contained IP packet. Therefore, it is critical that an end-to-end QoS system be in place.

QoS Baseline Priority Mapping

The CAPWAP AP and WLC perform QoS baseline conversion so that WMM values, as described in Table 5-7, are mapped to the appropriate QoS baseline DSCP values, rather than the IEEE values.

Table 5-7 Access Point QoS Translation Values[1]

AVVID 802.1 UP-Based Traffic Type	AVVID IP DSCP	AVVID 802.1p UP	IEEE 802.11e UP
Network control	56	7	—
Inter-network control (CAPWAP control, 802,11 management	48	6	7
Voice	46 (EF)	5	6
Video	34 (AF41)	4	5
Voice Control	26 (AF31)	3	4
Background (gold)	18 (AF21)	2	2
Background (gold)	20 (AF22)	2	2
Background (gold)	22 (AF23)	2	2
Background (silver)	10 (AF11)	1	1
Background (silver)	12 (AF12)	1	1
Background (silver)	14 (AF13)	1	1
Best Effort	0 (BE)	0	0, 3
Background	2	0	1
Background	4	0	1
Background	6	0	1

[1] The IEEE 802.11e UP (user priority) value for DSCP values that are not mentioned in the table is calculated by considering 3 MSB bits of DSCP. For example, the IEEE 802.11e UP value for DSCP 32 (100 000 in binary), would be the decimal converted value of the MSB (100) which is 4. The 802.11e UP value of DSCP 32 is 4.

Deploying QoS Features on CAPWAP-based APs

When deploying WLAN QoS features on the APs, consider the following:

- The wired CAPWAP AP interface reads or writes Layer 2 CoS (802.1P) information. The WLC and the APs depend on Layer 3 classification (DSCP) information to communicate WLAN client traffic classification. This DSCP value could be subject to modification by intermediate routers, and therefore the Layer 2 classification received by the destination might not reflect the Layer 2 classification marked by the source of the CAPWAP traffic.
- The APs no longer use NULL VLAN ID. As a consequence, Layer 2 CAPWAP does not effectively support QoS because the AP does not send the 802.1P/Q tags and in Layer 2 CAPWAP there is no outer DSCP on which to fall back.
- APs do not re-classify frames; they prioritize them based on CoS value or WLAN profile.
- APs carry out EDCF-like queuing on the radio egress port only.
- APs do FIFO queuing only on the Ethernet egress port.

WAN QoS and FlexConnect

For WLANs that have data traffic forwarded to the WLC, the behavior is same as non-hybrid remote edge FlexConnect APs. For locally-switched WLANs with WMM traffic, FlexConnect APs mark the dot1p value in the dot1q VLAN tag for upstream traffic. This occurs only on tagged non-native VLANs.

For downstream traffic, FlexConnect APs use the incoming dot1q tag from the Ethernet side and then use this to queue and mark the WMM values on the radio of the locally-switched VLAN.

The WLAN QoS profile is applied to both upstream and downstream packets. For downstream traffic, if an 802.1P value that is higher than the default WLAN value is received, the default WLAN value is used. For upstream traffic, if the client sends an WMM value that is higher than the default WLAN value, the default WLAN value is used. For non-WMM traffic there is no CoS marking on the client frames from the AP.

Guidelines for Deploying Wireless QoS

The same rules for deploying QoS in a wired network apply to deploying QoS in a WLAN. The first and most important guideline in QoS deployment is to know your traffic. Know your protocols, the sensitivity to delay of your application, and traffic bandwidth. QoS does not create additional bandwidth, it simply gives more control over where the bandwidth is allocated.

QoS LAN Switch Configuration Example

AP Switch Configuration

The QoS configuration of the AP switch is minor because the switch must trust the DSCP of the CAPWAP packets that are passed to it from the AP. There is no CoS marking on the CAPWAP frames coming from the AP. Below is an example of this configuration. Note that this configuration addresses only the classification and that queuing commands can be added depending on local QoS policy.

```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 mls qos trust dscp
 spanning-tree portfast
end
```

In trusting the AP DSCP values, the access switch is trusting the policy set for that AP by the WLC. The maximum DSCP value assigned to client traffic is based on the QoS policy applied to the WLAN on that AP.

WLC Switch Configuration

The QoS classification decision at the WLC-connected switch is slightly more complicated than at the AP-connected switch because the choice can be to either trust the DSCP or the CoS of traffic coming from the WLC. When making this decision, consider the following:

- Traffic leaving the WLC can be either upstream (to the WLC or network) or downstream (to the AP and WLAN client). The downstream traffic is CAPWAP encapsulated, and the upstream traffic is either CAPWAP encapsulated or decapsulated WLAN client traffic leaving the WLC.
- DSCP values of CAPWAP packets are controlled by the QoS policies on the WLC; the DSCP values set on the WLAN client traffic (encapsulated by the CAPWAP tunnel header) has not been altered from those set by the WLAN client.
- CoS values of frames leaving the WLC are set by the WLC QoS policies, regardless of whether they are upstream, downstream, encapsulated, or decapsulated.

The following example chooses to trust the CoS settings of the WLC because this allows a central location for the management of WLAN QoS rather than having to manage the WLC configuration and an additional policy at the WLC switch connection.

```
interface GigabitEthernet1/0/13
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 11-13,60,61
 switchport mode trunk
 mls qos trust cos
end
```

If you want to have a more precise degree of control you can implement QoS classification policies on the WLAN-client VLANs.

Traffic Shaping, Over the Air QoS, and WMM Clients

Traffic shaping and over-the-air QoS are useful tools in the absence of WLAN WMM features, but they do not address the prioritization of 802.11 traffic directly. For WLANs that support WMM clients or 792x handsets, the WLAN QoS mechanisms of these clients should be relied on; no traffic shaping or over-the-air QoS should be applied to these WLANs.

WLAN Voice and Cisco Phones

The data sheets for Cisco Unified Communication Endpoints can be found at:

http://www.cisco.com/en/US/prod/voicesw/ps6788/ip_phones.html

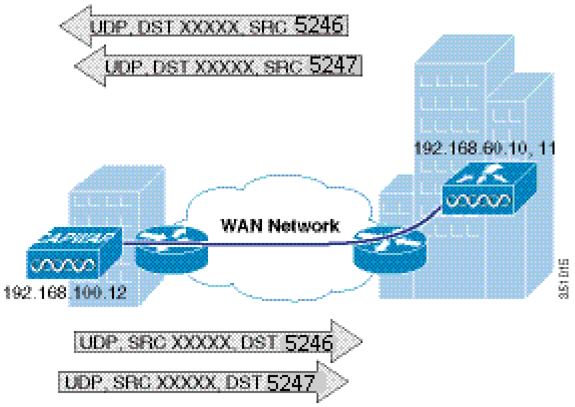
For a general overview of Cisco Jabber, see:

http://www.cisco.com/web/products/voice/jabber.html

CAPWAP over WAN Connections

This section describes QoS strategies when CAPWAP APs are deployed across WAN links, as shown in Figure 5-23.

Figure 5-23 CAPWAP Traffic Across the WAN



CAPWAP Traffic Classification

CAPWAP APs can be generally separated into the following two types:

- CAPWAP control traffic—Identified by UDP port 5246
- CAPWAP 802.11 traffic—Identified by UPD port 5247

CAPWAP Control Traffic

CAPWAP control traffic can be generally divided into the following two additional types:

- Initialization traffic—Generated when a CAPWAP AP is booted and joins a CAPWAP system. For example, initialization traffic could be generated by controller discovery, AP configuration, and AP firmware updates.

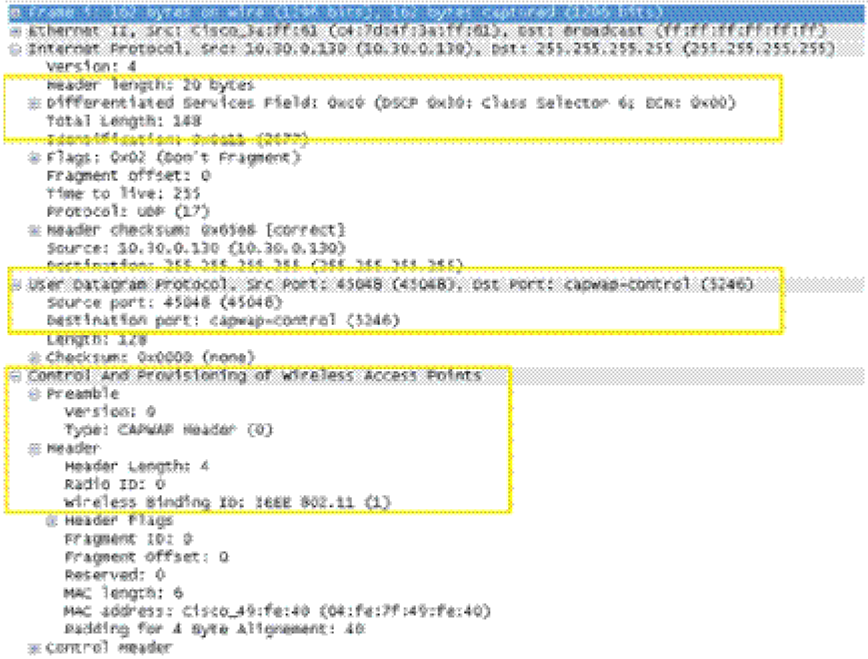
Note CAPWAP image packets from the controller are marked best effort, but their acknowledgement is marked CS6. Note that no sliding window protocol is used and each additional packet is sent only after an acknowledgement. This type of handshaking minimizes the impact of downloading files over a WLAN.

- Background traffic—Generated by an CAPWAP AP when it is an operating member of a WLAN network. Examples included CAPWAP heartbeat, radio resource management (RRM), and rogue AP measurements. Background CAPWAP control traffic is marked CS6.

Figure 5-23 show an example of an initial CAPWAP control message. The list of initial CAPWAP control messages includes:

- CAPWAP discovery messages
- CAPWAP join messages
- CAPWAP configuration messages
- Initial CAPWAP RRM messages

Figure 5-24 CAPWAP Discovery Request on a WISM-2



```
Frame 1: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
Ethernet II, Src: Cisco_3a:ff:61 (c4:7d:4f:3a:ff:61), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 10.30.0.130 (10.30.0.130), Dst: 255.255.255.255 (255.255.255.255)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
  Total Length: 148
  Identification: [illegible]
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 255
  Protocol: UDP (17)
  Header checksum: [illegible] [correct]
  Source: 10.30.0.130 (10.30.0.130)
  Destination: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: 45048 (45048), Dst Port: capwap-control (5246)
  Source port: 45048 (45048)
  Destination port: capwap-control (5246)
  Length: 128
  Checksum: 0x0000 (none)
Control And Provisioning of Wireless Access Points
  Preamble
    Version: 0
    Type: CAPWAP Header (0)
  Header
    Header Length: 4
    Radio ID: 0
    Wireless Binding ID: IEEE 802.11 (1)
    Header Flags
    Fragment ID: 0
    Fragment offset: 0
    Reserved: 0
    MAC length: 6
    MAC address: Cisco_49:fe:40 (04:fe:7f:49:fe:40)
    Padding for 4 Byte Alignment: 40
  Control Header
```

CAPWAP 802.11 Traffic

CAPWAP 802.11 traffic can be divided generally into the following two additional types:

- 802.11 management frames—802.11 management frames such as probe requests and association requests/responses are classified automatically with a DSCP of CS6.
- 801.11 data frames—Client data and 802.1X data from the client is classified according to the WLAN QoS settings, but packets containing 802.1X frames from the WLC are marked CS4. 802.11 data traffic classification depends on the QoS policies applied in the WLAN configuration and is not automatic. The default classification for WLAN data traffic is Best effort.

Classification Considerations

The DSCP classification used for CAPWAP control traffic is CS6 (an IP routing class) and is intended for IP routing protocols such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), and others.

The current CAPWAP DSCP classification represents a classification that, although optimal for the WLAN system, might not align with your QoS policies and needs.

In particular, you might want to minimize the amount of CS6-classified traffic generated by the WLAN network. You might want to stop CS6 traffic generated by client activity such as probe requests. The easiest way to do this is to reclassify the CAPWAP 802.11 CS6 traffic to be a DSCP value with a lower QoS priority. The fact that the CAPWAP UDP port used is different from that used by CAPWAP data, and the default DSCP marking, allow for remarking this traffic without resorting to deep packet inspection.

In addition, you might want to ensure that CAPWAP initialization traffic does not impact routing traffic. The easiest way to ensure this is to mark with a lower priority the CAPWAP control traffic that is in excess of the background rate.

Router Configuration Examples

This section provides examples of router configurations that you can use as guides when addressing CS6 remarking or CAPWAP control traffic load.

The examples use CAPWAP APs on the 192.168.101.0/24 subnet and two WLCs with AP managers at 192.168.60.11 and 192.168.62.11.

Remarking Client Generated CS6 Packets

The following example shows a router configuration for remarking CAPWAP data packets marked as CS6 to a more appropriate value of CS3. This moves the traffic to a more suitable classification, at the level of call control, rather than at the level of network control.

```
class-map match-all CAPWAPDATACS6
 match access-group 110
 match  dscp cs6
!
policy-map CAPWAPDATACS6
 class CAPWAPDATACS6
  set dscp cs3
!
interface FastEthernet0
 ip address 192.168.203.1 255.255.255.252
service-policy input CAPWAPDATACS6
!
access-list 110 remark CAPWAP Data
access-list 110 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 5247
access-list 110 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 5247
access-list 111 remark CAPWAP Control
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 5246
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 5246
```

Changing the DSCP of CAPWAP Control Traffic above a predefined rate

The following is an example of rate limiting the CAPWAP control traffic from the WAN site to minimize the impact of the CS6-marked control traffic on routing traffic. Note that the rate limit configuration does not drop non-conforming traffic, but simply reclassifies that traffic.

Note The following is an example and not a recommendation. Under normal circumstances, and following the design guidelines for deploying APs over a WAN connection, it is unlikely that CAPWAP control traffic would impact the WAN routing protocol connection.

```
interface Serial0
 ip address 192.168.202.2 255.255.255.252
 rate-limit output access-group 111 8000 3000 6000 conform-action transmit exceed-action
set-dscp-transmit 26
access-list 111 remark CAPWAP Control
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 5246
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 5246
!
```

For more information on WLAN QoS and 802.11e, see the *IEEE 802.11 Handbook: A Designer's Companion, 2nd Edition*, by Bob O'Hara and Al Petrick. ISBN: 978-0-7381-4449-8

QoS Mapping in Release 8.1 MR1

Currently, there is a misalignment between the Differentiated Services Code Point (DSCP) and User Priority (UP) mappings between different vendors of clients and APs. This leads to confusion as different DSCP values imply different UP in different hardware. So, the same packet sent by two different clients (A) and (B) with the same DSCP can have different UP, depending on the internal DSCP – UP map that client uses. Similarly, when a packet leaves the AP to the client, the DSCP – UP map can be different. So, a particular DSCP does not guarantee a particular UP across the same network.

The solution, proposed as part of 802.11u standard, is available in 8.1MR1 code and above:

- Provide a way for user to configure DSCP to UP mapping in the WLC.
- When a capable client joins, transmit the QoS map from an AP to a non-AP STA in a Reassociation Response frame.
- If a change is made to this map when an AP is already associated, the map is transmitted as an unsolicited frame.

With this enhancement, when sending packets, all clients will use the same QoS map. This results in the same UP being used, independent of the manufacturer of the client.

Clients not compatible with 802.11u standard will not receive the frames with QoS map. However, the packets sent by these clients will follow the new DSCP – UP map that has been configured.

When QoS Map is disabled, the current default map is pushed to the AP and the clients. Table 5-8 shows the default QoS mapping.

Table 5-8 Default QoS Mapping

A VVID 802.1p UP based Traffic Type	A VVID 802.1p CoS	A VVID IP DSCP	IEEE IP DSCP	IEEE 802.11e UP	Comments
Reserved (Network Control)	7	56	56	7	TBD
Reserved	6	48	—	—	TBD
Voice	5	46 (EF)	48	6	
Video	4	34 (AF41)	40	5	
Voice Control	3	26 (AF31)	32	4	
Background (Gold)	2	18 (AF21)	16	3	
Background (Gold)	2	20 (AF22)	16	3	
Background (Gold)	2	22 (AF23)	16	3	
Background (Silver)	1	10 (AF11)	8	2	
Background (Silver)	1	12 (AF12)	8	2	
Background (Silver)	1	14 (AF13)	8	2	
Best Effort	0	0 (BE)	0, 24	0	
Background	0	2	8	1	
Background	0	4	8	1	

Table 5-8 Default QoS Mapping

A VVID 802.1p UP based Traffic Type	A VVID 802.1p CoS	A VVID IP DSCP	IEEE IP DSCP	IEEE 802.11e UP	Comments
Background	0	6	8	1	
Unknown DSCP from Wired	Access Port	D	Do Not Care	D >> 3	On the AP

Configuring QoS Mapping by Controller administrator

The controller administrator can configure QoS mapping:

- Lower to Upper DSCP ranges for all UP from 0 to 7. The QoS Map Set has a DSCP Range field corresponding to each of the 8 user priorities. The DSCP Range value is between 0 and 63 inclusive, or 255.
  - The DSCP range for each user priority is non-overlapping.
  - The DSCP high value is greater than or equal to the DSCP low value.
  - If the DSCP range high value and low value are both equal to 255, then the corresponding UP is not used.
- DSCP exceptions to explicitly mark certain DSCPs to a certain UP. DSCP Exception fields are optionally included in the QoS Map Set. If included, the QoS Map Set has a maximum of 21 DSCP Exception fields.
- Enable/ Disable QoS Map.
- User configured mapping is transmitted to clients and used for both Up Stream and Down Stream traffic.

Note Currently, we cap an incoming DSCP packet based on the configured QoS profile. There exists a default DSCP value for each QoS profile. Any packet with DSCP value greater than this is capped to this default value.

With QoS Map, the capping values need to be dynamic. All UPs are configured with a lower to higher DSCP range. The capping values should be the upper DSCP of the QoS Profile UP. For example, UP 5 is configured with 30 to 40. So, Gold QoS Profile should be capped with DSCP 40.

Configuring QoS Mapping from CLI

To compensate for the possible incorrect or unexpected markings, AireOS controller code 8.1MR1 offers the possibility to configure a customized DSCP to UP, and UP to DSCP translation table. You can also trust the DSCP marking on the client 802.11 upstream frames, instead of the 802.11e UP marking.

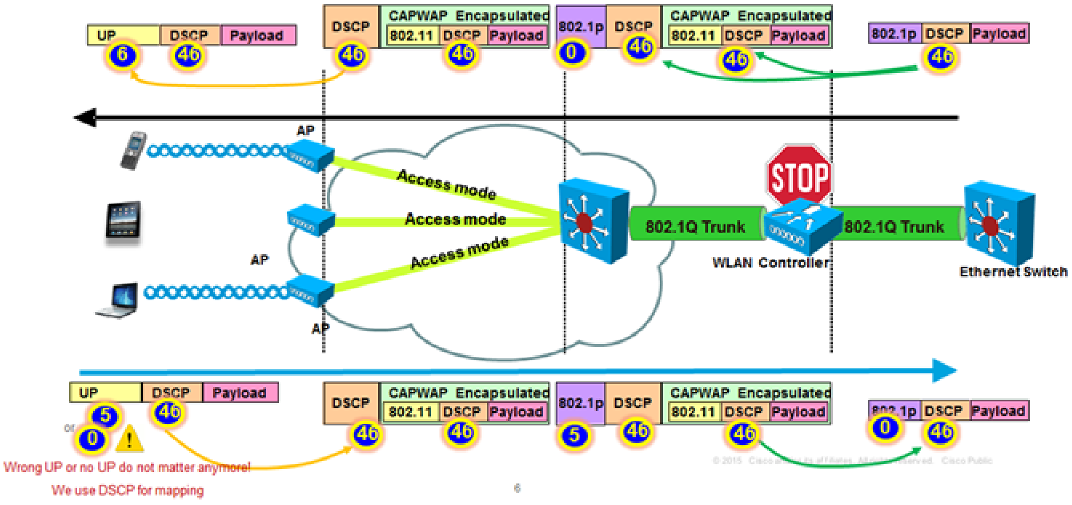
Trusting DSCP upstream is enabled from the controller command line with two commands:

```
(Cisco Controller) >config qos qosmap trust-dscp-upstream enable
```

```
(Cisco Controller) >config qos qosmap enable
```

When you enable this feature, DSCP is used instead of UP. DSCP is already used to determine the CAPWAP outer header QoS marking downstream. Therefore, the logic of downstream marking is unchanged. In the upstream direction though, trusting DSCP compensates for unexpected or missing UP marking. The AP will use the incoming 802.11 frame DSCP value to decide the CAPWAP header outer marking. The QoS profile ceiling logic still applies, but the marking logic operates on the frame DSCP field instead of the UP field. In a platinum profile, DSCP 46 is maintained in the outer header for the upstream traffic, even if UP is absent or unexpected.

Figure 5-25 An Example: Effect of Platinum Profile – 8.1 MR

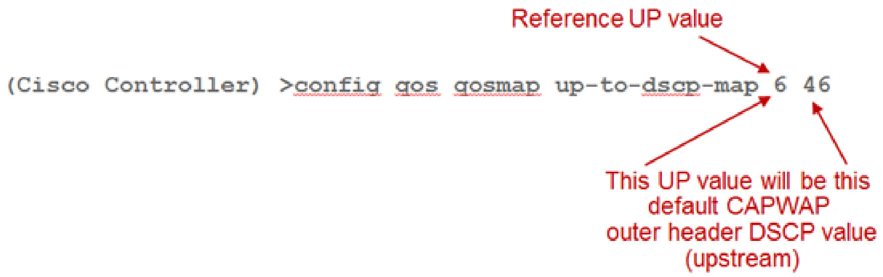


Note DSCP trust model (wireless client uses unexpected UP)

In a Video profile, DSCP would still be capped to 34. In other words, DSCP is used to derive the CAPWAP outer header DSCP value upstream and downstream, but the QoS profile ceiling still applies.

AireOS controller code 8.1 MR1 also allows you to manually define the DSCP to UP and UP to DSCP translation values. This flexibility allows you to face any upstream and downstream unexpected QoS markings and still maintain a consistent policy. The UP to DSCP and DSCP to UP customized mapping is configured in a single command. For example, suppose that UP 6 should always translate to DSCP 46 upstream, you would configure this combination with the following command:

(Cisco Controller) >**config qos qosmap up-to-dscp-map 6 46**

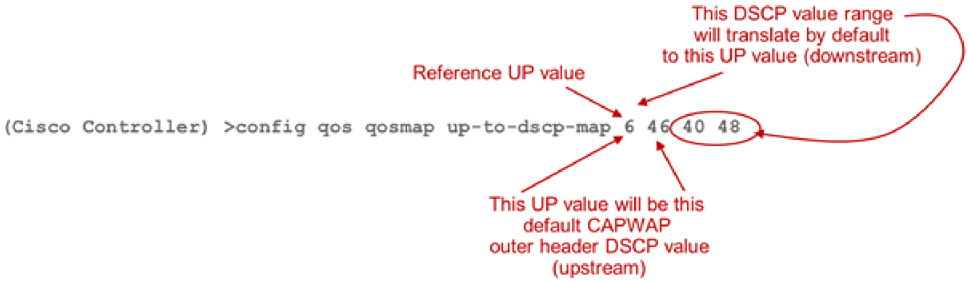


```
(Cisco Controller) >config qos qosmap up-to-dscp-map 6 46
```

Reference UP value
This UP value will be this default CAPWAP outer header DSCP value (upstream)

The same command can be extended to also configure the reverse mapping. For example, suppose that DSCP 40 to 48 should translate to UP 6 downstream, you would configure this combination with the following command:

(Cisco Controller) >**config qos qosmap up-to-dscp-map 6 46 40 48**



```
(Cisco Controller) >config qos qosmap up-to-dscp-map 6 46 40 48
```

This DSCP value range will translate by default to this UP value (downstream)
Reference UP value
This UP value will be this default CAPWAP outer header DSCP value (upstream)

Note that the above configuration is not intended to be a recommended configuration, but is just an example. You would configure with the same logic the 7 UPs and their DSCP mapping. Also, note that the default value upstream (46 in the example above) does not need to be in the range defined for the downstream direction (40 to 48 in the example above). For example, suppose that you decided that UP 6 should translate upstream to DSCP 34, but also that downstream DSCP 40 to 48 should translate to UP 6, you could enter the following command (this is a possibility, not a recommended configuration):

```
(Cisco Controller) >config qos qosmap up-to-dscp-map 6 34 40 48
```

You can also configure exceptions in the range for the downstream traffic DSCP to UP mapping. For example, suppose that a specific traffic marked DSCP 44 should translate to UP 5 in your network, you could configure the 40 to 48 range to translate to UP 6, with an exception for DSCP 44, as follows:

```
(Cisco Controller) >config qos qosmap up-to-dscp-map 6 46 40 48
(Cisco Controller) >config qos qosmap dscp-to-up-exception 44 5
```

Note that this exception applies to the downstream mapping, not to the upstream mapping. The upstream mapping will follow the rules determined by the up to DSCP map.

Configuring QOS Maps on Cisco AireOS Release 8.1 MR1

To configure QoS maps, perform the following steps:

Step 1 To configure the manual mapping, make sure that your target networks are disabled, as you are going to change the way these networks forward frames:

```
(Cisco Controller) >config 802.11a disable network
(Cisco Controller) >config 802.11b disable network
```

Step 2 QoS maps are disabled by default. If you enabled the maps, temporarily disable the custom mapping to make changes:

```
(Cisco Controller) >config qos qosmap disable
```

QoS map is now disabled.

Step 3 Configure the custom UP to DSCP and DSCP to UP mapping. Note that you have to configure all 7 UPs to enable customization. For example:

```
(Cisco Controller) >config qos qosmap up-to-dscp-map 0 0 0 63
(Cisco Controller) >config qos qosmap up-to-dscp-map 1 8
(Cisco Controller) >config qos qosmap up-to-dscp-map 2 10
(Cisco Controller) >config qos qosmap up-to-dscp-map 3 18
(Cisco Controller) >config qos qosmap up-to-dscp-map 4 34
```

```
(Cisco Controller) >config qos qosmap up-to-dscp-map 5 32
(Cisco Controller) >config qos qosmap up-to-dscp-map 6 46
(Cisco Controller) >config qos qosmap up-to-dscp-map 7 0
```

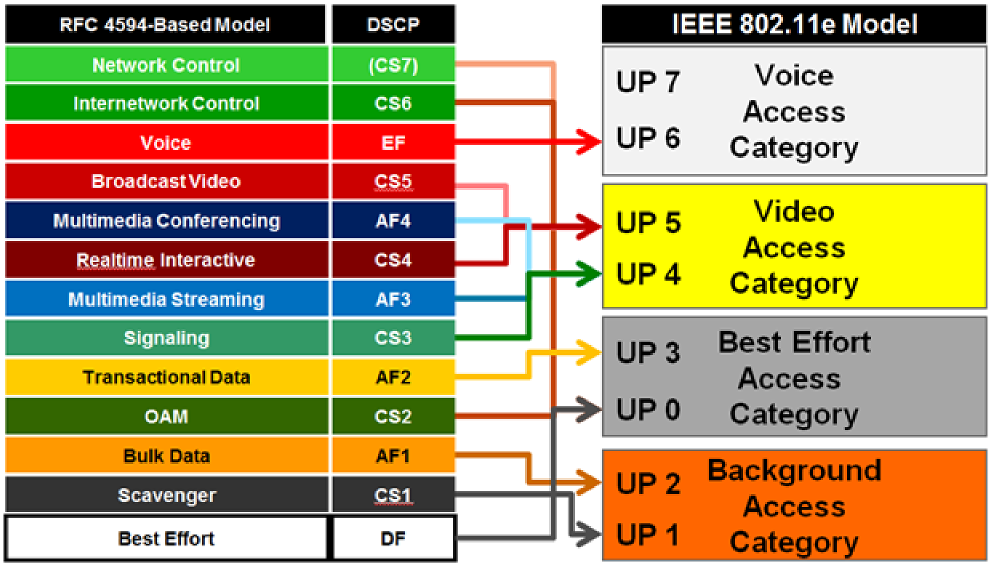
The first line achieves two objectives: map UP 0 to DSCP 0, but also maps all DSCP values to UP 0. This allows you to be compliant with IETF RFC 4594 section 3.1 and reset all unspecified DSCP values to 0.

Step 4 Configure exceptions for standard traffic, for example as follows:

```
(Cisco Controller) >config qos qosmap dscp-to-up-exception 8 1
(Cisco Controller) >config qos qosmap dscp-to-up-exception 10 2
(Cisco Controller) >config qos qosmap dscp-to-up-exception 12 2
(Cisco Controller) >config qos qosmap dscp-to-up-exception 14 2
(Cisco Controller) >config qos qosmap dscp-to-up-exception 16 0
(Cisco Controller) >config qos qosmap dscp-to-up-exception 18 3
(Cisco Controller) >config qos qosmap dscp-to-up-exception 20 3
(Cisco Controller) >config qos qosmap dscp-to-up-exception 22 3
(Cisco Controller) >config qos qosmap dscp-to-up-exception 24 4
(Cisco Controller) >config qos qosmap dscp-to-up-exception 26 4
(Cisco Controller) >config qos qosmap dscp-to-up-exception 28 4
(Cisco Controller) >config qos qosmap dscp-to-up-exception 30 4
(Cisco Controller) >config qos qosmap dscp-to-up-exception 32 5
(Cisco Controller) >config qos qosmap dscp-to-up-exception 34 4
(Cisco Controller) >config qos qosmap dscp-to-up-exception 36 4
(Cisco Controller) >config qos qosmap dscp-to-up-exception 38 4
(Cisco Controller) >config qos qosmap dscp-to-up-exception 40 5
(Cisco Controller) >config qos qosmap dscp-to-up-exception 46 6
```

These exceptions map standard DSCP values to the appropriate UP values. Note that this command allows you to configure up to 21 exceptions.

The above configuration reflects Cisco recommended mapping depicted in the following illustration.



Step 5 You can also decide to use the wireless client packet DSCP in the upstream direction, instead of the UP value. Note that if you enable DSCP trust upstream, you will not use the UP to DSCP translation values for the upstream traffic. However, you will still use the DSCP ranges to UP translations for the downstream traffic, as well as any exceptions:

(Cisco Controller) >**config qos qosmap trust-dscp-upstream enable**

The DSCP trust upstream is enabled.

Step 6 At any time during your configuration, you can remove the exceptions you created:

(Cisco Controller) >**config qos qosmap delete-dscp-exception**

Step 7 You can also delete the manual mapping entirely:

(Cisco Controller) >**config qos qosmap default**

Step 8 Once your configuration is complete, you can verify the mapping:

(Cisco Controller) >**show qos qosmap**

```
Status: Disabled
        UP-TO-DSCP Map:
        Up      Default DSCP    Start DSCP      End DSCP
        0       0               0               63
        1       8
        2       10
        3       18
        4       34
        5       32
        6       46
        7       0
        Exception List:
        DSCP    UP
        8        1
        10       2
        12       2
        14       2
        16       0
        18       3
        20       3
        22       3
        24       3
        26       4
        28       4
        30       4
        32       5
        34       4
        36       4
        38       4
        40       5
        46       6
Trust DSCP Upstream: Enabled
```

Step 9 Once the configuration is completed, you can activate the manual mapping, and re-enable your networks:

(Cisco Controller) >**config qos qosmap enable**

QoS map is now enabled.

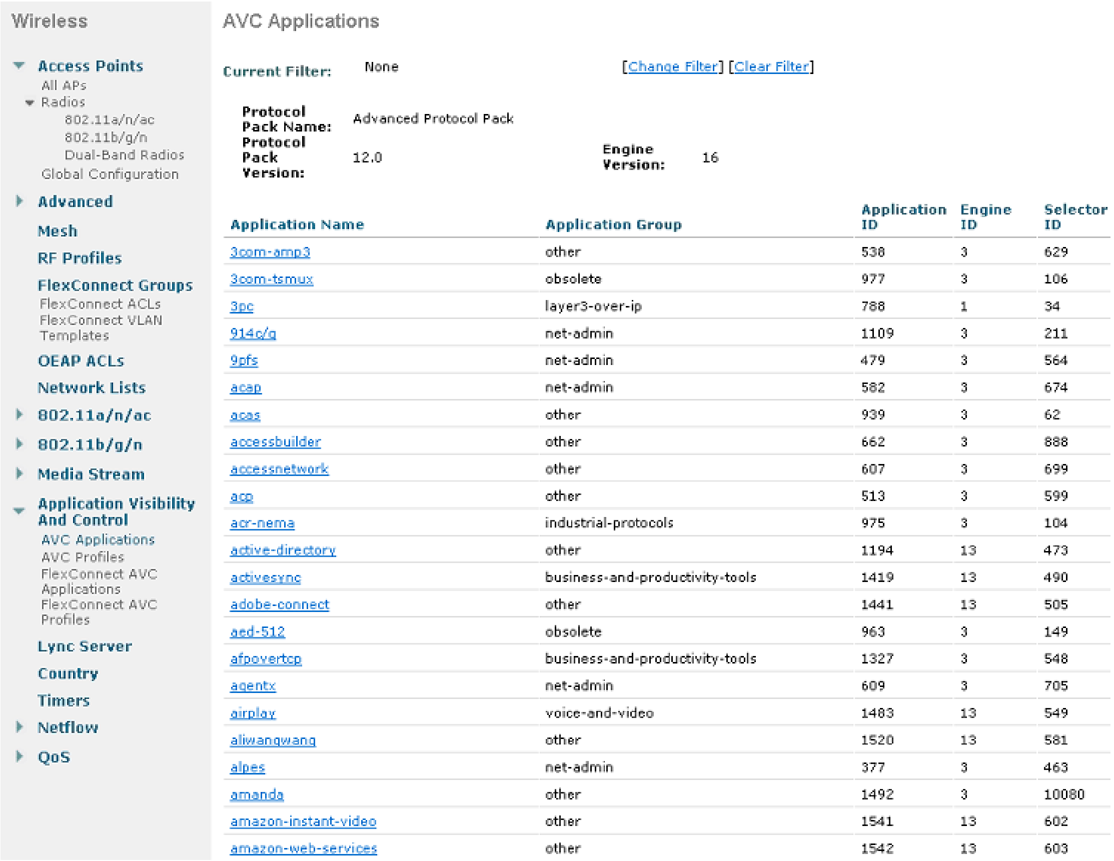
(Cisco Controller) >**config 802.11a enable network**

(Cisco Controller) >**config 802.11b enable network**

Application Visibility and Control

The key use cases for NBAR are capacity planning, network usage base lining, and better understanding of the applications that are consuming bandwidth. Trending of application usage helps network administrator to plan for network infrastructure upgrade, improve quality of experience by protecting key applications from bandwidth-hungry applications when there is congestion on the network, capability to prioritize or de-prioritize, and drop certain application traffic.

NBAR is supported on 2500, 5500 series, 7500, 8500 series and WiSM2 controllers on Local, Mesh, and Flex Connect Mode APs.



AVC Applications

Current Filter: None

Protocol Pack Name: Advanced Protocol Pack

Protocol Pack Version: 12.0

Engine Version: 16

Application Name	Application Group	Application ID	Engine ID	Selector ID
3com-amp3	other	538	3	629
3com-tsmux	obsolete	977	3	106
3pc	layer3-over-ip	788	1	34
914c/g	net-admin	1109	3	211
9pfs	net-admin	479	3	564
acap	net-admin	582	3	674
acas	other	939	3	62
accessbuilder	other	662	3	888
accessnetwork	other	607	3	699
acp	other	513	3	599
acr-nema	industrial-protocols	975	3	104
active-directory	other	1194	13	473
activesync	business-and-productivity-tools	1419	13	490
adobe-connect	other	1441	13	505
aed-512	obsolete	963	3	149
afpovertcp	business-and-productivity-tools	1327	3	548
agentx	net-admin	609	3	705
airplay	voice-and-video	1483	13	549
aliwangwang	other	1520	13	581
alpes	net-admin	377	3	463
amanda	other	1492	3	10080
amazon-instant-video	other	1541	13	602
amazon-web-services	other	1542	13	603

NBAR Supported Feature

NBAR can perform the following tasks:

- Classification—Identification of Application/Protocol.
- AVC—Provides visibility of classified traffic and also gives an option to control the traffic using Drop or Mark (DSCP) action.
- NetFlow—Updating NBAR stats to NetFlow collector such as Cisco Prime Assurance Manager (PAM).
- NBAR/AVC phase 2 on WLC can classify and take action on 1054 different applications.
- Three actions, either DROP, MARK, or Rate Limit is possible on any classified application.
- A maximum of 16 AVC profiles can be created on the WLC.
- Each AVC profile can be configured with a maximum of 32 rules.
- The AVC profile can be mapped to multiple WLANs. But one WLAN can have only one AVC profile.
- Only one NetFlow exporter and monitor can be configured on the WLC.
- NBAR statistics are displayed only for the top 30 applications on the GUI. The CLI can be used to see all applications.

- NBAR is supported on WLANs configured for central switching only.
- If the AVC profile mapped to the WLAN has a rule for MARK action, that application will get precedence as per QOS profile configured in the AVC rule overriding the QOS profile configured on the WLAN.
- Directional Marking can only be applied either Bidirectional, Upstream or Downstream on a particular application.
- Currently, Rate Limit can only be applied to three applications.
- Any application that is not supported/recognized by the NBAR engine on the WLC is captured under bucket of UNCLASSFIED traffic.
- IPv6 traffic cannot be classified.
- AAA override of AVC profiles is supported in 8.0 release.
- The AVC profile can be configured per WLAN and applied per user basis.
- NBAR is not supported in vWLC and SRE WLC.

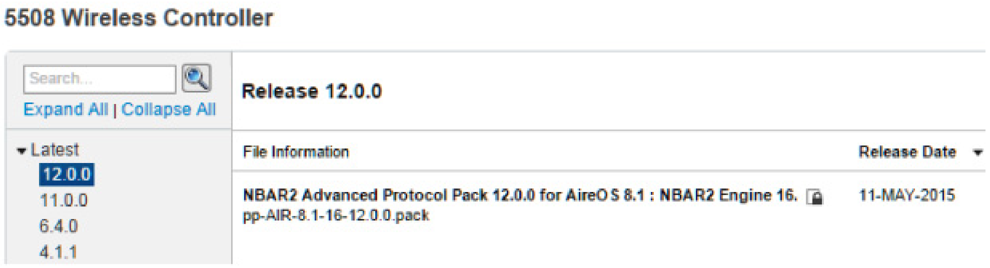
To dynamically update supported applications, an AVC support for protocol packs is added. Protocol packs are software packages that allow update of signature support without replacing the image on the controller. You have an option to load protocol packs dynamically when new protocol support is added. There are two kinds of protocol packs: Major and Minor:

- Major protocol packs include support for new protocols, updates, and bug fixes.
- Minor protocol packs do not include support for new protocols.
- Protocol packs are targeted to specific platform types, software versions, and releases separately. Protocol packs can be downloaded from CCO using the software type “NBAR2 Protocol Pack”.

Protocol packs are released with specific NBAR engine versions. For example, WLC 8.1 has NBAR engine 16, so protocol packs for it are written for engine 16 (pp-AIR-8.1-16-12.pack). Loading a protocol pack can be done if the engine version on the platform is same or higher than the version required by the protocol pack (16 in the example above).

Complete list of protocols supported in the release is posted at the following link:

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html



NBAR2 Advanced Protocol Pack 12.0.0 for AireOS 8.1 : NBAR2 Engine 16.
pp-AIR-8.1-16-12.0.0.pack
11-MAY-2015

Use **show** command to view the currently loaded protocol pack:

(Cisco Controller) >**show avc protocol-pack version**

```
AVC Protocol Pack Name: Advanced Protocol Pack AVC Protocol Pack Version: 12.0
```

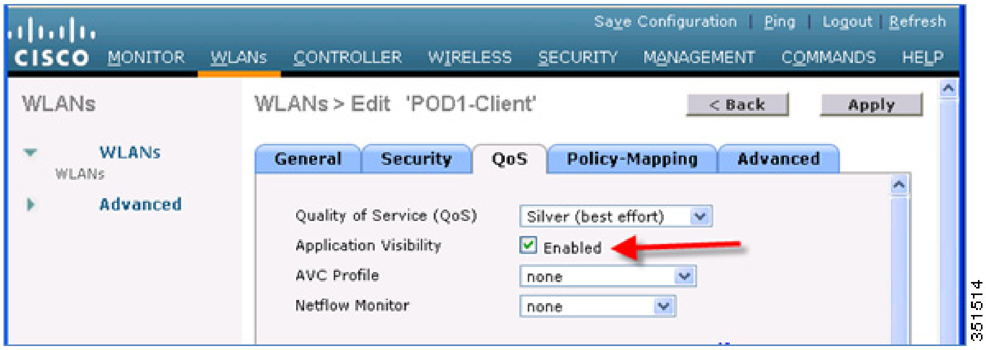
Use **show** command to view the current Nbar2 engine version

(Cisco Controller) >**show avc engine version**

```
AVC Engine Version: 16
```

AVC Configuration Options

When Application Visibility is enabled on the specific WLAN and the associated wireless client starts different types of applications such as Cisco Jabber/WebEx Connect, Skype, Yahoo Messenger, HTTP, HTTPS/SSL, Microsoft Messenger, YouTube, Ping, Trace route, and so on, visibility of different traffic from those applications can be observed globally for all WLANs, per client basis, and per WLAN basis. This provides a good overview to the administrator of the network bandwidth utilization and type of traffic in the network per client, per WLAN, and globally.

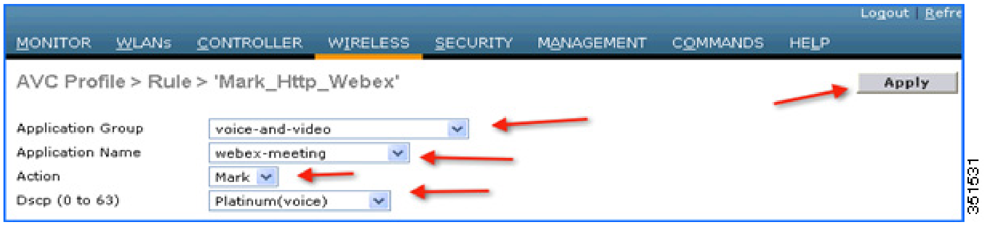


WLANs > Edit 'POD1-Client'

Quality of Service (QoS) Silver (best effort)
Application Visibility ☑ Enabled
AVC Profile none
Netflow Monitor none

AVC discovered applications can be dropped or marked with DSCP Platinum, Gold, Silver, and Bronze values.

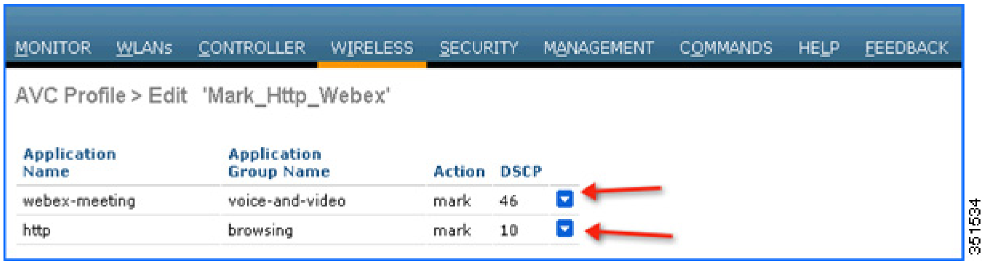
The administrator has flexibility while configuring Action as MARK to choose the Differentiated Services Code Point (DSCP) value as Custom instead of selecting “Platinum/Gold/Silver/Bronze”. Once Custom is selected as DSCP value, a text file is visible where administrator can enter a custom DSCP value in range of 0 – 63.



AVC Profile > Rule > 'Mark_Http_Webex'

Application Group voice-and-video
Application Name webex-meeting
Action Mark
Dscp (0 to 63) Platinum(voice)

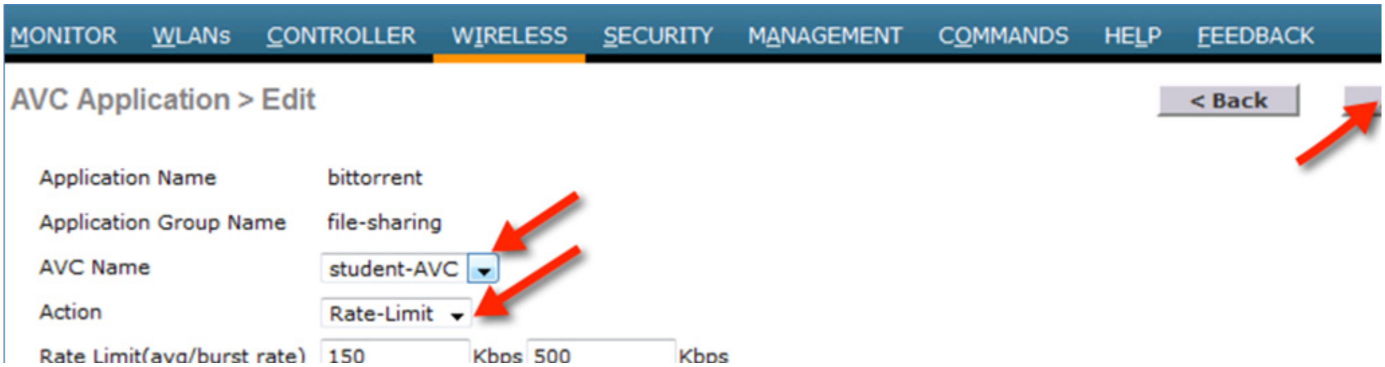
As shown in the following screen shot, two rules are created for AVC profile. The administrator can configure up to 32 rules in the same AVC profile. Individual rules can be configured for action MARK or DROP in the same profile. A single rule can only be configured with a single action, that is, either MARK or DROP.



AVC Profile > Edit 'Mark_Http_Webex'

Application Name	Application Group Name	Action	DSCP
webex-meeting	voice-and-video	mark	46
http	browsing	mark	10

Prior to release 8.0, the DSCP marking is only applied bi-directionally for traffic. But, in release 8.0 and above, an extra configuration parameter named **Direction** is available, where marking can be specified with respect to direction, that is, Upstream or Downstream as shown in the following screen shot.



AVC Application > Edit

Application Name	bittorrent
Application Group Name	file-sharing
AVC Name	student-AVC
Action	Rate-Limit
Rate Limit(avg/burst rate)	150 Kbps 500 Kbps

AVC and QoS Interaction on the WLAN

The AVC/NBAR2 engine on the controller interoperates with the QoS settings on the specific WLAN. The NBAR2 functionality is based on the DSCP setting. The following occurs to the packets in Upstream and Downstream directions if AVC and QoS are configured on the same WLAN:

Upstream

1. Packet comes with or without inner DSCP from wireless side (wireless client).
2. AP adds DSCP in the CAPWAP header that is configured on WLAN (QoS based configuration).
3. WLC removes CAPWAP header.
4. AVC module on the controller overwrites the DSCP to the configured marked value in the AVC profile and sends it out.

Downstream

1. Packet comes from switch with or without inner DSCP wired side value.
2. AVC module overwrites the inner DSCP value.
3. Controller compares WLAN QoS configuration (as per 802.1p value, that is, 802.11e) with inner DSCP value that NBAR had overwritten. WLC will choose the lesser value and put it into CAPWAP header for DSCP.
4. WLC sends out the packet to AP with QoS WLAN setting on the outer CAPWAP and AVC inner DSCP setting.
5. AP strips the CAPWAP header and sends the packet on air with AVC DSCP setting. If AVC is not applied to an application, then that application adopts the QoS setting of the WLAN.

AVC Operation with Anchor/Foreign Controller Setup

In the case of Anchor and Foreign controller configuration, the AVC has to be configured where the application control is required. In most cases in Anchor/Foreign setups, the AVC should be enabled on the Anchor controller. AVC profile enforcement happens on the WLAN on the Anchor controller. If Anchor controller is release 7.4 or higher, the above mentioned setup will work.

Application Rate Limiting Through AVC

In release 8.0 and above, three applications can be configured for rate limiting which can be done from the WLC CLI through the following command:

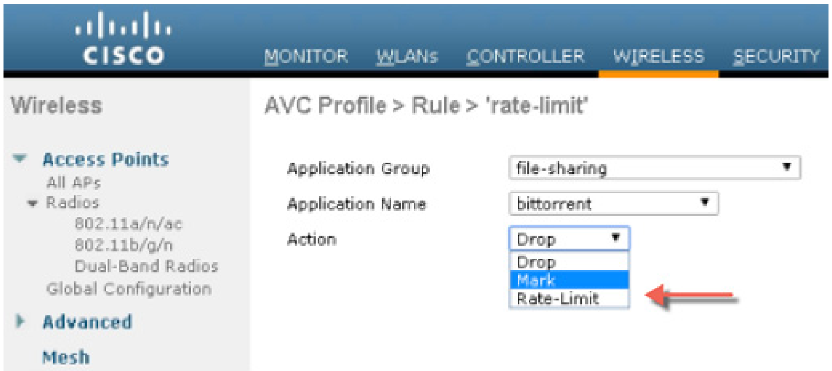
(WLC) >**config avc profile <prof-name> {add|remove} rule application <app-name> {drop|mark<dscp-value>|ratelimit <avg_rate> <burst_rate>}**

Note The minimum rate limit value can be set from minimum 0 Kbps to maximum 2147483647 Kbps.

The following configuration example is performed on the profile "student-AVC" when using the BitTorrent application:

(WLC) >**config avc profile student-AVC rule add application bittorrent ratelimit 150 500**

Similarly, from the WLC GUI, the rate limiting can be configured by selecting the application on which the user wants to apply rate limit. From the **Action** drop-down list, choose **Rate-Limit**.

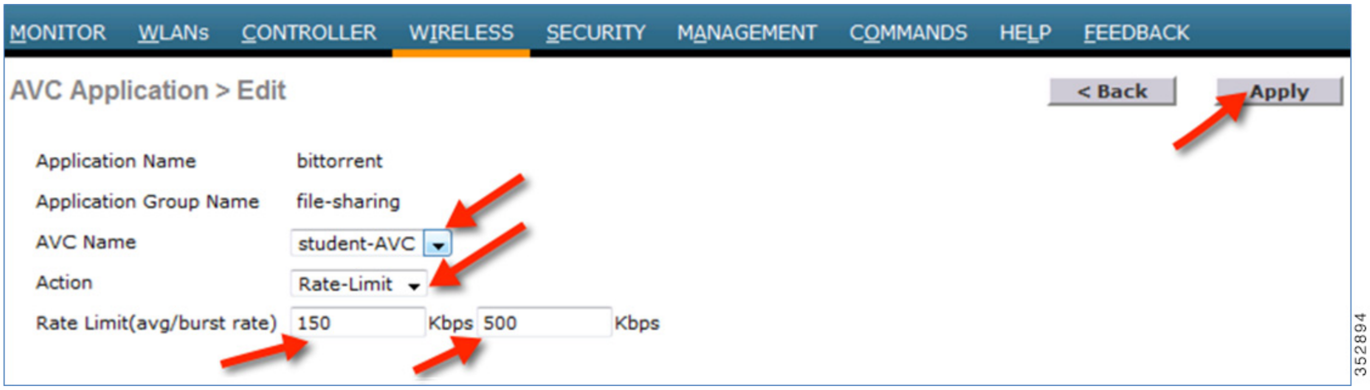


AVC Profile > Rule > 'rate-limit'

Application Group file-sharing
Application Name bittorrent
Action Drop

Now, you have an option to configure the average and burst rates for the desired application that you need to rate limit. You can assign any value in Kbps from 0 to 2147483647. Once the rate limit is set, you can choose the **AVC Name** on which you want to apply the rate limit and click **Apply**.

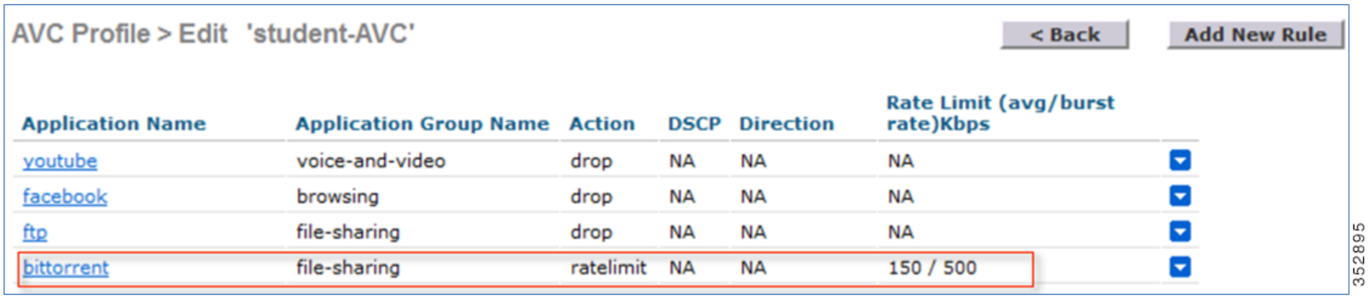
In this example, the BitTorrent application is rate limited with the average rate set to 150 Kbps and burst rate set to 500 Kbps and applying this to the AVC profile **student-AVC**.



AVC Application > Edit

Application Name bittorrent
Application Group Name file-sharing
AVC Name student-AVC
Action Rate-Limit
Rate Limit(avg/burst rate) 150 Kbps 500 Kbps

The BitTorrent application displays **rate limit** in the **Action** column with rate limit average and burst rate values.



AVC Profile > Edit 'student-AVC'

Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps
youtube	voice-and-video	drop	NA	NA	NA
facebook	browsing	drop	NA	NA	NA
ftp	file-sharing	drop	NA	NA	NA
bittorrent	file-sharing	ratelimit	NA	NA	150 / 500

AVC Profiles Attached to Local Policies

In Release 8.0, an AVC profile can be mapped to a local policy for a client with a particular device type. Local policies can be configured with a different AVC/mDNS profile name based on the AAA override to restrict the policy from being able to use the services not allowed by the profile on the same WLAN.

Introduction to Profiling and Policy Engine on the WLC

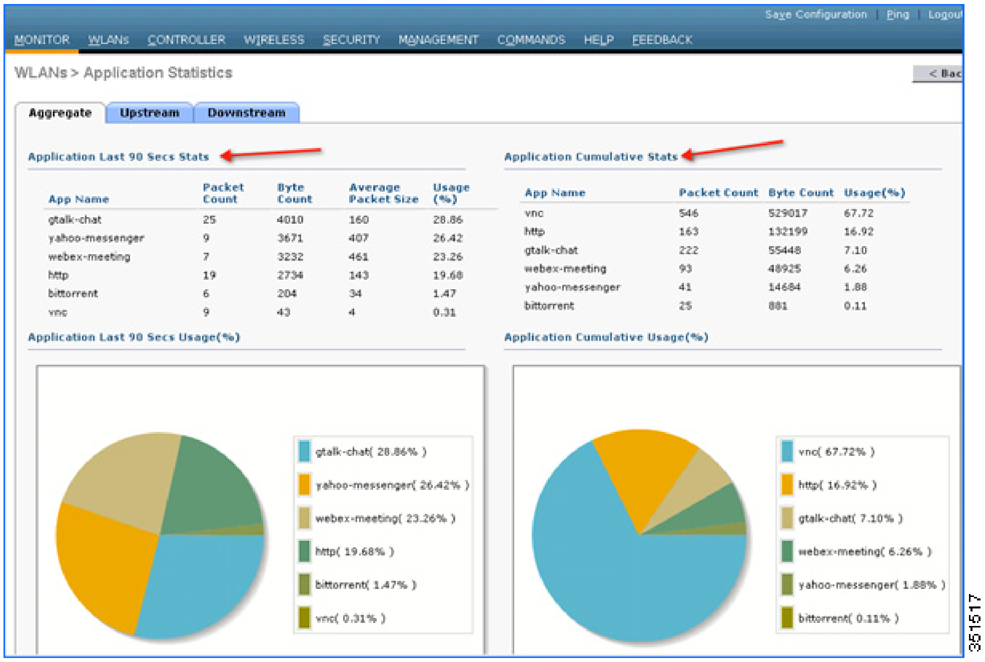
Cisco currently offers a rich set of features which provide device identification, onboarding, posture, and policy, through ISE. This new feature on the WLC does the profiling of devices based on protocols such as HTTP, DHCP, and so on to identify the end devices on the network. The user can configure the device-based policies and enforce per user or per device policy on the network. The WLC also displays statistics based on per user or per device end points and policies applicable per device.

With BYOD (Bring your own device), this feature has an impact on understanding the different devices on the network. With this, BYOD can be implemented on a small scale within the WLC itself.

AVC Monitoring

As previously mentioned, visibility of traffic can be monitored:

- Globally for all WLANs
- Individual WLAN
- Individual client



WLANs > Application Statistics

Application Last 90 Secs Stats

App Name	Packet Count	Byte Count	Average Packet Size	Usage (%)
gtalk-chat	25	4010	160	28.86
yahoo-messenger	9	3671	407	26.42
webex-meeting	7	3232	461	23.26
http	19	2734	143	19.68
bittorrent	6	204	34	1.47
vnc	9	43	4	0.31

Application Cumulative Stats

App Name	Packet Count	Byte Count	Usage(%)
vnc	546	529017	67.72
http	163	132199	16.92
gtalk-chat	222	55448	7.10
webex-meeting	93	48925	6.26
yahoo-messenger	41	14684	1.88
bittorrent	25	881	0.11

Application Last 90 Secs Usage(%)

Application Cumulative Usage(%)

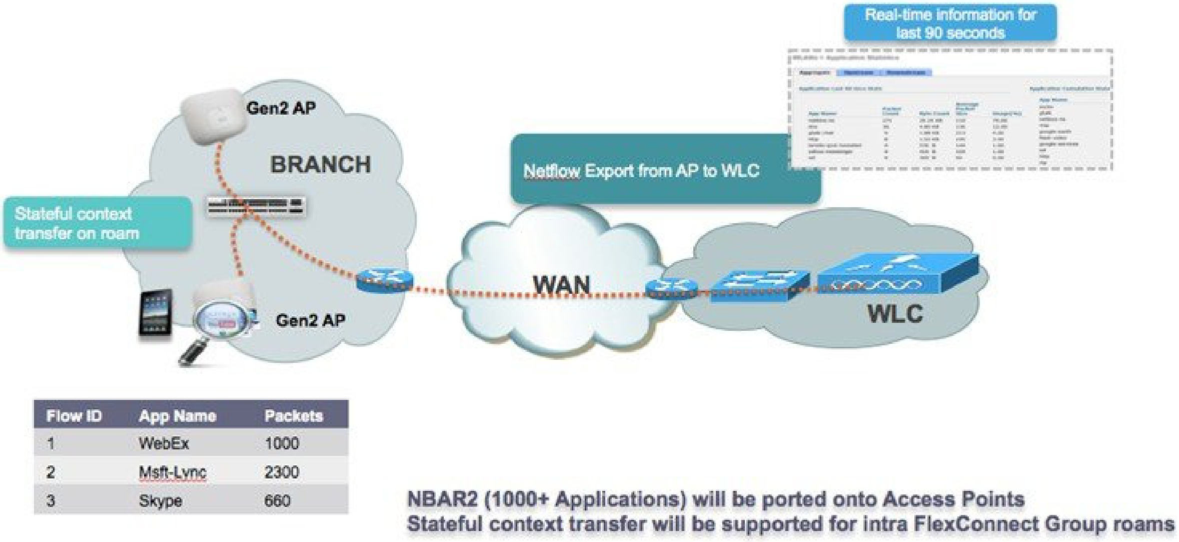
Application Visibility and Control for FlexConnect

The key use cases for NBAR AVC are capacity planning, network usage base lining, and better understanding of the applications that are consuming bandwidth. Trending of application usage helps the network administrator to plan for network infrastructure upgrade, improve quality of experience by protecting key applications from bandwidth-hungry applications when there is congestion on the network, capability to prioritize or de-prioritize, and drop certain application traffic.

AVC is supported on the 5520, 8540, 2500, 5508, 7500, 8500, and WiSM2 controllers on Local and FlexConnect modes (for WLANs configured for central switching only) since release 7.4. Release 8.1 introduces support for Application Visibility and Control (AVC) for locally switched WLANs on FlexConnect APs. For more information on Flex AVC, see Chapter 7, "FlexConnect".

How AVC Works on FlexConnect AP

- NBAR2 engine runs on the FlexConnect AP.
- Classification of applications happens at the access point using the DPI engine (NBAR2) to identify applications using L7 signatures.
- AP collects application information and exports it to controller every 90 seconds.
- Real-time applications are monitored on the controller user interface.
- Ability to take actions, drop, mark or rate-limit, is possible on any classified application on the FlexConnect access point.


Real-time information for last 90 seconds
Gen2 AP
BRANCH
Netflow Export from AP to WLC
Stateful context transfer on roam
WAN
WLC
Gen2 AP

Flow ID	App Name	Packets
1	WebEx	1000
2	Msft-Lync	2300
3	Skype	660

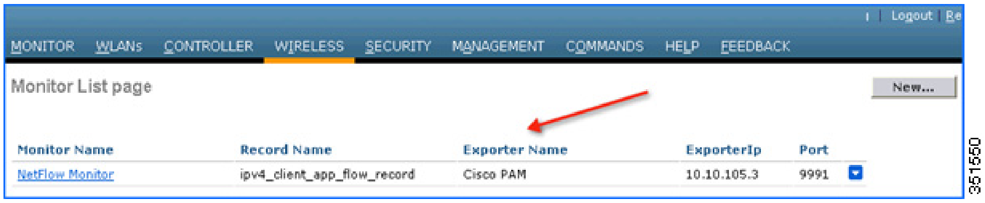
NBAR2 (1000+ Applications) will be ported onto Access Points
Stateful context transfer will be supported for intra FlexConnect Group roams

AVC FlexConnect Facts and Limitations

- AVC on the FlexConnect AP can classify and take action on 1000+ different applications.
- The protocol pack running on the FlexConnect APs is different from the one running on the WLC.
- AVC stats on the GUI are displayed for the top 10 applications by default. This can be changed to top 20 or 30 applications as well.
- Intra FlexConnect Group roaming support.
- IPv6 traffic cannot be classified.
- AAA override of AVC profiles is not supported.
- Multicast traffic is not supported by AVC application.
- Netflow export for FlexConnect AVC is not supported in 8.1.

NBAR NetFlow Monitor

A NetFlow monitor can also be configured on the WLC to collect all the stats generated on a WLC and these stats can be exported to the NetFlow collector. In the following example, Cisco Performance Application Manager (PAM) is used as a NetFlow collector. PAM is a licensed application running on Cisco Prime Infrastructure.



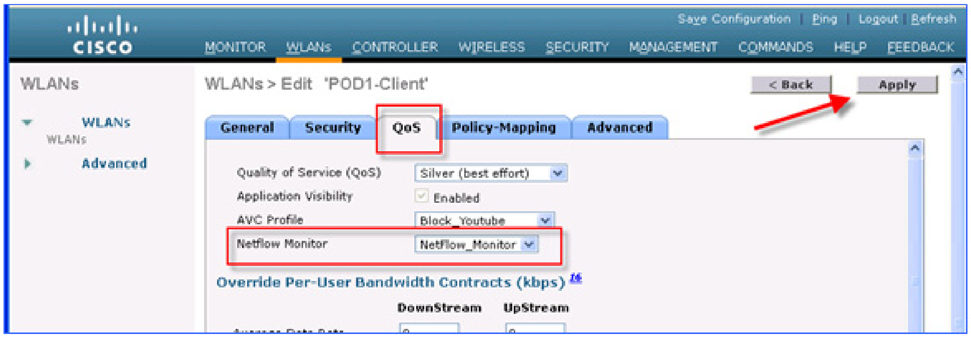
Monitor List page

Monitor Name	Record Name	Exporter Name	ExporterIp	Port
NetFlow Monitor	ipv4_client_app_flow_record	Cisco PAM	10.10.105.3	9991

Once the monitor entry is created and the exporter entry is mapped to the same, it should be mapped to the WLAN.

To map the exporter entry to WLAN:

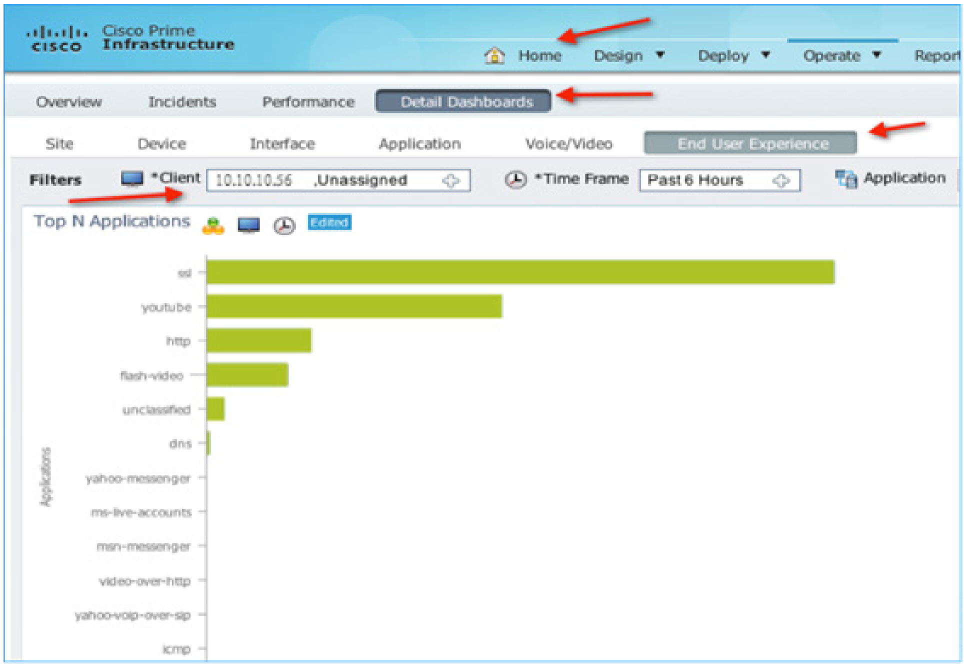
1. Click **WLANs**
2. Click the specific **WLAN ID**.
3. Click the **QoS** tab
4. Choose the created monitor entry from the **NetFlow Monitor** drop-down list.
5. Click **Apply**.


Save Configuration | Ping | Logout | Refresh
cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General Security QoS Policy-Mapping Advanced
Override Per-User Bandwidth Contracts (kbps)
DownStream UpStream
351551

WLANs > Edit 'POD1-Client'

Quality of Service (QoS) Silver (best effort)
Application Visibility ☑ Enabled
AVC Profile Block_Youtube
Netflow Monitor NetFlow_Monitor

Cisco Prime has to be preconfigured with PAM. After PAM is configured with WLAN and wireless client has traffic going with specific preconfigured applications, administrator should see application usage per WLAN. Navigate to **Home > Detail Dashboards > End User Experience.** In the **Filters** area, select **Network Aware** as WLAN, that is, **10.10.10.56** client in the following example, and then click **GO**.


cisco Cisco Prime Infrastructure
Home Design Deploy Operate Report
Overview Incidents Performance Detail Dashboards
Site Device Interface Application Voice/Video End User Experience
Application
Top N Applications
Edited
ssl
youtube
http
flash-video
unclassified
dns
yahoo-messenger
ms-live-accounts
msn-messenger
video-over-http
yahoo-voip-over-sip
icmp
Applications
351557

Filters *Client 10.10.10.56 ,Unassigned *Time Frame Past 6 Hours

CHAPTER 6

Cisco Unified Wireless Multicast Design

Introduction

This chapter describes the Cisco Unified Wireless Multicast in IP multicast forwarding and provides information on how to deploy multicast in a wireless environment. A prerequisite for using the multicast performance functionality is that a multicast-enabled network must be configured on all routers between the controllers and the Access Points (APs). To accommodate networks that do not support multicast, the controller continues to support the original unicast packet forwarding mechanism.

IP multicast is a delivery protocol for information to a group of destinations. It uses the most efficient strategy to deliver the information over each link of the network. It sends only one copy of the information at each hop of the network, creating copies only when the links to the destinations split. Typically, many of today's networks applications use unicast packets i.e., from one source to one destination. However, when multiple receivers require the same data, replicating the data from the source to all the receivers as individual unicast packets increases the network load. IP multicast enables efficient transfer of data from a set of sources to a dynamically formed set of receivers.

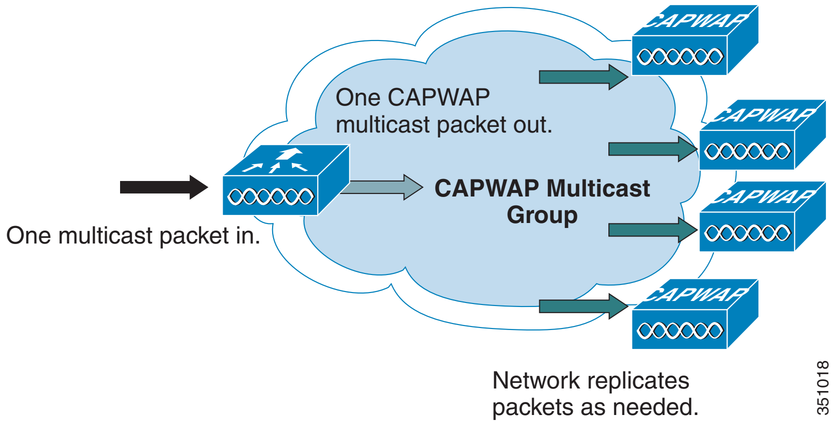
IP multicast is typically used today for one way streaming media, such as video to large groups of receivers. Many cable TV operators, educational institutions and large enterprises have deployed IP multicast for their content delivery needs. Additionally, there have been some uses of audio and video conferencing using multicast. Another widespread use of multicast within campus and commercial networks is for file distribution, particularly to deliver operating system images and updates to remote hosts. IP multicast has also seen deployment within the financial sector for applications such as stock tickers and hoot-n-holler systems.

Overview of IPv4 Multicast Forwarding

With Cisco Unified Wireless Network Software Releases, significant enhancements were made to support the effective use of multicast in a wireless network.

With the current Cisco Unified Wireless multicast support, each multicast frame received by the controller from a VLAN on the first hop router is copied and sent to the multicast group configured on the controller for the AP that is associated, as shown in Figure 6-1. The multicast CAPWAP packet containing the multicast packet uses a WLAN bitmap, which tells the receiving AP which WLAN it must forward the packet to. When the AP receives the CAPWAP packet, it strips off the outer CAPWAP encapsulation and transmits the multicast packet to the WLAN (on all radios associated to the WLAN) identified in the CAPWAP WLAN ID bitmask.

Figure 6-1 Multicast Forwarding Mechanism


One CAPWAP multicast packet out.
CAPWAP Multicast Group
One multicast packet in.
CAPWAP
Network replicates packets as needed.
351018

Effectively, enabling Global Multicast mode delivers the multicast packet to each access point. This allows the routers in the network to use standard multicast techniques to replicate and deliver multicast packets to the APs. For the CAPWAP multicast group, the controller becomes the multicast source and the APs become the multicast receivers.

Note A prerequisite for using the multicast performance functionality is that a multicast enabled network is configured on all routers between the controllers and the APs. To accommodate networks that do not support multicast, the controller continues to support the original unicast packet forwarding mechanism.

Note With multicast enabled, any kind of multicast packet received on the VLAN from the first hop router is transmitted over the wireless including HSRP hellos, all router, routing protocol, and PIM multicast packets.

After the administrator enables multicast (multicast mode is disabled by default), configures a CAPWAP multicast group, and enables IGMP snooping, the access point downloads the controller's CAPWAP multicast group address during the normal join process (at boot time) to the controller. After an access point joins a controller and downloads its configuration, the AP issues an Internet Group Management Protocol (IGMP) join request to join the controller's CAPWAP multicast group. This triggers the normal setup for the multicast state in the multicast-enabled routers between the controller and APs. The source IP address for the multicast group is the controller's management interface IP address, not the AP-manager IP address used for Layer 3 mode. Once the AP has joined the controllers CAPWAP multicast group, the multicast algorithm for client multicast traffic works as described below.

When the source of the multicast group is on the wired LAN:

- When the controller receives a multicast packet from any of the client VLANs on the first hop router, it transmits the packet to the CAPWAP multicast group via the management interface at the best effort QoS classification. The QoS bits for the CAPWAP multicast packet are hard coded at the lowest level and are not user changeable.
- The multicast-enabled network delivers the CAPWAP multicast packet to each of the access points that have joined the CAPWAP multicast group, using the normal multicast mechanisms in the routers to replicate the packet along the way as needed so that the multicast packet reaches all APs (Figure 6-1). This relieves the controller from replicating the multicast packets.

- Access points may receive other multicast packets but will only process the multicast packets that are sourced from the controller they are currently joined to; any other copies are discarded. If more than one WLAN is associated to the VLAN interface where the original multicast packet was sourced, the AP transmits the multicast packet over each WLAN (following the WLAN bitmap in the CAPWAP header). Additionally, if that WLAN is on both radios (802.11g and 802.11a), both radios transmit the multicast packet on the WLAN if there are clients associated, even if those clients did not request the multicast traffic.

When the source of the multicast group is a wireless client:

- The multicast packet is unicast (CAPWAP encapsulated) from the AP to the controller similar to standard wireless client traffic.
- The controller makes two copies of the multicast packet. One copy is sent out the VLAN associated with the WLAN it came on, enabling receivers on the wired LAN to receive the multicast stream and the router to learn about the new multicast group. The second copy of the packet is CAPWAP-encapsulated and is sent to the CAPWAP multicast group so that wireless clients may receive the multicast stream.

Wireless Multicast Roaming

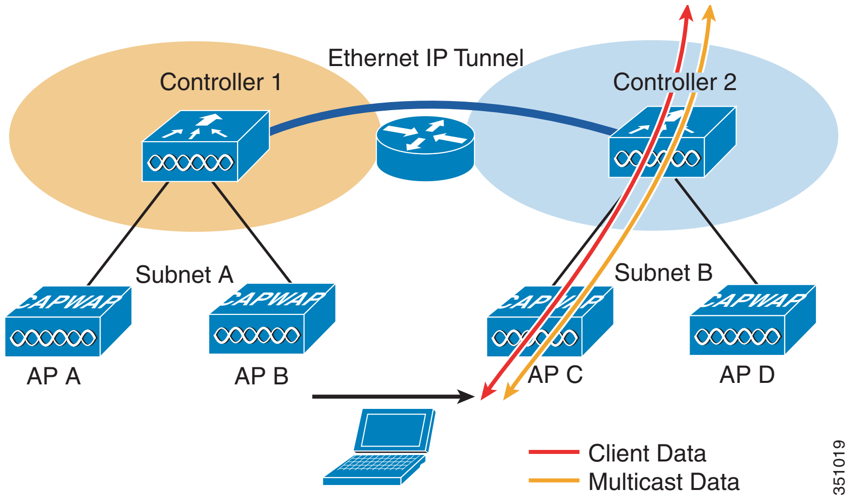
A major challenge for a multicast client in a wireless environment is maintaining its multicast group membership when moving about the WLAN. Drops in the wireless connection moving from AP-to-AP can cause a disruption in a client’s multicast application. Internet Group Management Protocol (IGMP) plays an important role in the maintenance of dynamic group membership information.

A basic comprehension of IGMP is important for understanding what happens to a client’s multicast session when it roams about the network. In a Layer 2 roaming case, sessions are maintained simply because the foreign AP, if configured properly, already belongs to the multicast group and traffic is not tunneled to a different anchor point on the network. Layer 3 roaming environments are a little more complex in this manner and depending on what tunneling mode you have configured on your controllers, the IGMP messages sent from a wireless client will be affected. The default mobility tunneling mode on a controller is asymmetrical. As discussed in the Chapter 2, “Cisco Unified Wireless Technology and Architecture,” this means that return traffic to the client is sent to the anchor WLC then forwarded to the foreign WLC where the associated client connection resides. Outbound packets are forwarded out the foreign WLC interface. In symmetrical mobility tunneling mode, both inbound and outbound traffic are tunneled to the anchor controller. For more information on mobility tunneling, see Chapter 2, “Cisco Unified Wireless Technology and Architecture.”

Asymmetric Multicast Tunneling

In asymmetric multicast tunneling, when a client roams to a new AP associated to a different WLC and on a different subnet, it is queried for its multicast group memberships by the foreign WLC and send out an IGMP group membership report. This is forwarded out the foreign WLC dynamic interface assigned to the VLAN and the client rejoins the multicast stream through the foreign subnet. Figure 6-2 illustrates the traffic flow for normal data and multicast data.

Figure 6-2 Asymmetric Tunneling



Note In the event of a client roam, there is a slight disruption in the multicast session; in some applications it might be considered unsuitable for use.

Multicast Enabled Networks

A prerequisite for using this new multicast performance functionality is that a multicast enabled network is configured on all routers between the controllers and the APs. A multicast-enabled network allows for an efficient way to deliver a packet to many hosts across the network. IP multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients. Packets are replicated as necessary at each Layer 3 point in the network. A multicast routing protocol, such as PIM, is required if there is more than one router between the controllers and APs. For more information on setting up a multicast-enabled network, refer to the following URL: http://www.cisco.com/go/multicast.

CAPWAP Multicast Reserved Ports and Addresses

The controller blocks all multicast packets sent to any multicast group that have a destination port of 5246, 5247, and 5248. Additionally, all packets with a multicast group address equal to the controller's CAPWAP multicast group address are blocked at the controller. This is to prevent fragmented CAPWAP encapsulated packets from another controller being retransmitted (see the Fragmentation and CAPWAP Multicast Packets section for more information). Ensure that the multicast applications on your network do not use these reserved ports or CAPWAP multicast group addresses.

Enabling IPv4 Multicast Forwarding on the Controller

IP Multicast traffic through the controller is disabled by default. WLAN clients cannot receive multicast traffic when it is disabled. If you wish to turn on multicast traffic to the WLAN clients, follow these steps:

Enabling IPv4 Multicast Mode (GUI)

Step 1 Choose **Controller > Multicast** to open the Multicast page.

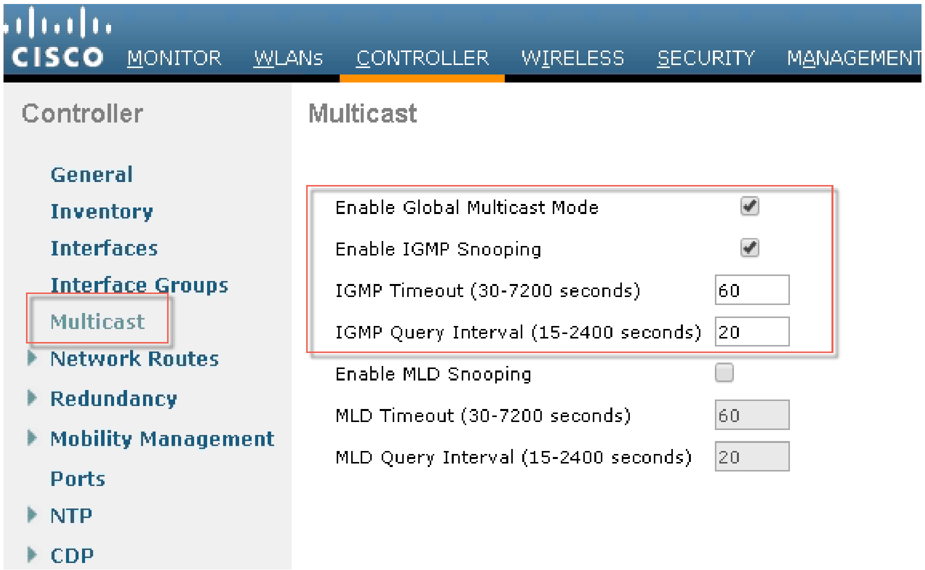
Step 2 Check the **Enable Global Multicast Mode** check box to configure sending multicast packets. The default value is disabled.

Note FlexConnect supports unicast mode only.

Step 3 If you want to enable IGMP snooping, check the **Enable IGMP Snooping** check box. If you want to disable IGMP snooping, leave the check box unchecked. The default value is disabled.

Step 4 To set the IGMP timeout, enter a value between 30 and 7200 seconds in the **IGMP Timeout** text box. The controller sends three queries in one timeout value at an interval of *timeout/ 3* to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (that is, to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

Step 5 Enter the IGMP Query Interval (seconds).



Multicast

Enable Global Multicast Mode ☑
Enable IGMP Snooping ☑
IGMP Timeout (30-7200 seconds) 60
IGMP Query Interval (15-2400 seconds) 20
Enable MLD Snooping ☐
MLD Timeout (30-7200 seconds) 60
MLD Query Interval (15-2400 seconds) 20

When IGMP snooping is disabled, the following is true:

- The controller always uses Layer 2 MGID when it sends multicast data to the access point. Every interface created is assigned with one Layer 2 MGID. For example, the management interface has an MGID of 0, and the first dynamic interface created is assigned an MGID of 8, which increments as each dynamic interface is created.
- The IGMP packets from clients are forwarded to the router. As a result, the router IGMP table is updated with the IP address of the clients as the last reporter.

When IGMP snooping is enabled, the following is true:

- The controller always uses Layer 3 MGID for all Layer 3 multicast traffic sent to the access point. For all Layer 2 multicast traffic, it continues to use Layer 2 MGID.
- IGMP report packets from wireless clients are consumed or absorbed by the controller, which generates a query for the clients. After the router sends the IGMP query, the controller sends the IGMP reports with its interface IP address as the listener IP address for the multicast group. As a result, the router IGMP table is updated with the controller IP address as the multicast listener.
- When the client that is listening to the multicast groups roams from one controller to another, the first controller transmits all the multicast group information for the listening client to the second controller. As a result, the second controller can immediately create the multicast group information for the client. The second controller sends the IGMP reports to the network for all multicast groups to which the client was listening. This process aids in the seamless transfer of multicast data to the client.
- If the listening client roams to a controller in a different subnet, the multicast packets are tunneled to the anchor controller of the client to avoid the reverse path filtering (RPF) check. The anchor then forwards the multicast packets to the infrastructure switch. The MGIDs are controller specific. The same multicast group packets coming from the same VLAN in two different controllers may be mapped to two different MGIDs.

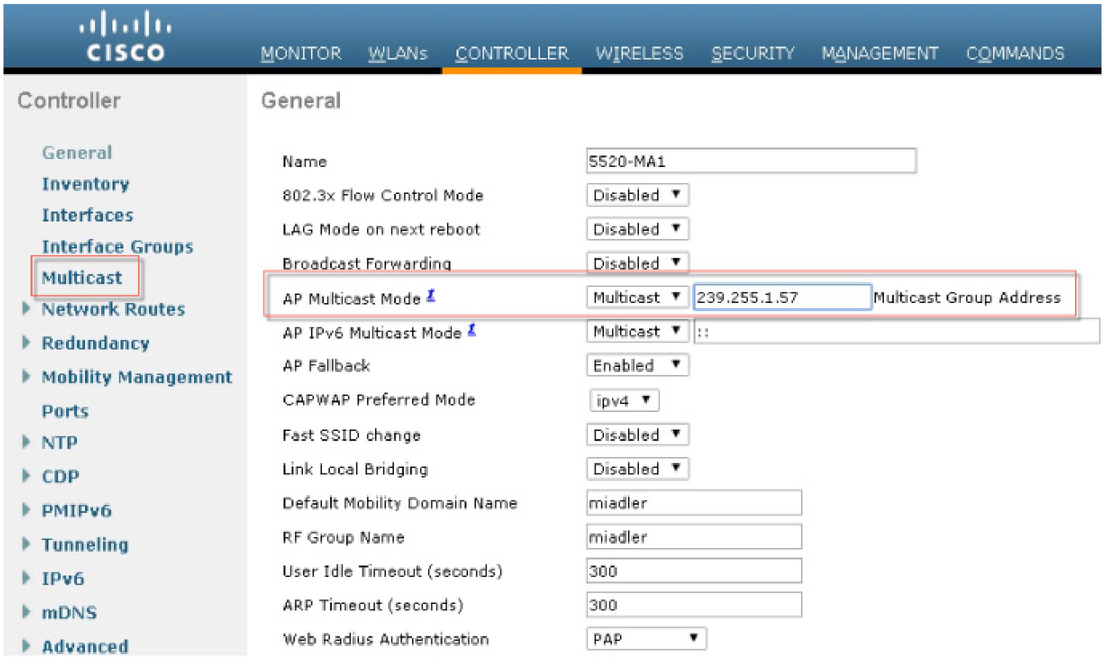
Note The number of multicast addresses supported per VLAN for a Cisco WLC is 100.

Step 6 If you have a multicast enabled network, choose **Multicast** from the **AP Multicast Mode** drop-down list to use the method where the network replicates the packets.

Step 7 If you do not have a multicast enabled network, choose **Unicast** from the **AP Multicast Mode** drop-down list to use the method where the controller replicates the packets.

Step 8 Choose **Multicast** from the **AP Multicast Mode** drop-down list and enter a multicast group address. This option is shown in Figure 6-3.

Figure 6-3 Commands to turn on Ethernet Multicast Mode via the GUI.



General

Name	5520-MA1
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Disabled
Broadcast Forwarding	Disabled
AP Multicast Mode	Multicast 239.255.1.57 Multicast Group Address
AP IPv6 Multicast Mode	Multicast ::
AP Fallback	Enabled
CAPWAP Preferred Mode	ipv4
Fast SSID change	Disabled
Link Local Bridging	Disabled
Default Mobility Domain Name	miadler
RF Group Name	miadler
User Idle Timeout (seconds)	300
ARP Timeout (seconds)	300
Web Radius Authentication	PAP

Information About Multicast Mode

If your network supports packet multicasting, you can configure the multicast method that the controller uses.

The controller performs multicasting in two modes:

Unicast mode—In this mode, the controller unicasts every multicast packet to every access point associated to the controller. This mode is inefficient but might be required on networks that do not support multicasting.

Multicast mode—In this mode, the controller sends multicast packets to a CAPWAP multicast group. This method reduces overhead on the controller processor and shifts the work of packet replication to your network, which is much more efficient than the unicast method.

When you enable multicast mode and the controller receives a multicast packet from the wired LAN, the controller encapsulates the packet using CAPWAP and forwards the packet to the CAPWAP multicast group address. The controller always uses the management interface for sending multicast packets. Access points in the multicast group receive the packet and forward it to all the BSSIDs mapped to the interface on which clients receive multicast traffic. From the access point perspective, the multicast appears to be a broadcast to all SSIDs.

Multicast Deployment Considerations

Recommendations for Choosing a CAPWAP Multicast Address

Caution Although not recommended, any multicast address can be assigned to the CAPWAP multicast group including the reserved link local multicast addresses used by OSPF, EIGRP, PIM, HSRP, and other multicast protocols.

Cisco recommends that multicast addresses be assigned from the administratively scoped block 239/8. IANA has reserved the range of 239.0.0.0-239.255.255.255 as administratively scoped addresses for use in private multicast domains (see the note below for additional restrictions). These addresses are similar in nature to the reserved private IP unicast ranges (such as 10.0.0.0/8) defined in RFC 1918. Network administrators are free to use the multicast addresses in this range inside of their domain without fear of conflicting with others elsewhere in the Internet. This administrative or private address space should be used within the enterprise and blocked from leaving or entering the autonomous domain (AS).

Note Do not use the 239.0.0.*X* address range or the 239.128.0.*X* address range. Addresses in these ranges overlap with the link local MAC addresses and will flood out all switch ports even with IGMP snooping turned on.

Cisco recommends that enterprise network administrators further subdivide this address range into smaller geographical administrative scopes within the enterprise network to limit the "scope" of particular multicast applications. This is used to prevent high-rate multicast traffic from leaving a campus (where bandwidth is plentiful) and congesting the WAN links. It also allows for efficient filtering of the high bandwidth multicast from reaching the controller and the wireless network.

For more information on multicast address guidelines, refer to the document at the following URL:

http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a00802d4643.shtml

Fragmentation and CAPWAP Multicast Packets

When a controller receives a multicast packet, it encapsulates the packet inside of CAPWAP using the CAPWAP multicast group as a destination address and forwards it to the APs via the management interface (source address). If the packet exceeds the MTU of the link, the controller fragments the packet and send out both packets to the CAPWAP multicast group. If another controller were to receive this CAPWAP encapsulated multicast packet via the wired network, it would re-encapsulate it again, treating it as a normal multicast packet and forward it to its APs.

There are two different options to prevent this from happening, either of which is effective by itself. One, you may assign all controllers to the same CAPWAP multicast group address. Or two, you can apply standard multicast filtering techniques to ensure that CAPWAP encapsulated multicast packets do not reach any other controller. If all controllers have the same CAPWAP multicast group or different groups, Table 6-1 lists the pros and cons of these two techniques.

Table 6-1 Pros and Cons of using the same Multicast Group or Different Groups

Technique	PRO	CON
All controllers have the same CAPWAP multicast group	No need to do any additional fragmentation protection measures	Each controller's multicast traffic is flooded throughout the network (APs will drop multicast packets that do not have a source IP address equal to their controller management interface)
Standard multicast techniques are used to block CAPWAP multicast fragments	Can use a range of addresses thus preventing flooding throughout the network.	ACL filtering must be applied on first hop router on all VLANs configured on multicast enabled controllers

All Controllers have the Same CAPWAP Multicast Group

To prevent the second controller from retransmitting these CAPWAP encapsulated packets, the controller blocks incoming multicast packets to the CAPWAP multicast group and the CAPWAP reserved ports. By blocking the reserved ports, the controller blocks the first part of a fragmented packet in an encapsulated CAPWAP multicast packet. However, the second packet does not contain port numbers and can only be blocked by filtering it on the multicast group address (destination address). The controller blocks any packets where the destination address is equal to the CAPWAP multicast group address assigned to the controller.

However, assigning every controller to the same CAPWAP multicast group creates other problems. IGMP version 1 and 2 used by the APs to join the CAPWAP multicast group use Any Source Multicast (ASM) and the APs will receive multicast traffic from all sources of the multicast group in the network. This means the APs will receive multicast packets from all of the controllers on the network if the controllers are configured with the same multicast group address, and no multicast boundaries have been applied. One controller's multicast traffic will flood out to all of the APs across the network and every APs receive (and drop it if the source address is not equal to its controller's management address) the multicast traffic that is being received from any wireless multicast client in the entire network. Additionally, locally sourced multicast packets from any client VLAN such as HSRP, PIM, and EIGRP and OSPF multicast packets will also be flooded throughout the network.

Controlling Multicast on the WLAN Using Standard Multicast Techniques

Normal boundary techniques should be used in your multicast enabled network. These include using the **ip multicast boundary** interface mode command, which filters IP multicast traffic and also Auto-RP messages.

Note A wired client anywhere in the network may request the CAPWAP multicast stream and receive it from all sources (if multicast boundaries are not applied). Multicast streams are not encrypted when they are encapsulated in the CAPWAP multicast packet. Therefore, it is recommended that multicast boundaries be implemented to block this type of access.

In the past, Time To Live field in the IP Multicast datagram was used for creating Auto-RP administrative boundaries using the **ttl-threshold** command. This has been superseded by the **ip multicast boundary** interface mode command, which filters IP multicast traffic and also Auto-RP messages. Cisco recommends using the new command.

Other useful commands include the **ip multicast rate-limit interface** command. This command enforces low rates on the wireless VLANs. Without it, even if the network engineer filters the high rate multicast addresses, a low rate multicast address cannot exceed its rate.

A typical example on a wireless client VLAN is given below. For more information on other multicast commands for a multicast enabled network refer to http://www.cisco.com/go/multicast. Filtering for multicast-enabled traffic also allows you to prevent propagation of certain worms like the sasser worm which relied on the TCP and ICMP transports with multicast addresses. Blocking these types of traffic with multicast group addresses does not affect most applications since they typically use UDP or TCP for streaming.

In the following example, packets to the multicast group range 239.0.0.0 to 239.127.255.255 from any source will have their packets rate-limited to 128 kbps. The example also sets up a boundary for all multicast addresses not in the lower administratively scoped addresses. In addition, hosts serviced by Vlan40 can only join the lower administrative groups 239.0.0.0 to 239.127.255.255.

```
mls qos
!
class-map match-all multicast_traffic
description Permit Low Rate Multicast Range of 239.0.0.0 to 239.127.0.0 match access-group
101
!
policy-map multicast
description Rate Limit Multicast traffic to 2.56mps with burst of 12800 bytes class
multicast_traffic
police cir 2560000 bc 12800 be 12800 conform-action transmit exceed-action drop
!
interface Vlan40
description To Wireless Clients
ip address 10.20.40.3 255.255.255.0
ip pim sparse-mode
ip multicast boundary 1 ip igmp access-group 30 standby 40 ip 10.20.40.1
standby 40 preempt
service-policy output multicast
!
access-list 1 remark Permit Low Rate Multicast Range of 239.0.0.0 to 239.127.0.0 for
multicast boundary
access-list 1 permit 239.0.0.0 0.127.255.255
!
access-list 30 remark Only Allow IGMP joins to this Multicast Group Range access-list 30
permit 239.0.0.0 0.127.255.255
!
access-list 101 remark Permit Low Rate Multicast Range of 239.0.0.0 to 239.127.0.0 for
class-map
access-list 101 permit ip any 239.0.0.0 0.127.255.255
```

How Controller Placement Impacts Multicast Traffic and Roaming

Note The multicast stream in either deployment, distributed or collocated, is not rate-limited and there is no way to put ACLs on it. Once enabled, all multicast traffic is forwarded to the wireless LAN including HSRP, EIGRP, OSPF, and PIM packets.

We look at two different deployments (distributed and centralized) and how they impact roaming with multicast clients. In a centralized deployment, WLC WLAN interfaces are attached to the same VLANs/subnets, the multicast streams is uninterrupted when a multicast client roams from APs on one WLC to an AP on another WLC. The centralized deployment creates a flat WLC client multicast network. The reason centralized WLCs do not affect multicast roaming is because once the multicast stream is requested from a single multicast client on a WLAN, it streams out all APs on that WLAN, on all radios (802.11g and 802.11a), on all WLCs, even if that access point WLAN has no clients associated with it that have requested the multicast traffic. If you have more than one WLAN associated to the VLAN, the AP transmits the multicast packet over each WLAN. Both the unicast mode CAPWAP packet and the multicast mode CAPWAP packet contain a WLAN bitmap that tells the receiving AP which WLAN it must forward the packet over.

The distributed deployment does not have this problem because while the WLANs are the same, the WLCs are attached to different VLANs. This means that when the multicast client roams to a new WLC, the WLC will first query the client for its multicast group memberships. At this point the client responds with its group membership report and the WLC forwards this message to the appropriate multicast group address through the VLAN associated with its local VLAN. This allows the client to resume its multicast session through the foreign WLC.

The distributed deployment reduces the amount of multicast traffic on the APs because, although the WLAN SSIDs are the same, the WLCs are attached to different VLANs. WLAN multicast traffic depends on a client request on the VLAN of that WLC. Table 6-2 lists the advantages and disadvantages of distributed and collocated deployments.

Table 6-2 Pros and Cons of Centralized WLCs and Distributed WLCs

Deployment	PRO	CON
All centralized WLC WLANs connected to the same VLANs (subnets)	Multicast traffic started on any client VLAN will be transmitted to all APs so clients roaming to any AP will receive multicast stream	If only one client requests multicast traffic, all APs attached to all controllers will receive the stream and transmit it if they have any clients associated even if those clients did not request the multicast stream
Distributed WLCs on different VLANs and subnet	Multicast streams are isolated to APs attached to controller	Disruptions caused by multicast stream establishments after client roam

Additional Considerations

Two areas for additional consideration in multicast deployment are when implementing AP groups, and FlexConnect and APs. AP groups allow APs on the same controller to map the same WLAN (SSID) to different VLANs. If a client is roaming between APs in different groups, the multicast session will not function properly as this is currently not supported. Currently, the WLC forwards multicast only for the VLAN configured on the WLAN and does not take into consideration VLANs configured in AP groups.

FlexConnect APs allow the local termination of WLANs at the network edge rather than at the WLC, and the multicast behavior is controlled at that edge. If a FlexConnect WLAN is terminated on a WLC and multicast is enabled on that WLC, multicast is delivered to that FlexConnect WLAN, if the CAPWAP multicast group is allowed to extend to the FlexConnect network location.

Even if the CAPWAP multicast packets are not able to transit the network to the FlexConnect AP, WLAN clients on that FlexConnect AP are able to send IGMP joins to the network connected to the WLC, as these are unicast messages.

Information About 802.11v and Directed Multicast

From Release 8.1, controller supports 802.11v amendment for wireless networks, which describes numerous enhancements to wireless network management.

One such enhancement is **Network assisted Power Savings** which helps clients to improve battery life by enabling them to sleep longer. As an example, mobile devices typically use a certain amount of idle period to ensure that they remain connected to access points and therefore consume more power when performing the following tasks while in a wireless network.

Another enhancement is **Network assisted Roaming** which enables the WLAN to send requests to associated clients, advising the clients to choose better APs to associate. This is useful for both load balancing and for directing poorly connected clients.

Enabling 802.11v Network Assisted Power Savings

Wireless devices consume battery to maintain their connection to the clients, in several ways:

- By waking up at regular intervals to listen to the access point beacons containing a DTIM, which indicates buffered broadcast or multicast traffic that the access point will deliver to the clients.
- By sending null frames to the access points, in the form of keepalive messages to maintain connection with access points.
- Devices also periodically listen to beacons (even in the absence of DTIM fields) to synchronize their clock to that of the corresponding access point.

All these processes consume battery and this consumption particularly impacts devices (such as Apple), because these devices use a conservative session timeout estimation, and therefore, wake up often to send keepalive messages. The 802.11 standard, without 802.11v, does not include any mechanism for the controller or the access points to communicate to wireless clients about the session timeout for the local client.

To save the power of clients due to the mentioned tasks in wireless network, the following features in the 802.11v standard are used:

- Directed Multicast Service
- Base Station Subsystem (BSS) Max Idle Period

Directed Multicast Service

Using Directed Multicast Service (DMS), the client requests the access point to transmit the required multicast packet as unicast frames. This allows the client to receive the multicast packets it has ignored while in sleep mode and also ensures Layer 2 reliability. Also, the unicast frame will be transmitted to the client at a potentially higher wireless link rate, which enables the client to receive the packet quickly by enabling the radio for a shorter duration, thus saving battery power. As the wireless client does not have to wake up at each DTIM interval to receive multicast traffic, longer sleeping intervals are allowed.

BSS Max Idle Period

The BSS Max Idle period is the timeframe during which an access point (AP) does not disassociate a client due to non-receipt of frames from the connected client. This ensures that the client device does not send keepalive messages frequently. The idle period timer value is transmitted using the association and reassociation response frame from the access point to the client. The idle time value indicates the maximum time a client can remain idle without transmitting any frame to an access point. As a result, the clients remain in sleep mode for a longer duration without transmitting the keepalive messages often. This in turn contributes to saving battery power.

Configuring 802.11v Network Assisted Power Savings (CLI)

- Configure the value of BSS Max Idle period by entering these commands:
  - **config wlan usertimeout** *wlan-id*
  - **config wlan bssmaxidle {enable | disable}** *wlan-id*
- Configure DMS by entering the command:
  - **config wlan dms {enable | disable}** *wlan-id*

Overview of IPv6 Multicast

A multicast address is defined as an identifier for a set of interfaces that belong to different nodes. Multicast addresses are normally used to identify groups of interfaces that are interested in receiving similar content (for example, video). The conversation model in this case is a one-to-many model. Multicast addresses are all assigned out of the FF00::/8 block.

Multicast addresses also have a scope associated with them. The scopes are very similar to the scopes defined for unicast addresses:

- Link local—Link local multicast addresses are only intended for systems on a link and must not be forwarded by network equipment off that link. This behavior is the same as link local unicast addresses.
- Organization—Organizational multicast addresses are intended for use within an organization. These addresses are similar to the unicast unique local addresses.
- Global—Global multicast addresses are usable across the Internet similar to the unicast globally unique addresses.

There are some additionally defined scopes for IPv6 multicast addresses:

- Interface local—Interface local multicast addresses are intended for transmission of multicast within a node.
- Site local—Site local multicast addresses are intended for use within a single site.

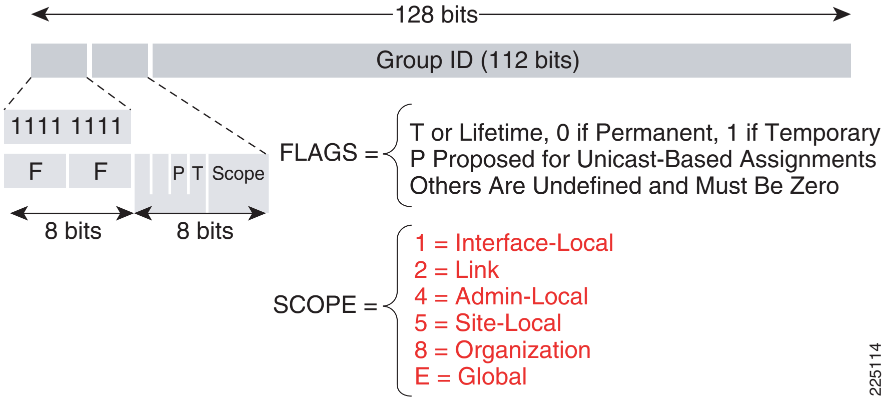
Figure 6-4 lays out the format of an IPv6 multicast address.

Similar to the unicast address space, there are some reserved or special use multicast addresses. A couple of the more common multicast groups and their intended use are mentioned below. For a more comprehensive list of currently assigned multicast addresses, see: http://www.iana.org/assignments/ipv6-multicast-addresses

Some of the more common multicast addresses seen on IPv6 systems include:

- FF02::1—Link local, all nodes address
- FF02::2—Link local, all routers address
- FF02:0:0:0:0:1:FFXX:XXXX—Link local, solicited-node address

Figure 6-4 Multicast Address Representation



Multicast Listener Discover – MLD

Cisco software supports the following protocols to implement IPv6 multicast routing:

- MLD for IPv6. MLD is used by IPv6 routers and controllers to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links. There are two versions of MLD: MLD version 1 is based on version 2 of the Internet Group Management Protocol (IGMP) for IPv4, and MLD version 2 is based on version 3 of the IGMP for IPv4. IPv6 multicast for Cisco software uses both MLD version 2 and MLD version 1.
  MLD version 2 is fully backward compatible with MLD version 1 (described in RFC 2710). Hosts that support only MLD version 1 will interoperate with a router running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.
- PIM-SM is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- PIM in Source Specific Multicast (PIM-SSM) is similar to PIM-SM with the additional ability to report interest in receiving packets from specific source addresses (or from all but the specific source addresses) to an IP multicast address.

IPV6 Multicast Support on Wireless LAN Controllers

Beginning with release 8.0, the wireless LAN controller supports MLDv1 snooping for IPv6 multicast allowing it to intelligently keep track of and deliver multicast flows to clients that request them.

Note Unlike previous versions of releases, IPv6 Unicast traffic support does not mandate for **Global Multicast Mode** to be enabled on the controller. IPv6 Unicast traffic support is enabled automatically.

To configure Multicast for IPv6, perform the following steps:

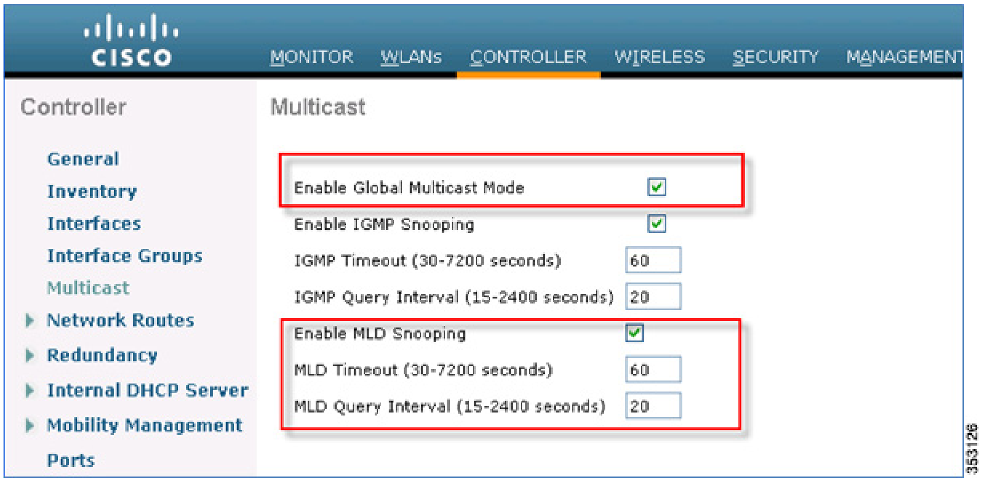
Step 1 For IPv6 Multicast to be enabled, check the **Enable Global Multicast Mode** check box.

Step 2 Check the **Enable MLD Snooping** check box to support IPv6 forwarding decisions.

Note To enable MLD Snooping, you must enable **Global Multicast Mode** of the controller.

Step 3 Configure Multicast Mode:

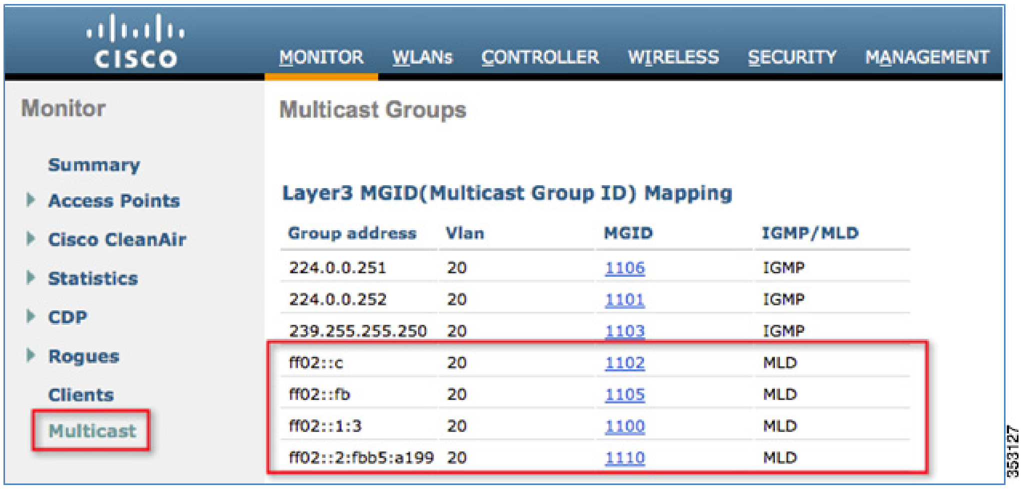
- **a.** In the **MLD Timeout** text box, enter a value between 30 and 7200 seconds to set the MLD timeout.
- **b.** In the **MLD Query Interval** text box, enter a value between 15 and 2400 seconds.
- **c.** Click **Apply**.
- **d.** Click **Save Configuration**.



Multicast

Enable Global Multicast Mode ☑
Enable IGMP Snooping ☑
IGMP Timeout (30-7200 seconds) 60
IGMP Query Interval (15-2400 seconds) 20
Enable MLD Snooping ☑
MLD Timeout (30-7200 seconds) 60
MLD Query Interval (15-2400 seconds) 20

Step 4 To verify that IPv6 multicast traffic is being snooped, go to **Monitor > Multicast**. Note that both IPv4 (IGMP) and IPv6 (MLD) multicast groups are listed. Click **MGID** to view the wireless clients joined to that group address.



Multicast Groups

Layer3 MGID(Multicast Group ID) Mapping

Group address	Vlan	MGID	IGMP/MLD
224.0.0.251	20	1106	IGMP
224.0.0.252	20	1101	IGMP
239.255.255.250	20	1103	IGMP
ff02::c	20	1102	MLD
ff02::fb	20	1105	MLD
ff02::1:3	20	1100	MLD
ff02::2:fbb5:a199	20	1110	MLD

Multicast Domain Name System – mDNS/Bonjour

Table 6-3 lists the Bonjour features from release 7.4 through 8.1.

Table 6-3 Summary of Services in Phase 1, 2, 3, and 4

Bonjour - 7.4 (Phase 1)	Bonjour - 7.5 (Phase 2)	Bonjour - 8.0 (Phase 3)	Bonjour - 8.1 (Phase 4)
• Bonjour service with mDNS gateway for wired and wireless services • Bonjour service policy applied per interface or per WLAN • mDNS services cached on the controller • Bonjour services available on all controller seen L2 domains • Bonjour services supported on the Anchor controller • Bonjour services supported with L2 and L3 roaming • 100 services and 64 service providers per service type • Support of FlexConnect APs in central mode	• Support of mDNS services across L3 domains • Introduction of mDNS AP for Bonjour service snooping on 10 wired VLANs • LSS – Location Specific Services • Priority MAC of Bonjour service • Origin based service discovery • 6400 services and service providers per service type	• Bonjour GW with access policy controlled service discovery • Device service mapping to access policy • Bonjour group and single access policy management • Bonjour profile control by local policy • Introduction of Bonjour administrator to manage specific Bonjour services from Cisco Prime	• Number of supported services is scaled

Information About Multicast Domain Name System

Multicast Domain Name System (mDNS) service discovery provides a way to announce and discover the services on the local network. The mDNS service discovery enables wireless clients to access Apple services such as Apple Printer and Apple TV advertised in a different Layer 3 network. mDNS performs DNS queries over IP multicast. mDNS supports zero-configuration IP networking.

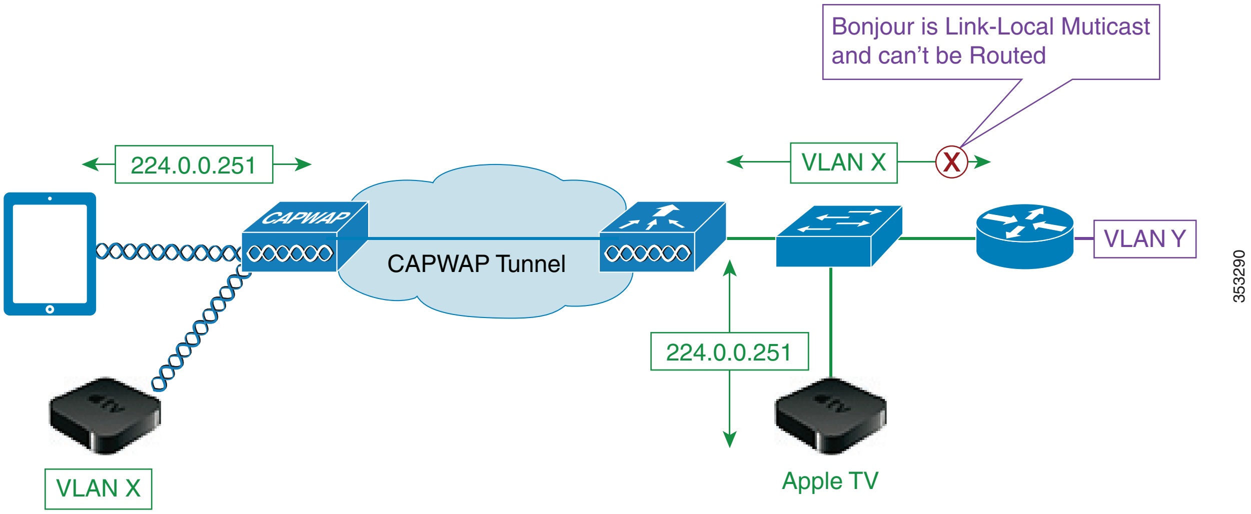
Bonjour protocol operates on service announcements and service queries, which allow devices to ask and advertise specific applications such as:

- Printing Services
- File Sharing Services
- Remote Desktop Services
- iTunes File Sharing
- iTunes Wireless iDevice Syncing (in Apple iOS v5.0+)
- AirPlay offering the following streaming services:
  - Music broadcasting in iOS v4.2+
  - Video broadcasting in iOS v4.3+
  - Full screen mirroring in iOS v5.0+ (iPad2, iPhone4S or later)

Each query or advertisement is sent to the Bonjour multicast address for delivery to all clients on the subnet. Apple's Bonjour protocol relies on mDNS operating at UDP port 5353 and sent to the following reserved group addresses:

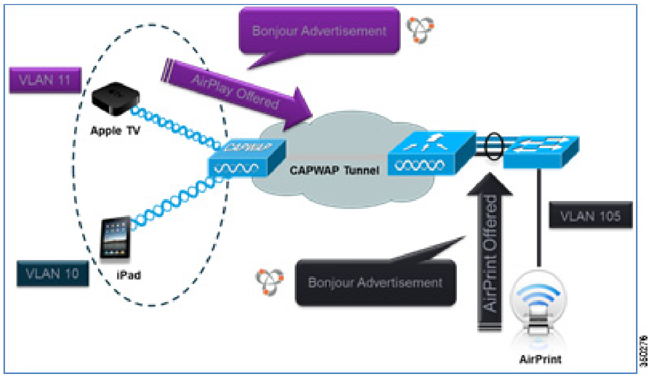
- IPv4 Group Address – 224.0.0.251
- IPv6 Group Address – FF02::FB

The addresses used by the Bonjour protocol are link-local multicast addresses, and thus are only forwarded to the local L2 domain. Routers cannot use multicast routing to redirect the traffic because the time to live (TTL) is set to one, and link-local multicast is meant to stay local by design.

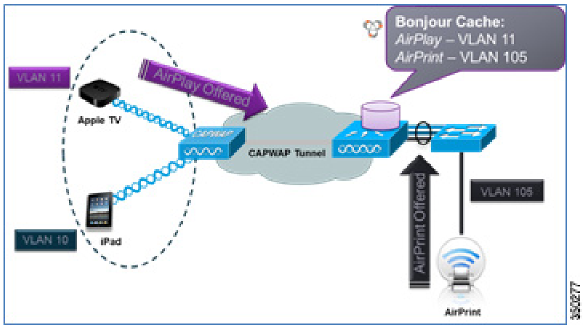


To address this issue, Cisco WLC acts as a Bonjour Gateway. The WLC listens for Bonjour services and by caching those Bonjour advertisements (AirPlay, AirPrint, and so on) from the source/host, for example AppleTV, it responds back to Bonjour clients when a request for service is initiated. The following illustrates this process:

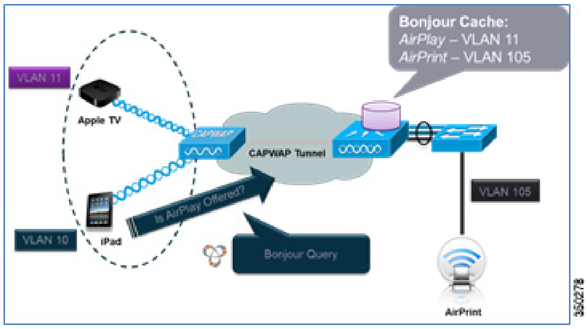
Step 1 The controller listens for the bonjour services.



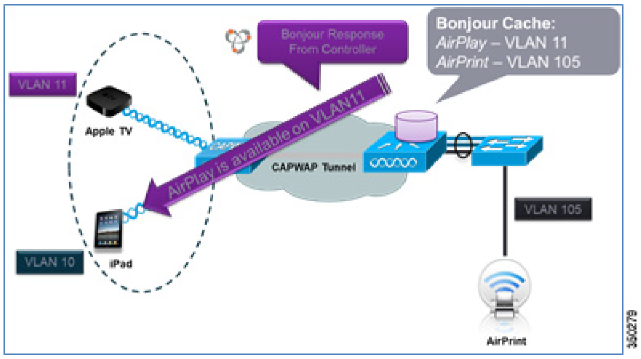
Step 2 The controller cache those bonjour services.



Step 3 The controller listens for the client queries for services.



Step 4 The controller sends a unicast response to the client queries for bonjour services.

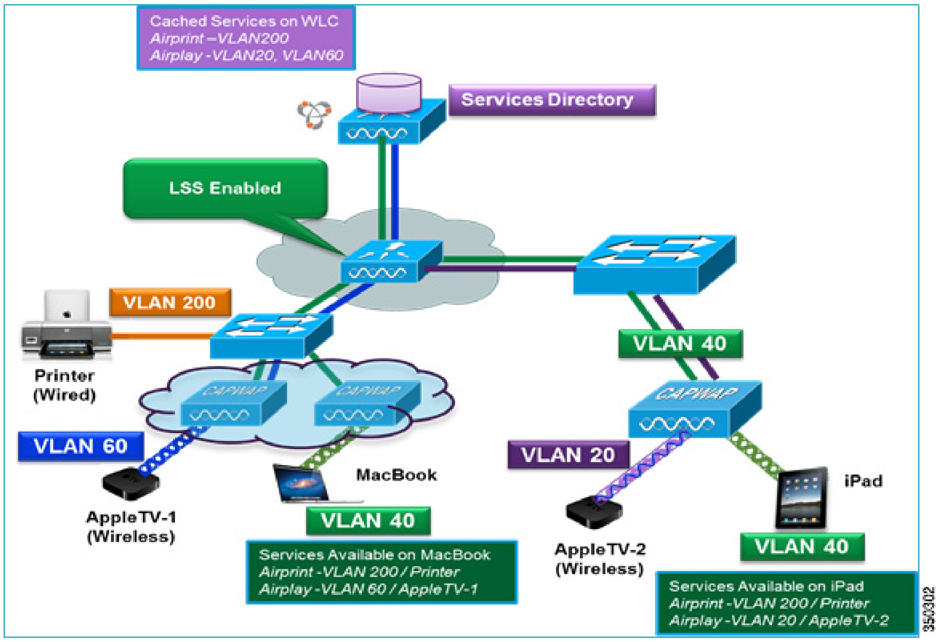


Location Specific Services

The processing of mDNS service advertisements and mDNS query packets support Location Specific Services (LSS). All the valid mDNS service advertisements that are received by the controller are tagged with the MAC address of the AP that is associated with the service advertisement from the service provider while inserting the new entry into the service provider database. The response formulation to the client query filters the wireless entries in the service provider database using the MAC address of the AP associated with the querying client. The wireless service provider database entries are filtered based on the AP-NEIGHBOR-LIST if LSS is enabled for the service. If LSS is disabled for any service, the wireless service provider database entries are not filtered when they respond to any query from a wireless client for the service.

LSS applies only to wireless service provider database entries. There is no location awareness for wired service provider devices.

The status of LSS cannot be enabled for services with ORIGIN set to wired and vice versa.



mDNS AP

The mDNS AP feature allows the controller to have visibility of wired service providers that are on VLANs not visible to the controller. You can configure any AP as an mDNS AP and enable the AP to forward mDNS packets to the controller. VLAN visibility on the controller is achieved by APs that forward the mDNS advertisements to the controller. The mDNS packets between the AP and the controller are forwarded in Control and Provisioning of Wireless Access Points (CAPWAP) data tunnel that is similar to the mDNS packets from a wireless client. Only CAPWAP v4 tunnels are supported. APs can be in either the access port or the trunk port to learn the mDNS packets from the wired side and forward them to the controller. You can use the configurable knob that is provided on the controller to start or stop mDNS packet forwarding from a specific AP. You can also use this configuration to specify the VLANs from which the AP should snoop the mDNS advertisements from the wired side. The maximum number of VLANs that an AP can snoop is 10.

If the AP is in the access port, you should not configure any VLANs on the AP to snoop. The AP sends untagged packets when a query is to be sent. When an mDNS advertisement is received by the mDNS AP, the VLAN information is not passed on to the controller. The service provider's VLAN that is learned through the mDNS AP's access VLAN is maintained as 0 in the controller.

By default, the mDNS AP snoops in native VLAN. When an mDNS AP is enabled, native VLAN snooping is enabled by default and the VLAN information is passed as 0 for advertisements received on the native VLAN.

The mDNS AP feature is supported only on local mode and monitor mode APs. The mDNS AP configuration is retained on those mDNS APs even if global mDNs snooping is disabled. If an mDNS AP is reset or associated with the same controller or another controller, one of the following occurs:

- If the global snooping is disabled on the controller, a payload is sent to the AP to disable mDNS snooping.
- If the global snooping is enabled on the controller, the configuration of the AP before the reset or the association procedure is retained.

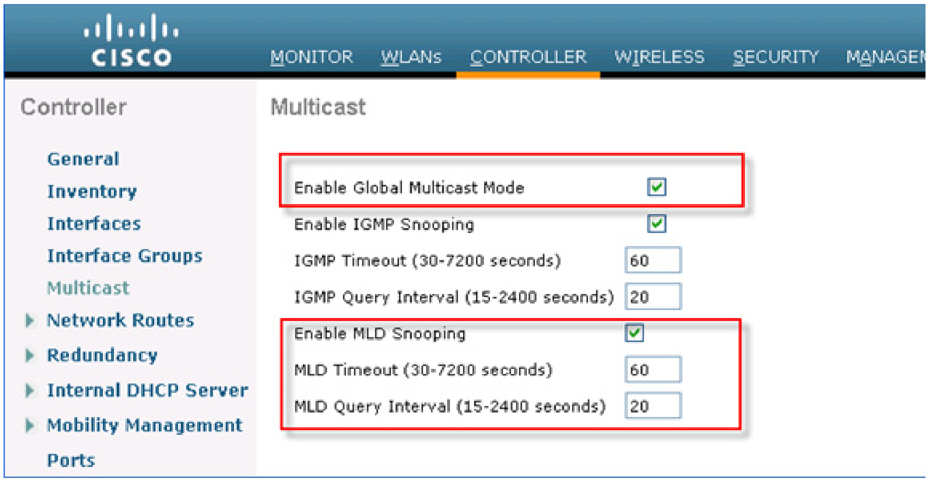
The process flow for the mDNS AP feature is as follows:

Uplink (Wired infrastructure to AP to Controller)

1. Receives the 802.3 mDNS packet on configured VLANs.
2. Forwards the received mDNS packet over CAPWAP.
3. Populates multicast group ID (MGID) based on the received VLAN.

Downlink (Controller to AP to Wired Infrastructure)

1. Receives an mDNS query over CAPWAP from the controller.
2. Forwards the query as 802.3 packet to wired infrastructure.
3. The VLAN is identified from dedicated MGIDs.



Multicast

Enable Global Multicast Mode ☑
Enable IGMP Snooping ☑
IGMP Timeout (30-7200 seconds) 60
IGMP Query Interval (15-2400 seconds) 20
Enable MLD Snooping ☑
MLD Timeout (30-7200 seconds) 60
MLD Query Interval (15-2400 seconds) 20

Restrictions for Configuring Multicast DNS

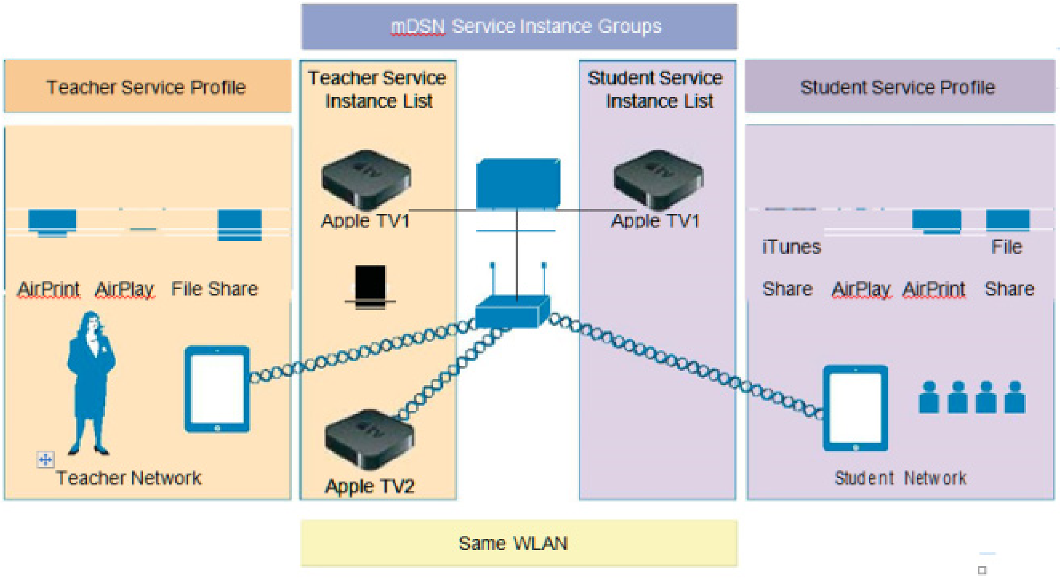
- mDNS over IPv6 is not supported.
- mDNS is not supported on access points in FlexConnect mode in a locally switched WLAN and mesh access points.
- mDNS is not supported on remote LANs.
- mDNS is not supported on Cisco AP 1240 and AP 1130.
- Third party mDNS servers or applications are not supported on the Cisco WLC using the mDNS feature. Devices that are advertised by the third party servers or applications are not populated on the mDNS service or device table correctly on the Cisco WLC.
- In a Layer2 network, if Apple servers and clients are in the same subnet, mDNS snooping is not required on the Cisco WLC. However, this relies on the switching network to work. If you use switches that do not work as expected with mDNS snooping, you must enable mDNS on the Cisco WLC.
- Video is not supported on Apple iOS 6 with WMM in enabled state.
- mDNS APs cannot duplicate the same traffic for the same service or VLAN.
- DLSS filtering is restricted to only wireless services.
- The LSS, mDNS AP, Priority MAC address, and origin-based discovery features cannot be configured using the controller GUI.
- mDNS-AP feature is not supported in CAPWAP V6.
- DISE dynamic mDNS policy mobility is not supported.
- mDNS user profile mobility is not supported in guest anchors.

- Apple devices such as iPads and iPhones can discover Apple TV through Bluetooth. This might result in Apple TVs being visible to end users. Because Apple TVs are not supported on mDNS access policy, Cisco recommends you to disable Bluetooth on Apple TVs.

Introduction to Bonjour Policies and New Requirements

Bonjour gateway snoops and caches Bonjour services across VLANs and periodically refreshes the services. WLC acts as a proxy for all Bonjour services published by wireless and wired devices. Prior to release 8.0, Bonjour gateway had inadequate capabilities to filter cached wired / wireless service instances based on the credentials of the querying client and its location.

With introduction of the Bonjour policies in the release 8.0, the administrator can configure to identify who uses the Bonjour service instances and in what location (all this applies to the same WLAN). With introduction of the Bonjour policies, the administrator does not need to create multiple WLANs to select which services are allowed or should be used on specific WLAN. Based on user 802.1x authentication, the AAA server or ISE can be configured to return USER-ROLE or BONJOUR-PROFILE in the form of the “CISCO-AV-PAIR”. This value gets plumbed into the policy created on the wireless controller. Based on the user authentication, a configured policy and profile are applied to a specific user on the same WLAN.



As mentioned in the figure above, improvements to Bonjour services are made. Bonjour policies are introduced to allow per service instance (MAC address) configuration that mandates how the service instance is shared, which is articulated as follows:

- Service instance is shared with whom (user-id).
- Service instance is shared with which role/s (client-role).
- Location where the Service Instance allowed to be accessed (Client Location)

This configuration can be applied to wired and wireless service instances, and the response to any query will solely be based on the policy configured for each service instance. This allows selective sharing of service instances based on the location, user-id, or role. As most service publishing devices are wired, this allows filtering of wired services at par with wireless service instances. While mDNS profile associated with the client checks for service type being queried before responding to the query, the access policy further allows filtering of specific service instances based on querying client location, role, or user-id.

With Bonjour access policy, there are two levels of filtering the client queries, which are as follows:

- At the service type level by using the mDNS profile.
- At the service instance level using the access policy associated with the service instance.

A service instance or a set of service instances discovered and cached by the WLC can be associated with an access policy filter, which acts like a lens that determines which clients and what kind of client context (role or user-id) can see and access the service instance.

Note Service instances that are not configured with any access policy will be mapped to the default access policy, which allows only the administrator user role, by default, to receive the service instances. Additional users can be configured and added in the default policy.

- Bonjour access policy filters can be configured for specific service instances identified by the MAC address of the devices publishing the services.
- Bonjour access policy is associated with a service group name that contains one or more MAC addresses of the devices publishing the Bonjour services.
- The service group name is then attached to the service instance when it is discovered and cached at the WLC.
- While traversing the list of service instances in response to a client query, each instance will be evaluated to verify if the querying client location, role, or user-id are allowed access to the service instance before including the same in the response.

If the same MAC address is configured in multiple service groups, it means the service instance will be associated with all the service group names that are configured with this MAC address. All the access policies associated with the MAC addressee’s service group names will be evaluated until the decision is to include the service instance. Currently, a maximum of five service groups are supported for a single MAC address. Service group configurations can be done even when mDNS snooping is disabled or offline, and the access policy comes into effect when the services are discovered. It can also be done dynamically when snooping is already enabled.

Bonjour Service Groups

A service group name can be associated with a set of MAC addresses. The maximum MAC addresses that can be configured for any service group is limited by the platform dependent global maximum number of service instances that can be discovered:

- In release 8.0, service limit: 6400 services on 2500, 5508, WiSM2, and vWLC and 16000 services on 7510 and 8510 UC controllers.
- In release 8.1, the service limit has changed to be more reflective of number of the AP licenses and clients supported and will change accordingly on 5508 and WiSM-2 controllers.

	Bonjour Cache @ Full Scale	Bonjour Cache @ 80% Scale
5508 in 8.0 release	6400	6400
5508 in 8.1 release	1000	2400

	Bonjour Cache @ Full Scale	Bonjour Cache @ 80% Scale
WiSM2 in 8.0 release	6400	6400
WiSM2 in 8.1 release	2000	4800
5520, 7500, 8500, vWLC	16,000	16,000
2504 IN 8.0 release	6400	6400
2500 IN 8.1 release	Not recommended	Not recommended

As shown in the table above, in release 8.1, 5508 controller is scaled down to support only 1000 services at full scale (500 APs and 7000 clients). With 80% scale (400 APs and 5400 users), the same 5508 controller supports 2400 services. Similarly, WiSM-2 supports 2000 services at full scale (1000 APs and 15000) and 4800 services at 80% scale. Number of Bonjour services remains unchanged on the 7500 and vWLC controllers. 5520 and 8500 series controllers support 16,000 services in release 8.1. On 2504 controller, the number of services drop significantly due to memory limitation. Therefore, Bonjour deployment should be limited to testing or very limited number of services. At full scale, it is not recommended to run Bonjour services on the 2504 controller with 8.1 software.

Wired and Wireless Location Specific Services

Each MAC address is configured with a unique name, which can be the service instance name, and the location of the MAC address for both wired and or wireless.

1. Since flexibility is desired when configuring the location using the AP-NAME, AP-GROUP, or AP-LOCATION, the administrator has to configure the type of location that is desired. This configuration implies that only clients from the same location as that of the device publishing the service can access the service. As long as the global maximum limit of MAC addresses is not exceeded, any service group can configure as many MAC addresses as desired.

   In case of wireless service instances, the device location can change. Yet, if you want only those devices whose location is same as that of the service instance, the keyword “same” could be configured for such wireless service providers.

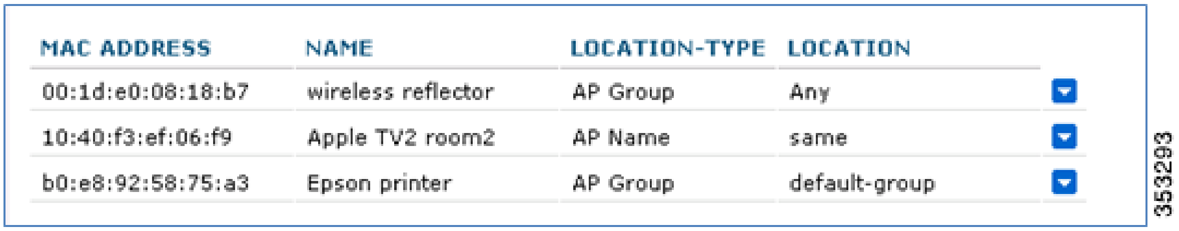
   In case of wired services, the same location does not apply because wired clients do not get associated to the AP.
2. If the keyword “Any” is configured for location, it implies that there is no location based filtering for the clients trying to access the device. This means the clients from any location can access the service subject to role and user-id credentials being allowed by the policy associated with the service group for that MAC address.
3. If the keyword “ap-name” is used, only clients associated to that AP can access the service instance.

Note Location validation is implicit and will be the first level of access policy filtering even before ROLE and USER-ID credentials of the client are verified.

Table 6-4 depicts a possible policy configuration with the service group named AppleTV-teachers.

Table 6-4 Example for Policy Configuration with the Service Group Name

Service Group Name	MAC Address	Service Name	Location Type	Location
AppleTV-teachers	e8:b7:48:9b:f0:20	AppleTV-class1	AP-GROUP	6-FLR
	e8:b7:48:9b:f0:21	AppleTV-class2	AP-NAME	AP4403.a740.bc97
	—	—	—	—
	e2:34:23:11:32:eb	AppleTV-class9	AP-NAME	same
	—	—	—	—
	e8:c7:38:9c:f1:32	AppleTV -class3	AP-GROUP	any



MAC ADDRESS	NAME	LOCATION-TYPE	LOCATION	
00:1d:e0:08:18:b7	wireless reflector	AP Group	Any	▾
10:40:f3:ef:06:f9	Apple TV2 room2	AP Name	same	▾
b0:e8:92:58:75:a3	Epson printer	AP Group	default-group	▾

Device Access Policy Constructs and Rules

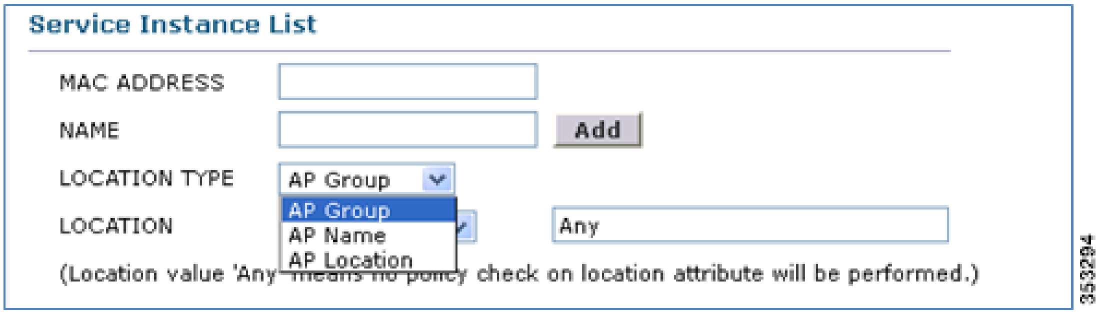
This section explains the access policy in terms of the client context attributes, its constructs, the rule components that make up of the policy, and how the rules and hence the policies are evaluated. This helps in deciding whether the given service instance should be included or not in the mDNS response for the client that made the mDNS query. Further, if multiple service instances are mapped to the same access policy, for a given mDNS query, the policy will be evaluated only once for all those instances which have the same access policy mapping to optimize the policy evaluation overhead for a given query.

Client Context Attributes in an mDNS Policy

Any client initiating an mDNS query can be associated with a set of attributes that describe the context of the client. The attributes, for example location, can change dynamically when the clients move to a different location. Only these enumerated attributes will be used to articulate a Bonjour access policy rule. The list of attributes and how they are fetched are detailed in Table 6-5. The user can formulate a rule by combining these attributes with logical OR operations and attach the rule to the policy. A policy is composed of a single rule, even though multiple rules can be provisioned.

Table 6-5 Attributes and Their Usage

S.No	Attribute Name	Description	When used in configuration
1	ROLE	Is a string like "teacher" or "student" and plumbed into the DB of the client. ISE or AAA can associate a role to a client.	Administrator must add the role name and user_id to create a rule.
2	LOCATION	Location of the client is a string, which is the "ap-location" of the client's AP.	When this is used to configure a rule, the user could mention any of the below three to specify location: • ap-location • ap-name • ap-group name
3	USER-ID	Uniquely identifies whether the client is plumed into the client DB by AAA or ISE during 802.1x authentication.	Exactly same string name must be used by user, while configuring a policy that uses user-id.



Service Instance List

MAC ADDRESS

NAME

LOCATION TYPE: AP Group

LOCATION: Any

(Location value 'Any' means no policy check on location attribute will be performed.)

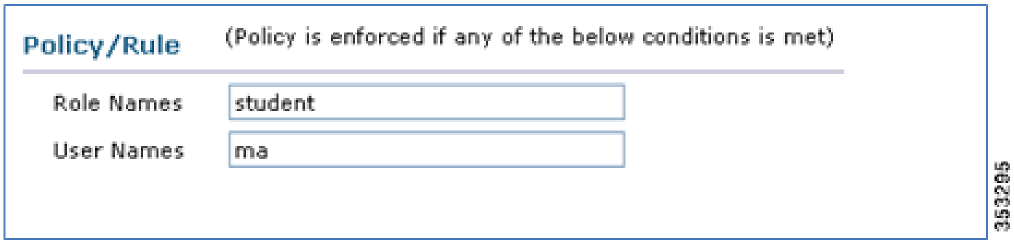
Access Policy Rules

An access policy service group is identified by a name and is associated with just one rule.

The rule is defined using the role or user-id (comma separated list). It implies that, a client, making an mDNS query, whose role is one of those listed in the policy roles or the client user-id is one of those listed in the user-id list, then access to the service instances is granted.

RULE is defined as,

[ROLE=teacher, student] AND [USER-ID = John, Mike]



Policy/Rule (Policy is enforced if any of the below conditions is met)

Role Names: student

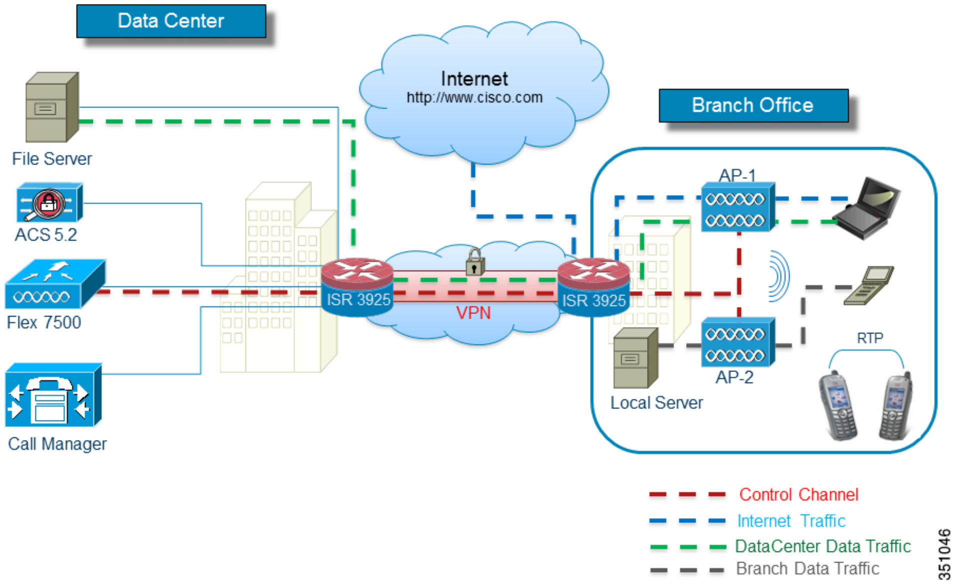
User Names: ma

CHAPTER 7

FlexConnect

FlexConnect (previously known as Hybrid Remote Edge Access Point or H-REAP) is a wireless solution for branch office and remote office deployments. It enables you to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without the deployment of a controller in each office. The FlexConnect access points (APs) can switch client data traffic locally and perform client authentication locally. When they are connected to the controller, they can also send traffic back to the controller.

Figure 7-1 FlexConnect Architecture



Note To view the FlexConnect feature matrix, see: http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b3690b.shtml#matrix

Supported Platforms

FlexConnect is only supported on these components:

- Cisco AP-1130, AP-1240, AP-1040, AP-1140, AP-1260, AP-1250, AP-3500, AP-1600, AP-2600, AP-3600, AP-3700, AP-1700, AP-2700, AP 700, AP-1520, AP-1530, AP-1550, AP-1570 access points
- Cisco 5520, 8540, Flex 7500, Cisco 8500, 4400, 5500, and 2500 series controllers
- Cisco WiSM-2
- Cisco virtual controller (vWLC)

FlexConnect Terminology

For clarity, this section provides a summary of the FlexConnect terminology and definitions used throughout this chapter.

Switching Modes

FlexConnect APs are capable of supporting the following switching modes concurrently, on a per-WLAN basis.

Local Switched

Locally-switched WLANs map wireless user traffic to discrete VLANs via 802.1Q trunking, either to an adjacent router or switch. If so desired, one or more WLANs can be mapped to the same local 802.1Q VLAN.

A branch user, who is associated to a local switched WLAN, has their traffic forwarded by the on-site router. Traffic destined off-site (to the central site) is forwarded as standard IP packets by the branch router. All AP control/management-related traffic is sent to the centralized Wireless LAN Controller (WLC) separately via Control and Provisioning of Wireless Access Points protocol (CAPWAP).

Central Switched

Central switched WLANs tunnel both the wireless user traffic and all control traffic via CAPWAP to the centralized WLC where the user traffic is mapped to a dynamic interface/VLAN on the WLC. This is the normal CAPWAP mode of operation.

The traffic of a branch user, who is associated to a central switched WLAN, is tunneled directly to the centralized WLC. If that user needs to communicate with computing resources within the branch (where that client is associated), their data is forwarded as standard IP packets back across the WAN link to the branch location. Depending on the WAN link bandwidth, this might not be desirable behavior.

Operation Modes

There are two modes of operation for the FlexConnect AP.

Connected mode—The WLC is reachable. In this mode the FlexConnect AP has CAPWAP connectivity with its WLC.

Standalone mode—The WLC is unreachable. The FlexConnect has lost or failed to establish CAPWAP connectivity with its WLC: for example, when there is a WAN link outage between a branch and its central site.

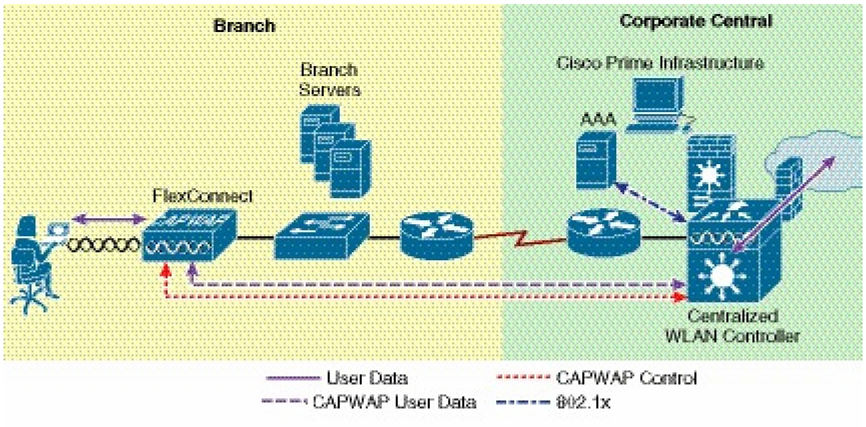
FlexConnect States

A FlexConnect WLAN, depending on its configuration and network connectivity, is classified as being in one of the following defined states.

Authentication-Central/Switch-Central

This state represents a WLAN that uses a centralized authentication method such as 802.1X, VPN, or web. User traffic is sent to the WLC via CAPWAP. This state is supported only when FlexConnect is in connected mode (Figure 7-2); 802.1X is used in the example, but other mechanisms are equally applicable.

Figure 7-2 Authentication-Central/Switch-Central WLAN



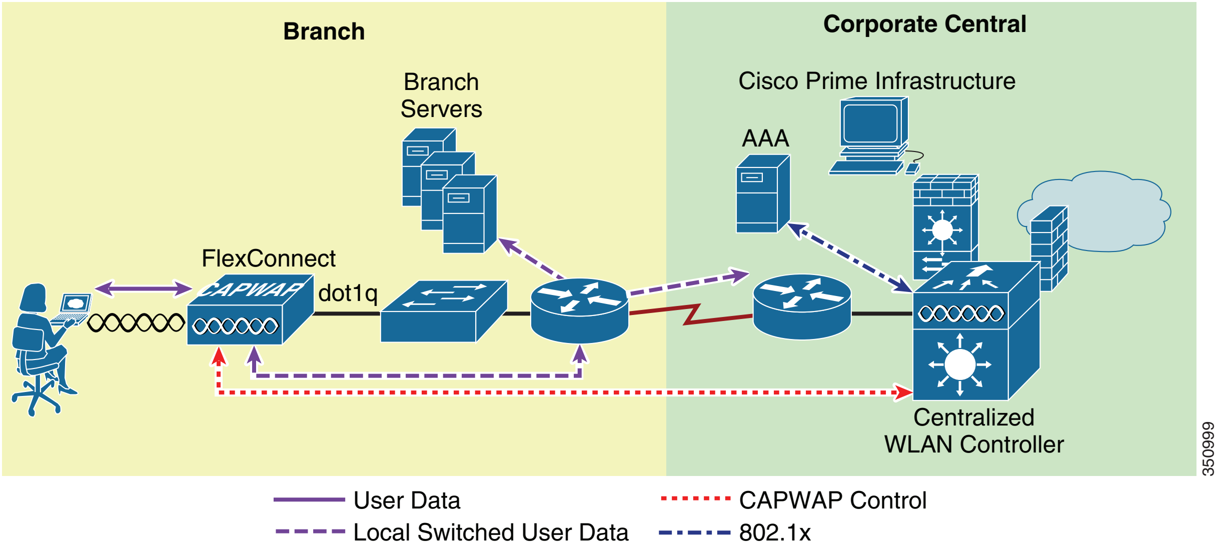
Authentication Down/Switching Down

Central switched WLANs (above) no longer beacon or respond to probe requests when the FlexConnect AP is in standalone mode. Existing clients are disassociated.

Authentication-Central/Switch-Local

This state represents a WLAN that uses centralized authentication, but user traffic is switched locally. This state is supported only when the FlexConnect AP is in connected mode (Figure 7-3); 802.1X is used in the Figure 7-3 example, but other mechanisms are equally applicable.

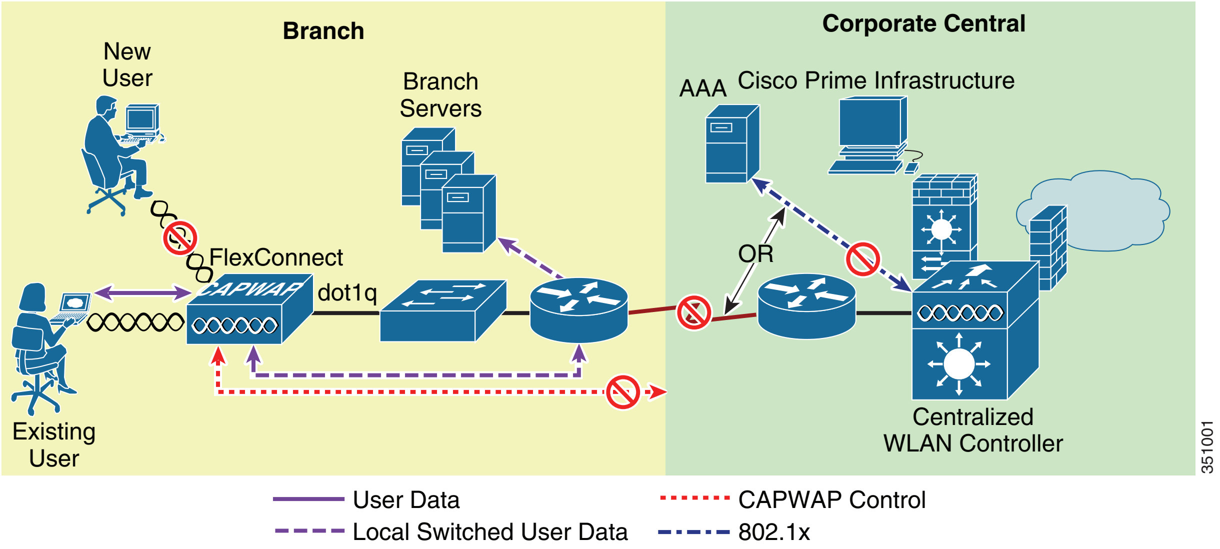
Figure 7-3 Authentication-Central/Switch-Local WLAN



Authentication-Down/Switch-Local

A WLAN that requires central authentication (as explained above) rejects new users. Existing authenticated users continue to be switched locally until session time-out (if configured). The WLAN continues to beacon and respond to probes until there are no more (existing) users associated to the WLAN. This state occurs as a result of the AP going into standalone mode (Figure 7-4).

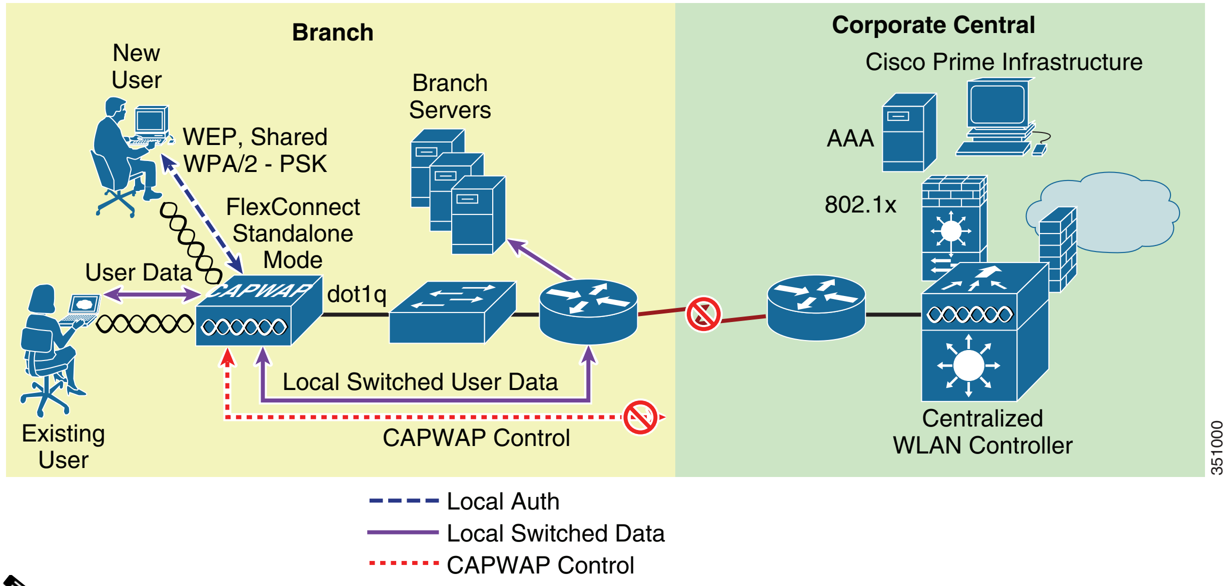
Figure 7-4 Authentication-Down/Local Switch



Authentication-local/switch-local

This state represents a WLAN that uses open, static WEP, shared, or WPA2 PSK security methods. User traffic is switched locally. These are the only security methods supported locally if a FlexConnect goes into standalone mode. The WLAN continues to beacon and respond to probes (Figure 7-5). Existing users remain connected and new user associations are accepted. If the AP is in connected mode, authentication information for these security types is forwarded to the WLC.

Figure 7-5 Authentication-Local/Switch-Local WLAN



Note All 802.11 authentication and association processing occurs regardless of which operational mode the AP is in. When in connected mode, the FlexConnect AP forwards all association/authentication information to the WLC. When in standalone mode, the AP cannot notify the WLC of such events, which is why WLANs that make use of central authentication/switching methods are unavailable.

Applications

The FlexConnect AP offers greater flexibility in how it can be deployed, such as:

- Branch wireless connectivity
- Branch guest access
- Public WLAN hotspot
- Wireless BYOD in Branch sites

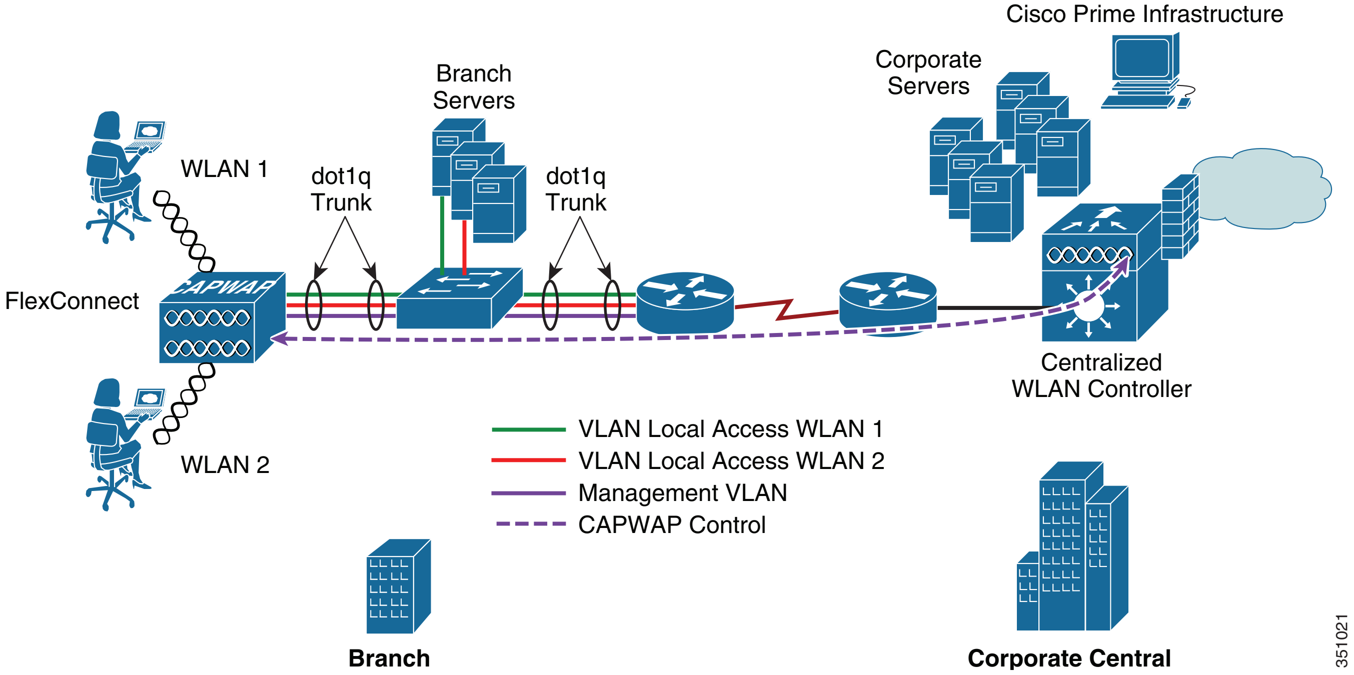
Branch Wireless Connectivity

FlexConnect addresses the wireless connectivity needs in branch locations by permitting wireless user traffic to terminate locally rather than tunneled across the WAN to a central WLC. With FlexConnect, branch locations can more effectively implement segmentation, access control, and QoS policies on a per-WLAN basis, as shown in Figure 7-6.

Branch Guest Access

The centralized WLC itself, as shown in Figure 7-6, can perform web authentication for guest access WLANs. The guest user's traffic is segmented (isolated) from other branch office traffic. For more detailed information on guest access, refer to Chapter 10, "Cisco Unified Wireless Network Guest Access Services."

Figure 7-6 FlexConnect Topology

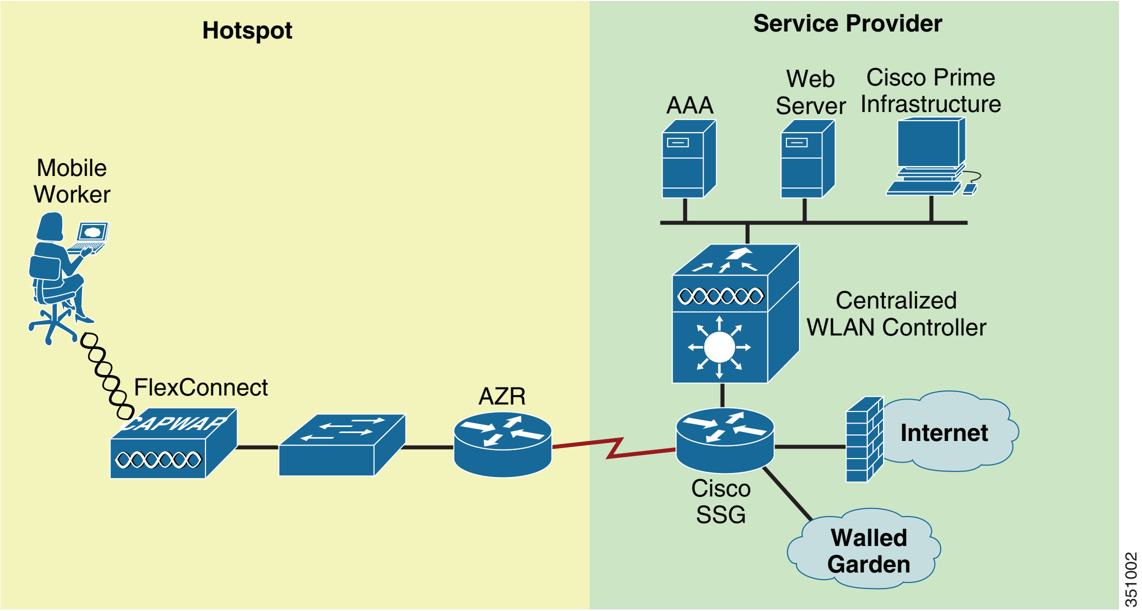


Public WLAN Hotspot

Many public hotspot service providers are beginning to implement multiple SSID/WLANs. One reason for this is because an operator might want to offer an open authentication WLAN for web-based access and another WLAN that uses 802.1x/EAP for more secure public access.

The FlexConnect AP, with its ability to map WLANs to separate VLANs, is an alternative to a standalone AP for small venue hotspot deployments where only one, or possibly two, APs are needed. Figure 7-7 provides an example of hotspot topology using a FlexConnect AP.

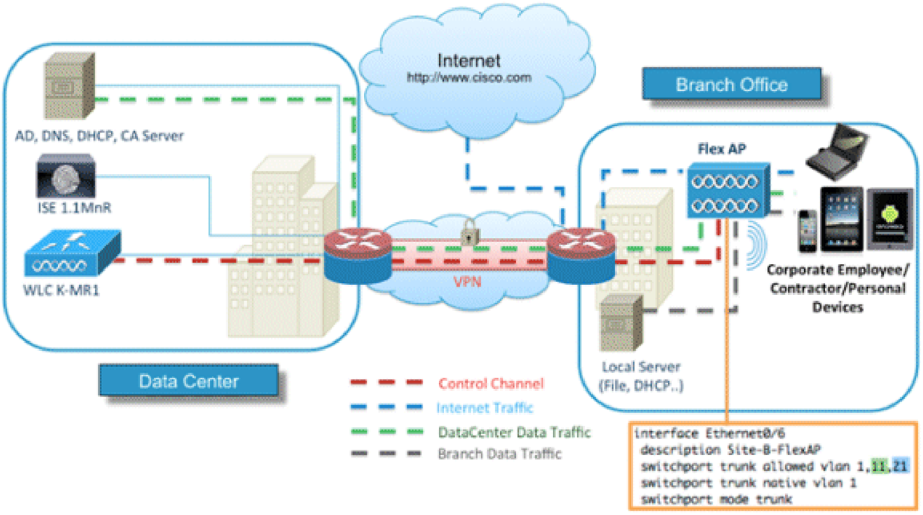
Figure 7-7 Hotspot Access using FlexConnect Local Switching



Wireless BYOD in Branch sites

Release 7.2.110.0 supports these ISE functionalities for FlexConnect APs for local switching and centrally authenticated clients. Also, release 7.2.110.0 integrated with ISE 1.1.1 provides (but is not limited to) these BYOD solution features for wireless:

- Device profiling and posture
- Device registration and supplicant provisioning
- Onboarding of personal devices (provision iOS or Android devices)



```
interface Ethernet0/6
 description Site-B-FlexAP
 switchport trunk allowed vlan 1,11,21
 switchport trunk native vlan 1
 switchport mode trunk
```

Deployment Considerations

The following section covers the various implementation and operational caveats associated with deploying FlexConnect APs.

WAN Link

For the FlexConnect AP to function predictably, keep in mind the following with respect to WAN link characteristics:

- Latency—A given WAN link should not impose latencies greater than 100 ms. The AP sends heartbeat messages to the WLC once every thirty seconds. If a heartbeat response is missed, the AP sends five successive heartbeats (one per second) to determine whether connectivity still exists. If connectivity is lost, the FlexConnect AP switches to standalone mode.

  Similarly, AP and WLC exchange echo CAPWAP packet to check the connectivity. If the echo CAPWAP packet response is missed, the AP sends five successive echo CAPWAP packets (every three seconds) to determine whether the connectivity still exists. If the connectivity is lost, the FlexConnect AP switches to standalone mode. (see Operation Modes, page 7-3 for operation mode definitions). The AP itself is relatively delay tolerant. However, at the client, timers associated with authentication are sensitive to link delay, and thus a constraint of $\leq$ 100 ms is required. Otherwise, the client can time-out waiting to authenticate, which can cause other unpredictable behaviors, such as looping.
- Bandwidth—WAN links should be at least 128 kbps for deployments when up to eight APs are being deployed at a given location. If more than eight APs are deployed, proportionally more bandwidth should be provisioned for the WAN link.
- Path MTU—An MTU no smaller than 500 bytes is required.

Roaming

When a FlexConnect AP is in connected mode, all client probes, association requests, 802.1x authentication requests, and corresponding response messages are exchanged between the AP and the WLC via the CAPWAP control plane. This is true for open, static WEP, and WPA PSK-based WLANs even though CAPWAP connectivity is not required to use these authentication methods when the AP is in standalone mode.

- Dynamic WEP/WPA—A client that roams between FlexConnect APs using one of these key management methods performs full authentication each time it roams. After successful authentication, new keys are passed back to the AP and client. This behavior is no different than a standard centralized WLAN deployment, except that in an FlexConnect topology, there can be link delay variations across the WAN, which can in turn impact total roam time. Depending on the WAN characteristics, RF design, back end authentication network, and authentication protocols being used, roam times may vary.
- WPA2—To improve client roam times, WPA2 introduced key caching capabilities, based on the IEEE 802.11i specification. Cisco created an extension to this specification called Proactive Key Caching (PKC). PKC today is supported only by the Microsoft Zero Config Wireless supplicant and the Funk (Juniper) Odyssey client. Cisco CCKM is also compatible with WPA2.

  Remote branch locations requiring predictable, fast roaming behavior in support of applications such as wireless IP telephony should consider deploying a local WLC (Virtual Controller on UCS blade or 2500 WLC).

- Cisco Centralized Key Management (CCKM)—CCKM is a Cisco-developed protocol in which the WLC caches the security credentials of CCKM-capable clients and forwards those credentials to other APs within a mobility group. When a client roams and associates with another AP, their credentials are forwarded to that AP, which allows the client to re-associate and authenticate in a two-step process. This eliminates the need for full authentication back to the AAA server. CCKM-capable clients undergo full 802.1x authentication each time they roam from one FlexConnect to another.
- FlexConnect Groups are required for CCKM/OKC fast roaming to work with FlexConnect access points. Fast roaming is achieved by caching a derivative of the master key from a full EAP authentication so that a simple and secure key exchange can occur when a wireless client roams to a different access point. This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one access point to another. The FlexConnect access points need to obtain the CCKM/OKC cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller. If, for example, you have a controller with 300 access points and 100 clients that might associate, sending the CCKM/OKC cache for all 100 clients is not practical. If you create a FlexConnect Group comprising a limited number of access points (for example, you create a group for four access points in a remote office), the clients roam only among those four access points, and the CCKM/OKC cache is distributed among those four access points only when the clients associate to one of them.
- Layer 2 switch CAM table updates—When a client roams from one AP to another on a locally-switched WLAN, FlexConnect does not announce to a Layer 2 switch that the client has changed ports. The switch will not discover that the client has roamed until the client performs an ARP request for its default router. This behavior, while subtle, can have an impact on roaming performance.

Note A client that roams (for a given local switched WLAN) between FlexConnect APs that map the WLAN to a different VLAN/subnet will renew their IP addresses to ensure that they have an appropriate address for the network to which they have roamed.

Radio Resource Management

While in connected mode, all radio resource management (RRM) functionality is fundamentally available. However, because typical FlexConnect deployments comprise a smaller number of APs, RRM functionality might not be operational at a branch location. For example, in order for transmit power control (TPC) to work, there must be a minimum of four FlexConnect APs in proximity to each other. Without TPC, other features such as coverage hole protection will be unavailable.

Location Services

FlexConnect deployments typically consist of only a handful of APs at a given location. Cisco maintains strict guidelines regarding the number and placement of APs to achieve the highest level of location accuracy. As such, although it is possible to obtain location information from FlexConnect deployments, the level of accuracy may vary greatly across remote location deployments.

QoS Considerations

For WLANs that are centrally-switched, the FlexConnect AP handles QoS in the same way as standard APs. Locally-switched WLANs implement QoS differently.

For locally-switched WLANs with Wi-Fi MultiMedia (WMM) traffic, the AP marks the dot1p value within the dot1q VLAN tag for upstream traffic. This happens only for tagged VLANs, not the native VLAN.

For downstream traffic, FlexConnect uses the incoming dot1p tag from the locally-switched Ethernet and uses this to queue and mark the WMM values associated with frames destined to a given user across the RF link.

The WLAN QoS profile is applied both for upstream and downstream packets. For downstream, if an 802.1p value that is higher than the default WLAN value is received, the default WLAN value is used. For upstream, if the client sends a WMM value that is higher than the default WLAN value, the default WLAN value is used. For non-WMM traffic, there is no CoS marking on the client frames from the AP.

For more information see Chapter 5, "Cisco Unified Wireless QoS and AVC."

Note Cisco strongly recommends that appropriate queuing/policing mechanisms be implemented across the WAN to ensure proper handling of traffic based on its DSCP setting. An appropriate priority queue should be reserved for CAPWAP control traffic to ensure that a FlexConnect AP does not inadvertently cycle between connected and standalone modes because of congestion.

FlexConnect Solution

The FlexConnect solution enables you to:

- Centralize control and management traffic.
- Distribute the client data traffic at each Branch Office.
- Ensure traffic flow is going to its final destination in the most efficient manner.

Advantages of Centralizing Access Point Control Traffic

The advantages of centralizing AP control traffic are:

- Single pane of monitoring and troubleshooting
- Ease of management
- Secured and seamless mobile access to Data Center resources
- Reduction in branch footprint
- Increase in operational savings

Advantages of Distributing Client Data Traffic

The advantages of distributing client data traffic are:

- No operational downtime (survivability) against complete WAN link failures or controller unavailability.

- Mobility resiliency within branch during WAN link failures.
- Increase in branch scalability. Supports branch size that can scale up to 100 APs and 250,000 square feet (5000 square feet per AP).

Central Client Data Traffic

The Cisco FlexConnect solution also supports Central Client Data Traffic, but it should be limited to Guest data traffic only. Table 7-1 and Table 7-2 outline the restrictions on WLAN security types only for non-guest clients whose data traffic is also switched centrally at the Data Center.

Table 7-1 Layer 2 Security Support for Centrally-Switched Non-Guest Users

WLAN Layer 2 Security	Type	Results
None	N/A	Allowed
WPA + WPA2	802.1x	Allowed
	CCKM	Allowed
	802.1x + CCKM	Allowed
	PSK	Allowed
802.1x	WEP	Allowed
Static WEP	WEP	Allowed
WEP + 802.1x	WEP	Allowed
CKIP	—	Allowed

Note These authentication restrictions do not apply to clients whose data traffic is distributed at the branch.

Table 7-2 Layer 3 Security Support for Centrally and Locally Switched Users

WLAN Layer 3 Security	Type	Results
Web Authentication	Internal	Allowed
	External	Allowed
	Customized	Allowed
Web Pass-Through	Internal	Allowed
	External	Allowed
	Customized	Allowed
Conditional Web Redirect	External	Allowed
Splash Page Redirect	External	Allowed

Primary Design Requirements

FlexConnect APs are deployed at the Branch site and managed from the Data Center over a WAN link. It is highly recommended that the minimum bandwidth restriction remains 24 kbps per AP with the round trip latency no greater than 300 ms. (see Table 7-3).

The maximum transmission unit (MTU) must be at least 500 bytes.

Table 7-3 Bandwidth Minimums

Deployment Type	WAN Bandwidth (Min)	WAN RTT Latency (Max)	APs per Branch (Max)	Clients per Branch (Max)
Data	64 kbps	300 ms	5	25
Data	640 kbps	300 ms	50	1000
Data	1.44 Mbps	1 sec	50	1000
Data + Voice	128 kbps	100 ms	5	25
Data + Voice	1.44 Mbps	100 ms	50	1000
Data + Flex AVC	75 Kbps	300 ms	5	25

The primary design requirements are:

- Branch size that can scale up to 100 APs and 250,000 square feet (5000 square feet per AP)
- Central management and troubleshooting
- No operational downtime
- Client-based traffic segmentation
- Seamless and secured wireless connectivity to corporate resources
- PCI compliant
- Support for guests

FlexConnect Groups

Because all of the FlexConnect APs at each branch site are part of a single FlexConnect Group, FlexConnect Groups ease the organization of each branch site.

Note FlexConnect Groups are not analogous to AP Groups.

The FlexConnect Group is primarily designed to solve the following challenges:

- How can wireless clients perform 802.1X authentication and access Data Center services if the controller fails?
- How can wireless clients perform 802.1X authentication if WAN link between Branch and Data Center fails?
- Is there any impact on branch mobility during WAN failures?

- Does the FlexConnect Solution provide no operational branch downtime?

You can configure the controller to allow a FlexConnect AP, in standalone mode, to perform full 802.1X authentication to a backup RADIUS server.

Note Backup RADIUS accounting is not supported.

To increase the resiliency of the branch, administrators can configure a primary backup RADIUS server or both a primary and secondary backup RADIUS server. These servers are used only when the FlexConnect AP is not connected to the controller.

Configuring FlexConnect Groups

Complete the following procedure to configure FlexConnect groups to support Local Authentication using Local Extensible Authentication Protocol (LEAP), when FlexConnect is either in connected or standalone mode.

Step 1 Click **New** under **Wireless > FlexConnect Groups**.

Step 2 Assign **Group Name** as Store 1.

Step 3 Click **Apply** when the Group Name is set.

Step 4 Click the newly created Group Name Store 1.

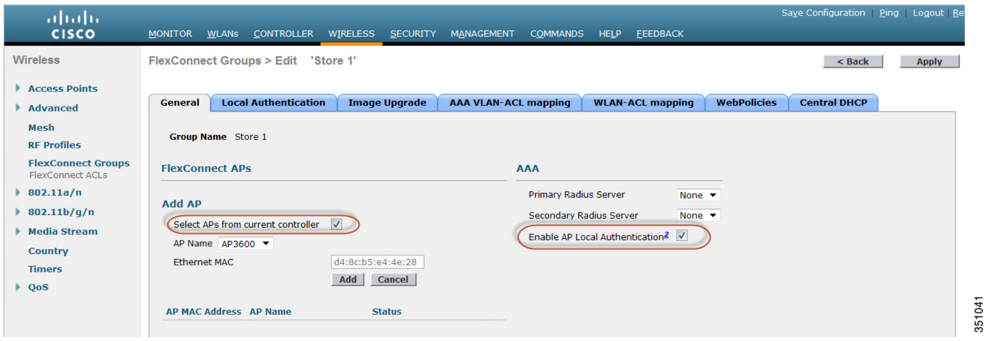
Step 5 Click **Add AP**.

Step 6 Check the **Enable AP Local Authentication** check box to enable Local Authentication when the AP is in standalone mode.

Step 7 Check the **Select APs from current controller** check box to enable the **AP Name** drop-down menu.

Step 8 Choose the AP from the **AP Name** drop-down menu that needs to be part of this FlexConnect Group.

Step 9 Click **Add**.



FlexConnect Groups > Edit 'Store 1'

Group Name Store 1

Select APs from current controller ☑

AP Name AP3600

Ethernet MAC d4:8c:b5:e4:4e:28

Primary Radius Server None

Secondary Radius Server None

Enable AP Local Authentication[2] ☑

Step 10 Repeat Step 7 and Step 8 to add all of the APs to this FlexConnect Group Store 1.

Note Maintaining 1:1 ratio between the AP-Group and FlexConnect group simplifies network management.

Step 11 Navigate to **Local Authentication > Protocols** tabs and then check the **Enable LEAP Authentication** check box.

Step 12 Click **Apply**.

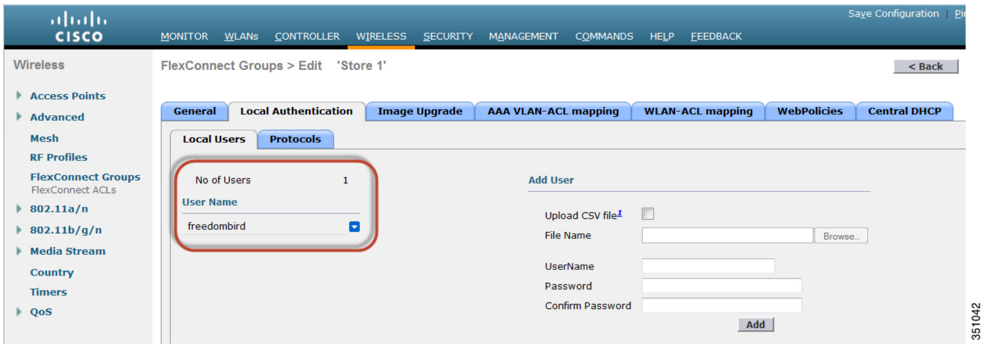
Note If you have a backup controller, make sure the FlexConnect groups are identical and AP MAC address entries are included per FlexConnect group.

Step 13 Navigate to **Local Authentication > Local Users** tabs.

Step 14 Set the **UserName**, **Password** and **Confirm Password** fields, and then click **Add** to create user entry in the LEAP server residing on the AP.

Step 15 Repeat Step 13 until your local username list is exhausted. You cannot configure or add more than 100 users.

Step 16 Click **Apply** after entering all local user information. The user count is verified.



FlexConnect Groups > Edit 'Store 1'

No of Users 1

User Name

freedombird

Upload CSV file[1] ☐

File Name

UserName

Password

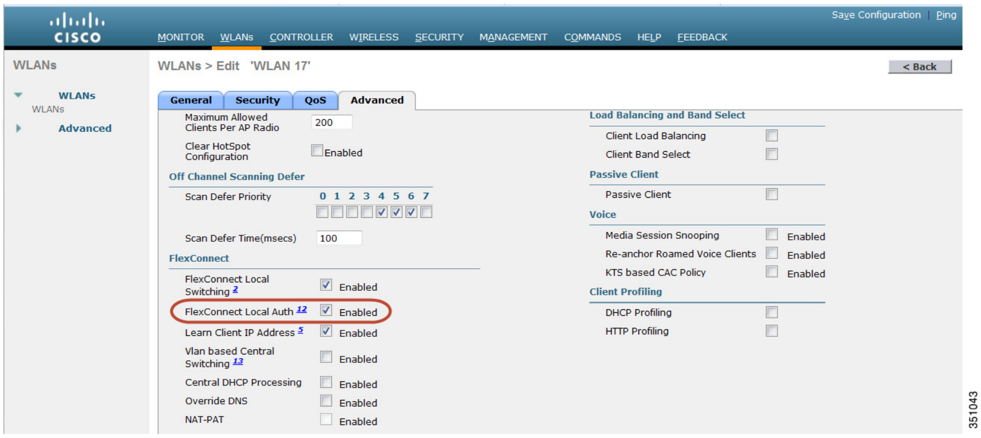
Confirm Password

Step 17 From the top pane, click **WLANs**.

Step 18 Click WLAN ID number that was created during the AP Group creation. In this example, WLAN 17

Step 19 Under **WLAN > Edit for WLAN ID 17**, click **Advanced**.

Step 20 Check the **FlexConnect Local Auth** check box to enable Local Authentication in connected mode.



Save Configuration | Ping
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
General
Security
QoS
Advanced
351043

WLANs > Edit 'WLAN 17'

Maximum Allowed Clients Per AP Radio 200

Clear HotSpot Configuration ☐ Enabled

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7
☐ ☐ ☐ ☐ ☑ ☑ ☑ ☐

Scan Defer Time(msecs) 100

FlexConnect

FlexConnect Local Switching [2] ☑ Enabled

FlexConnect Local Auth [12] ☑ Enabled

Learn Client IP Address [5] ☑ Enabled

Vlan based Central Switching [13] ☐ Enabled

Central DHCP Processing ☐ Enabled

Override DNS ☐ Enabled

NAT-PAT ☐ Enabled

Load Balancing and Band Select

Client Load Balancing ☐

Client Band Select ☐

Passive Client

Passive Client ☐

Voice

Media Session Snooping ☐ Enabled

Re-anchor Roamed Voice Clients ☐ Enabled

KTS based CAC Policy ☐ Enabled

Client Profiling

DHCP Profiling ☐

HTTP Profiling ☐

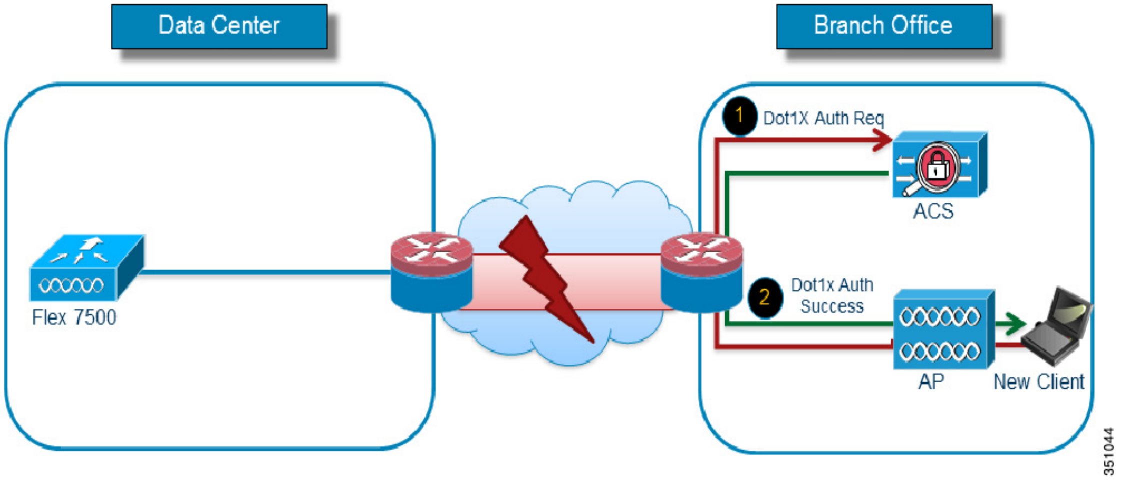
Note Local Authentication is supported only for FlexConnect with Local Switching. Always make sure to create the FlexConnect Group before enabling Local Authentication under WLAN

Local Authentication

Figure 7-8 illustrates clients continuing to perform 802.1X authentication even after the FlexConnect Branch APs lose connectivity with the controller. As long as the RADIUS/ACS server is reachable from the Branch site, wireless clients will continue to authenticate and access wireless services.

In other words, if the RADIUS/ACS is located inside the Branch, then clients will authenticate and access wireless services even during a WAN outage.

Figure 7-8 Local Authentication—AP Authenticator



- Configure Local Backup RADIUS server to increase the resiliency of the branch taking into consideration failures at the WAN, WLC failures, and failures at the RADIUS server.
- This feature is also used for remote offices where the WAN latency to the central site is high.
- Administrators can configure a primary backup RADIUS server or both the primary and secondary backup RADIUS server. FlexConnect AP in standalone mode can be configured to perform full 802.1X authentication to a backup RADIUS server.
- These servers are used when the FlexConnect AP is not connected to the controller or when the WLAN is configured for local authentication.
- If the RADIUS/ACS is located inside the branch, then the clients will authenticate and access wireless services even during a WAN outage.

Note When configuring local backup RADIUS server, note the following limitation: When a local backup RADIUS server is used in the branch, the IP addresses of all the APs acting as authenticators must be added on the RADIUS server.

Note The Local Authentication feature can be used in conjunction with the FlexConnect backup RADIUS server feature. If a FlexConnect Group is configured with both backup RADIUS server and local authentication, the FlexConnect AP always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally, the Local EAP Server on FlexConnect AP itself (if the primary and secondary are not reachable).

Local EAP

You can configure the controller to allow a FlexConnect AP in standalone or connected mode to perform LEAP or EAP-FAST authentication for up to 100 statically configured users. The controller sends the static list of user names and passwords to each FlexConnect AP of that particular FlexConnect Group when it joins the controller. Each AP in the group authenticates its own associated clients.

This feature is ideal for customers who are migrating from a standalone AP network to a lightweight FlexConnect AP network and are *not* interested in maintaining a large user database or adding another hardware device to replace the RADIUS server functionality available in the standalone AP.

Support for PEAP and EAP-TLS Authentication

FlexConnect AP can be configured as a RADIUS server for LEAP and EAP-FAST client authentication. In standalone mode and also when local authentication feature is enabled on the WLANs, FlexConnect AP will do dot1x authentication on the AP itself using the local radius. With controller release 7.5, PEAP and EAP-TLS EAP methods are also supported.

CCKM/OKC Fast Roaming

FlexConnect Groups are required for Cisco's Centralized Key Management (CCKM) and Opportunistic Key Caching (OKC) fast roaming to work with FlexConnect APs. Fast roaming is achieved by caching a derivative of the master key from a full EAP authentication so that a simple and secure key exchange can occur when a wireless client roams to a different AP.

This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one AP to another. The FlexConnect APs need to obtain the CCKM/OKC cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller.

For example, if you have a controller with 300 APs and 100 clients that might associate, sending the CCKM/OKC cache for all 100 clients may not be practical. If you create a FlexConnect Group comprising a limited number of APs (for example, you create a group for four APs in a remote office), the clients will then roam only among those four APs, and the CCKM/OKC cache is distributed among those four APs only when the clients associate to one of them.

This feature along with backup RADIUS and Local Authentication (Local-EAP) ensures no operational downtime for your branch sites.

Use FlexConnect groups in scenarios where CCKM/OKC fast roaming is required for clients when the FlexConnect AP is in connected or standalone mode.

This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one AP to another.

The FlexConnect APs need to obtain the CCKM/OKC cache information for all the clients that might associate so that they can process it quickly instead of sending it back to the controller.

Note CCKM/OKC fast roaming is supported on FlexConnect APs only.

FlexConnect VLAN Override

In the current FlexConnect architecture, there is a strict mapping of WLAN to VLAN, and thus the client getting associated on a particular WLAN on a FlexConnect AP has to abide by a VLAN that is mapped to it. This method has limitations because it requires clients to associate with different SSIDs in order to inherit different VLAN-based policies.

From 7.2 release onwards, AAA override of VLAN on individual WLAN configured for local switching is supported. In order to have a dynamic VLAN assignment, APs would have the interfaces for the VLAN pre-created based on a configuration using existing WLAN-VLAN mapping for individual FlexConnect APs or using ACL-VLAN mapping on a FlexConnect group. The WLC is used to pre-create the sub-interfaces at the AP.

FlexConnect VLAN Override Summary

- AAA VLAN override is supported from release 7.2 for WLANs configured for local switching in central and local authentication mode.
- AAA override should be enabled on WLANs configured for local switching.
- The FlexConnect AP should have VLAN pre-created from WLC for dynamic VLAN assignment.
- If VLANs returned by AAA override are not present on AP clients, they will get an IP from the default VLAN interface of the AP.

FlexConnect VLAN Based Central Switching

From release 7.3 onwards, traffic from FlexConnect APs can be switched centrally or locally depending on the presence of a VLAN on a FlexConnect AP.

In controller software release 7.2, AAA override of VLAN (Dynamic VLAN assignment) for locally-switched WLANs puts wireless clients on the VLAN provided by the AAA server. If the VLAN provided by the AAA server is not present at the AP, the client is put on a WLAN mapped VLAN on that AP and traffic switches locally on that VLAN. Further, prior to release 7.3, traffic for a particular WLAN from FlexConnect APs can be switched Centrally or Locally depending on the WLAN configuration.

FlexConnect VLAN Central Switching Summary

Traffic flow on WLANs configured for Local Switching when FlexConnect APs are in connected mode are as follows:

- If the VLAN is returned as one of the AAA attributes and that VLAN is not present in the FlexConnect AP database, traffic will switch centrally and the client is assigned this VLAN/Interface returned from the AAA server provided that the VLAN exists on the WLC.

- If the VLAN is returned as one of the AAA attributes and that VLAN is not present in the FlexConnect AP database, traffic will switch centrally. If that VLAN is also not present on the WLC, the client will be assigned a VLAN/Interface mapped to a WLAN on the WLC.
- If the VLAN is returned as one of the AAA attributes and that VLAN is present in the FlexConnect AP database, traffic will switch locally.
- If the VLAN is not returned from the AAA server, the client is assigned a WLAN mapped VLAN on that FlexConnect AP and traffic is switched locally.

Traffic flow on WLANs configured for Local Switching when FlexConnect APs are in standalone mode are as follows:

- If the VLAN returned by the AAA server is not present in the FlexConnect AP database, the client will be put on a default VLAN (that is, a WLAN mapped VLAN on a FlexConnect AP). When the AP connects back, this client is de-authenticated and will switch traffic centrally.
- If the VLAN returned by the AAA server is present in the FlexConnect AP database, the client is placed into a returned VLAN and traffic will switch locally.
- If the VLAN is not returned from the AAA server, the client is assigned a WLAN mapped VLAN on that FlexConnect AP and traffic will switch locally.

VLAN Name Override

The VLAN Name Override feature is useful in deployments that have a single central radius authenticating multiple branches. With hundreds of different branches, it becomes very difficult to standardize VLAN IDs across all sites and requires a configuration that provides a unique VLAN Name mapped locally to a VLAN ID that can be different across different branch locations.

This design involving different VLAN IDs across different sites is also useful from the sizing and scaling perspective to limit the number of clients per Layer 2 broadcast domain.

FlexConnect VLAN Name Override Summary

- The VLAN Name Override feature supports both Central and Local Authentication with local switching WLANs.
- If the AAA server returns multiple VLAN attributes, preference is given to the VLAN Name attribute.
- When Aire-Interface-Name and Tunnel-Private-Group-ID are both returned, the Tunnel-Private-Group-ID attribute is given preference.
- If AAA server returns an unknown VLAN name attribute, the client is defaulted to the WLAN-VLAN ID mapping present on the AP.
- This feature is also supported in the standalone mode.

FlexConnect ACL

With the introduction of ACLs on FlexConnect, there is a mechanism to cater to the need of access control at the FlexConnect AP for protection and integrity of locally-switched data traffic from the AP. FlexConnect ACLs are created on the WLC and should then be configured with the VLAN present on the FlexConnect AP or FlexConnect group using VLAN-ACL mapping, which will be for AAA override VLANs. These are then pushed to the AP.

FlexConnect ACL Summary

- Create FlexConnect ACL on the controller.
- Apply the same on a VLAN present on FlexConnect AP under AP Level VLAN ACL mapping.
- Can be applied on a VLAN present in FlexConnect Group under VLAN-ACL mapping (generally done for AAA overridden VLANs.
- While applying ACL on VLAN, select the direction to be applied: *ingress*, *egress*, or *ingress and egress*.

FlexConnect ACL Limitations

- A maximum of 512 FlexConnect ACLs can be configured on WLC.
- Each individual ACL can be configured with 64 rules.
- A maximum of 32 ACLs can be mapped per FlexConnect group or per FlexConnect AP.
- At any given point in time, there is a maximum of 16 VLANs and 32 ACLs on the FlexConnect AP.

Client ACL Support

Prior to release 7.5, FlexConnect ACLs are supported on the VLAN. Also, AAA override of VLANs is supported. If a client gets an AAA override of VLAN, it is placed on the overridden VLAN and the ACL on the VLAN applies for the client. If an ACL is received from the AAA for locally switched clients, it is ignored. With release 7.5, this limitation is addressed and the support for client based ACLs for locally switched WLANs is provided.

FlexConnect Split Tunneling

Split Tunneling introduces a mechanism by which the traffic sent by the client will be classified, based on packet content, using FlexConnect ACL. Matching packets are switched locally from FlexConnect AP and the rest of the packets are centrally-switched over CAPWAP.

The Split Tunneling functionality is an added advantage for OEAP setup where clients on a Corporate SSID can talk to devices on a local network (printers, wired machine on a Remote LAN Port, or wireless devices on a Personal SSID) directly without consuming WAN bandwidth by sending packets over CAPWAP.

FlexConnect ACL can be created with rules in order to permit all of the devices present at the local site/network. When packets from a wireless client on the Corporate SSID match the rules in the FlexConnect ACL configured on OEAP, that traffic is switched locally and the rest of the traffic (that is, implicit deny traffic) will switch centrally over CAPWAP.

The Split Tunneling solution assumes that the subnet/VLAN associated with a client in the central site is not present in the local site (that is, traffic for clients that receive an IP address from the subnet present on the central site will not be able to switch locally).

The Split Tunneling functionality is designed to switch traffic locally for subnets that belong to the local site in order to avoid WAN bandwidth consumption. Traffic that matches the FlexConnect ACL rules are switched locally, and NAT operation is performed changing the client's source IP address to the FlexConnect AP's interface IP address that is route-able at the local site/network.

Split Tunnel Summary

- The Split Tunneling functionality is supported on WLANs configured for central switching advertised by FlexConnect APs only.
- The DHCP required should be enabled on WLANs configured for Split Tunneling.
- The Split Tunneling configuration is applied per WLAN configured for central switching on a per FlexConnect AP basis or for all of the FlexConnect APs in a FlexConnect Group.

Split Tunnel Limitations

- FlexConnect ACL rules should not be configured with permit/deny statement with same subnet as source and destination.
- Traffic on a centrally-switched WLAN configured for Split Tunneling can be switched locally only when a wireless client initiates traffic for a host present on the local site. If traffic is initiated by clients/host on a local site for wireless clients on these configured WLANs, the traffic will not be able to reach the destination.
- Split Tunneling is not supported for Multicast/Broadcast traffic. Multicast/Broadcast traffic will switch centrally even if it matches the FlexConnect ACL.

Fault Tolerance

FlexConnect fault tolerance allows wireless access and services to branch clients when the FlexConnect Branch APs:

- Lose connectivity with the primary controller.
- Are switching to the secondary controller.
- Are re-establishing connection to the primary controller.

FlexConnect fault tolerance, along with the local EAP, provides zero branch downtime during a network outage. This feature is enabled by default and cannot be disabled. It requires no configuration on the controller or AP. However, to ensure fault tolerance works smoothly and is applicable, these criteria should be maintained:

- WLAN ordering and configurations have to be identical across the primary and backup controllers.
- VLAN mapping has to be identical across the primary and backup controllers.

- Mobility domain name has to be identical across the primary and backup controllers.
- Use FlexConnect 7500 as both the primary and backup controllers.

Fault Tolerance Summary

- FlexConnect will not disconnect clients when the AP is connecting back to the same controller provided there is no change in configuration on the controller.
- FlexConnect will not disconnect clients when connecting to the backup controller provided there is no change in configuration and the backup controller is identical to the primary controller.
- FlexConnect will not reset its radios on connecting back to the primary controller provided there is no change in configuration on the controller.

Fault Tolerance Limitations

- Supported only for FlexConnect with Central/Local Authentication with Local Switching.
- Centrally-authenticated clients require full re-authentication if the client session timer expires before the FlexConnect AP switches from standalone to connected mode.
- The primary and backup controllers must be in the same mobility domain.

Peer-to-Peer Blocking

Peer-to-peer (P2P) blocking is supported for clients associated on local switching WLAN. Per WLAN, peer-to-peer configuration is pushed by the controller to the FlexConnect AP. P2P blocking can be configured on a WLAN with any of these three actions:

- Disabled—Disables P2P blocking and bridged traffic locally, within the controller, for clients in the same subnet. This is the default value.
- Drop—This causes the controller to discard packets for clients in the same subnet.
- Forward Up-Stream—This forwards a packet on the upstream VLAN. The devices above the controller decide what action to take regarding the packet.

P2P Summary

- P2P Blocking is configured per WLAN.
- Per WLAN, P2P blocking configuration is pushed by the WLC to FlexConnect APs.
- P2P blocking action configured as drop or upstream-forward on a WLAN is treated as P2P blocking enabled on the FlexConnect AP.

P2P Limitations

- In FlexConnect solution, P2P blocking configuration cannot be applied only to a particular FlexConnect.
- AP or subset of APs. It is applied to all FlexConnect APs that broadcast the SSID.

- Unified solution for central switching clients supports P2P upstream-forward. However, this is not supported in the FlexConnect solution. This is treated as P2P drop, and client packets are dropped instead of forwarded to the next network node.
- Unified solution for central switching clients supports P2P blocking for clients associated to different APs. However, this solution targets only clients connected to the same AP. FlexConnect ACLs can be used as a work around for this limitation.

FlexConnect WGB/uWGB Support for Local Switching WLANs

From release 7.3 onward, Cisco's Work Group Bridge/Universal Work Group Bridge (WGB/uWGB) and wired/wireless clients behind WGBs are supported and will work as normal clients on WLANs configured for local switching.

After association, WGB sends the IAPP messages for each of its wired/wireless clients, and FlexConnect APs behave as follows:

- When a FlexConnect AP is in connected mode, it forwards all the IAPP messages to the controller and the controller will process the IAPP messages the same as of local mode AP. Traffic for wired/wireless clients is switched locally from FlexConnect APs.
- An AP in standalone mode processes the IAPP messages; wired/wireless clients on the WGB must be able to register and de-register. Upon transition to connected mode, FlexConnect AP sends the information of wired clients back to the controller. WGB will send registration messages three times when FlexConnect AP transitions from standalone to connected mode.

  Wired/Wireless clients will inherit the WGB's configuration, which means no separate configuration like AAA authentication, AAA override, and FlexConnect ACL is required for clients behind WGB.

FlexConnect WGB/uWGB Summary

- No special configuration is required on WLC in order to support WGB on FlexConnect AP.
- Fault Tolerance is supported for WGB and the clients behind WGB.
- WGB is supported on an IOS AP: 1240, 1130, 1140, 1260, and 1250.

FlexConnect WGB/uWGB Limitations

- Wired clients behind WGB will always be on the same VLAN as WGN itself. Multiple VLAN support for clients behind WGB is not supported on the FlexConnect AP for WLANs configured for local switching.
- A maximum of 20 clients (wired/wireless) is supported behind WGB when associated to FlexConnect AP on WLAN configured for local switching.
- WebAuth is not supported for clients behind WGB associated on WLANs configured for local switching.

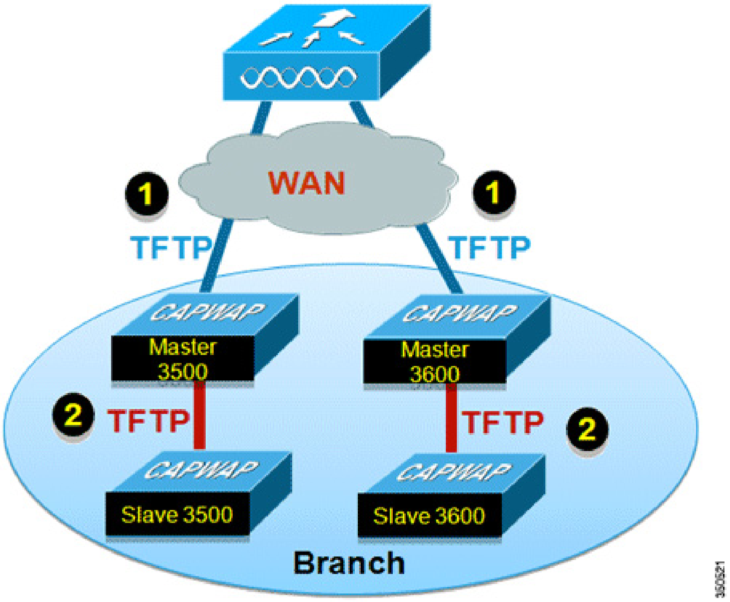
FlexConnect Smart AP Image Upgrade

The pre-image download feature reduces the downtime duration to a certain extent, but still all the FlexConnect APs have to pre-download the respective AP images over the WAN link with higher latency.

Efficient AP Image Upgrade will reduce the downtime for each FlexConnect AP. The basic idea is only one AP of each AP model will download the image from the controller and will act as Master/Server, and the rest of the APs of the same model will work as Slave/Client and will pre-download the AP image from the master.

The distribution of AP image from the server to the client will be on a local network and will not experience the latency of the WAN link. As a result, the process will be faster.

Figure 7-9 Smart AP Image Upgrade



Smart AP Image Upgrade Summary

- Master and Slave APs are selected for each AP model per FlexConnect Group.
- Master downloads image from WLC.
- Slave downloads image from Master AP.
- Reduces downtime and saves WAN bandwidth.

VideoStream for FlexConnect Local Switching

Release 8.0 introduces VideoStream for Local Switching feature, for branch office deployments.

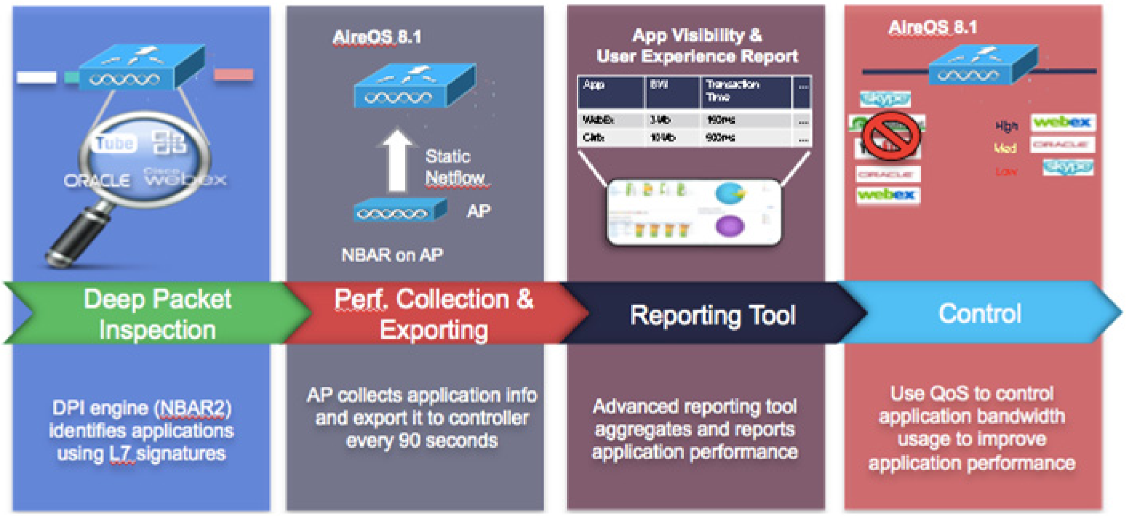
This feature enables the wireless architecture to deploy multicast video streaming across the branches, as it is currently possible for enterprise deployments.

This feature recompenses the drawbacks that degrade the video delivery as the video streams and clients scale in a branch network. VideoStream makes video multicast to wireless clients more reliable and facilitates better usage of wireless bandwidth in the branch.

Application Visibility and Control for FlexConnect

AVC provides application-aware control on a wireless network and enhances manageability and productivity. AVC is already supported on ASR and ISR G2 and WLC platforms. The support of AVC embedded within the FlexConnect AP extends, as this is an end-to-end solution. This gives a complete visibility of applications in the network and allows the administrator to take some action on the application.

Figure 7-10 Application Visibility and Control for FlexConnect


Tube
ORACLE
webex
AireOS 8.1
Static Netflow
AP
NBAR on AP
App Visibility & User Experience Report
App
B/W
Transaction Time
WebEx
Citrix
AireOS 8.1
skype
High
Med
Low
webex
ORACLE
Deep Packet Inspection
Perf. Collection & Exporting
Reporting Tool
Control
DPI engine (NBAR2) identifies applications using L7 signatures
AP collects application info and export it to controller every 90 seconds
Advanced reporting tool aggregates and reports application performance
Use QoS to control application bandwidth usage to improve application performance

- NBAR2 engine runs on the FlexConnect AP.
- Classification of applications happens at the access point using the DPI engine (NBAR2) to identify applications using L7 signatures.
- AP collects application information and exports it to controller every 90 seconds.
- Real-time applications are monitored on the controller user interface.
- Ability to take actions, drop, mark or rate-limit, is possible on any classified application on the FlexConnect access point.

AVC Facts and Limitations

- AVC on the FlexConnect AP can classify and take action on 1000+ different applications.
- The protocol pack running on the FlexConnect APs is different from the one running on the WLC.
- AVC stats on the GUI are displayed for the top 10 applications by default. This can be changed to top 20 or 30 applications as well.
- Intra FlexConnect Group roaming support.

- IPv6 traffic cannot be classified.
- AAA override of AVC profiles is not supported.
- Multicast traffic is not supported by AVC application.
- Netflow export for FlexConnect AVC is not supported in 8.1.

General Deployment Considerations

- Although it is possible for any WLC to support FlexConnect APs, depending on the number of branch locations and subsequently the total number of APs being deployed, it makes sense (from an administrative standpoint) to consider using a dedicated WLC(s) to support a FlexConnect deployment.
- FlexConnect APs typically do not share the same policies as APs within a main campus; each branch location is essentially an RF and mobility domain unto itself. Even though a single WLC cannot be partitioned into multiple logical RF and mobility domains, a dedicated WLC allows branch-specific configuration and policies to be logically separate from the campus.
- If deployed, a dedicated FlexConnect WLC should be configured with a different mobility and RF network name than that of the main campus. All FlexConnect APs joined to the dedicated WLC become members of that RF and mobility domain.
- From an auto-RF standpoint, assuming there are enough FlexConnect APs deployed within a given branch, the WLC attempts to auto manage the RF coverage associated with each branch.
- There is no advantage (or disadvantage) in having the FlexConnect APs consolidated into their own mobility domain. This is because client traffic is switched locally. EoIP mobility tunnels are not invoked between WLCs (of the same mobility domain) where client roaming with FlexConnect APs is involved.
- If a dedicated WLC is going to be used for a FlexConnect deployment, a backup WLC should also be deployed to ensure network availability. As with standard AP deployments, the WLC priority should be set on the FlexConnect APs to force association with the designated WLCs.
- Certain architectural requirements need to be considered when deploying a distributed branch office in terms of the Minimum WAN Bandwidth, Maximum RTT, Minimum MTU, and fragmentation.
- Check to make sure that the AP model being used has FlexConnect support. The AP model OEAP600 does not support FlexConnect mode.
- Set QoS to prioritize CAPWAP Control Channel traffic on UDP port 5246.
- You can deploy a FlexConnect AP with either a static IP address or a DHCP address. A DHCP server must be available locally and must be able to provide the IP address for the AP during boot-up.
- FlexConnect supports up to four fragmented packets or a minimum 500 byte maximum transmission unit (MTU) WAN link.
- Round-trip latency must not exceed 300 milliseconds (ms) between the AP and the controller. If the 300 milliseconds round-trip latency cannot be achieved, configure the AP to perform local authentication.
- FlexConnect includes robust fault tolerance methodology. When the AP and the controller have the same configuration, the connections (rejoin or standby) between the clients and the FlexConnect APs are maintained intact and the clients experience seamless connectivity.

- The primary and secondary controllers for a FlexConnect AP must have the same configuration. Otherwise, the AP might lose its configuration, and certain features (such as WLAN overrides, VLANs, static channel number, and so on) may not operate as expected. In addition, make sure to duplicate the SSID of the FlexConnect AP and its index number on both controllers.
- Client connections are restored only for locally-switched clients that are in the RUN state when the AP moves from standalone mode to connected mode. After the AP moves from the standalone mode to the connected mode, the AP's radio is also reset.
- Session time-out and re-authentication are performed when the AP establishes a connection to the controller.
- If a session timer expires, the client user name, current/support rate, and listen interval values are reset to the default values. When the client connection is re-established, the controller does not restore the client's original attributes.
- Multiple FlexConnect groups can be defined in a single location. There is no deployment restriction on the number of FlexConnect APs per location.
- In FlexConnect mode, the AP can receive multicast packets only in unicast form.
- FlexConnect APs support a 1-1 network address translation (NAT) configuration and a port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the unicast option. FlexConnect APs also support a many-to-one NAT/PAT boundary, except when you want true multicast to operate for all centrally-switched WLANs.

Note Although NAT and PAT are supported for FlexConnect APs, they are not supported on the corresponding controller. Cisco does not support configurations in which the controller is behind a NAT/PAT boundary.

- VPN and PPTP are supported for locally-switched traffic if these security types are accessible locally at the AP.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported on WLANs configured for FlexConnect local switching.
- Workgroup bridges and universal workgroup bridges are supported on FlexConnect APs for locally-switched clients.
- FlexConnect APs do not support client load balancing.
- FlexConnect supports IPv6 clients by bridging the traffic to a local VLAN, similar to IPv4 operation.
- FlexConnect does not support IPv6 ACLs, neighbor discovery caching, or DHCPv6 snooping of IPv6 NDP packets.
- FlexConnect APs with locally-switched WLANs cannot perform IP Source Guard and prevent ARP spoofing. For centrally-switched WLANs, the wireless controller performs the IP Source Guard and ARP Spoofing. To prevent ARP spoofing attacks in FlexConnect APs with local switching, Cisco recommends you to use ARP inspection.

CHAPTER 8

Cisco Wireless Mesh Networking

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

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

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

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

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

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

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

Mesh Access Points

Access Point Roles

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

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

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

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

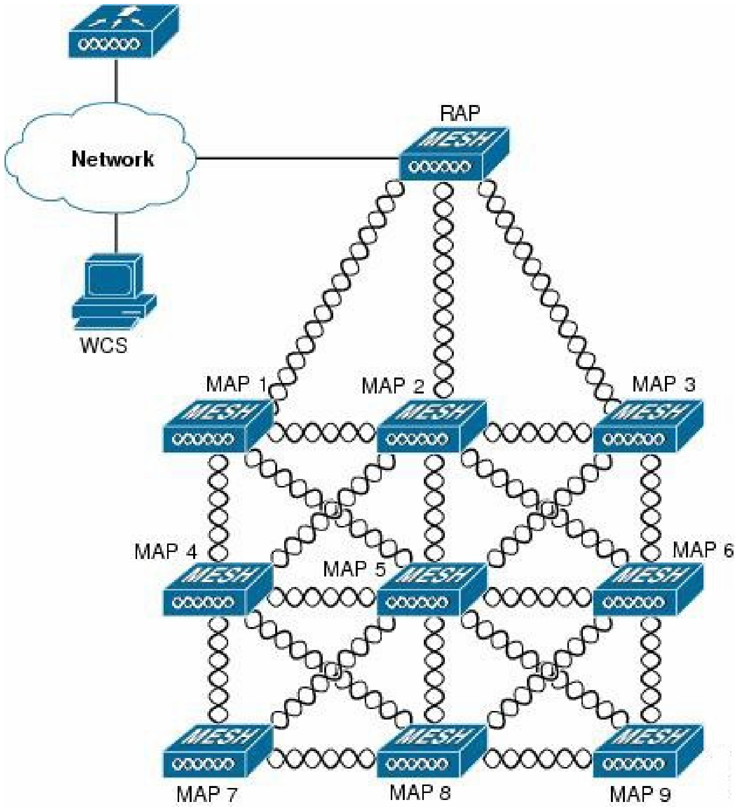
MAPs communicate among themselves and back to the RAP using wireless connections over the 802.11a/n radio backhaul. MAPs use the Cisco Adaptive Wireless Path Protocol (AWPP) to determine the best path through the other mesh access points to the controller.

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

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

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

Figure 8-1 Simple Mesh Network Hierarchy



Network Access

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

- Wireless LAN client traffic
- MAP Ethernet port traffic

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

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

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

Network Segmentation

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

Cisco Indoor Mesh Access Points

Indoor mesh is available on the following access points:

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

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

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

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

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

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

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

- 2.4-GHz radio used for client access
- 5-GHz radio used for data backhaul and client access if Universal Backhaul Access is enabled

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

Cisco Outdoor Mesh Access Points

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

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

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

AP1500s are manufactured in two different configurations:

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

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

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

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

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

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

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

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

Cisco Aironet 1570 Series Access Points

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

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

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

AP1572IC

The AP1572IC has the following features:

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

AP1572EC

The AP1572EC has the following features:

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

AP1572EAC

The AP1572EAC has the following features:

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

Note For more information, see Aironet 1572 Deployment Guide

Cisco Aironet 1530 Series Access Points

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

The following are the main features:

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

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

AP1532I

The AP1532I has the following features:

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

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

AP1532E

The AP1532E has the following features:

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

Note For more information, see the 1532 Deployment Guide.

Cisco Aironet 1552 Mesh Access Point

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

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

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

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

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

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

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

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

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

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

The 1550 series access points have the following features:

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

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

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

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

For more information, see Cisco 1550 Series Access Points.

1552E

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

The 1552E model has the following features:

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

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

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

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

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

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

1552C

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

The 1552C model has the following features:

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

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

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

1552I

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

The 1552I model has the following features:

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

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

1552H

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

The 1552H model has the following features:

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

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

1552CU

The 1552CU model has the following features:

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

1552EU

The 1552EU model has the following features:

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

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

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

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

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

Ethernet Ports

AP1500s support four Gigabit Ethernet interfaces.

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

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

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

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

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

Multiple Power Options

For the 1550 Series

Power options include the following:

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

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

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

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

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

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

Table 8-1 Power Options in 1552 Models

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

Battery Backup Module (Optional)

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

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

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

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

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

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

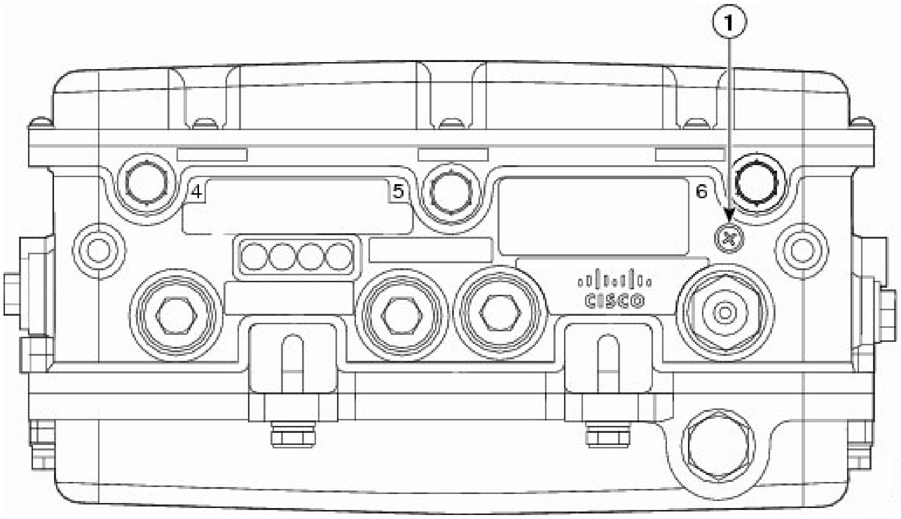
1550 Reset Button

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

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

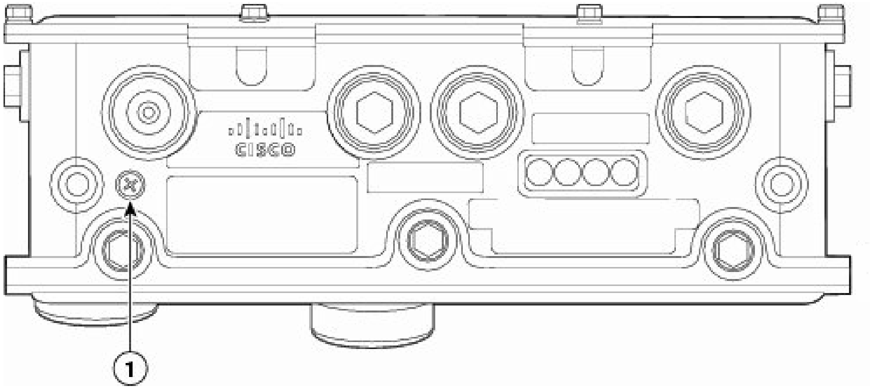
    ```
    config mesh battery-state disable AP_name
    ```
- Switch off LEDs—Press the reset button for more than 10 seconds, and the LEDs turn off, then on, and then stay off.

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



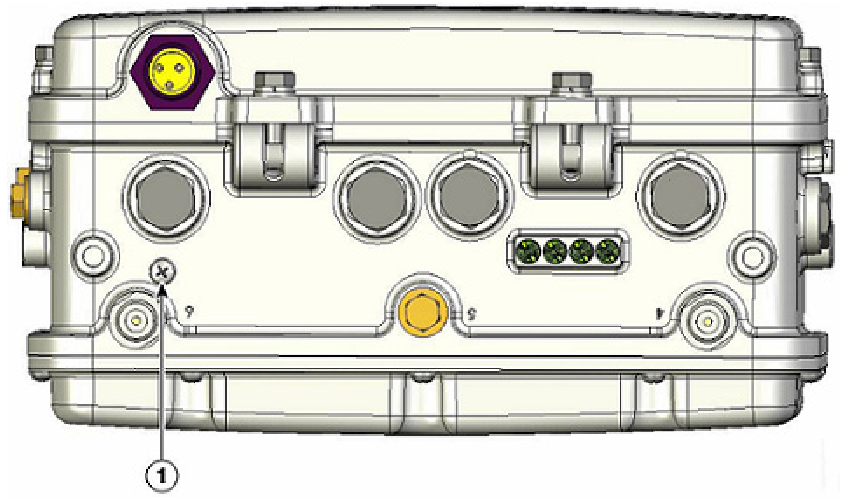
1	Reset Button

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



1	Reset Button

Figure 8-4 Reset Button Location for 1520 Series



1	Reset Button

Resetting 1550 Access Point

To reset the access point, follow these steps:

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

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

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

Monitoring the 1550s LED Status

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

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

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

There are four LED status indicators on AP1550s.

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

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

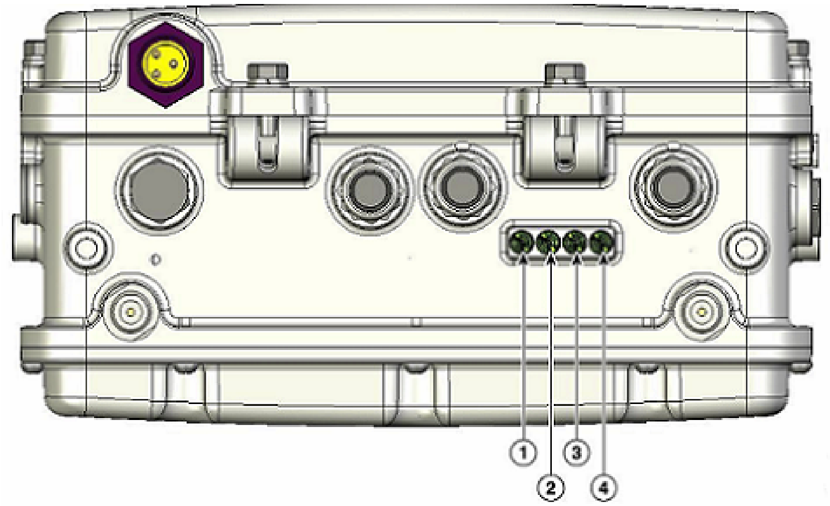


Table 8-2 below describes each LED and its status.

Table 8-2 LED and its Status

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

[1] Slot 3 is disabled.

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

Table 8-3 lists the Access Point LED signals.

Table 8-3 Access Point LED Signals

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

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

1570

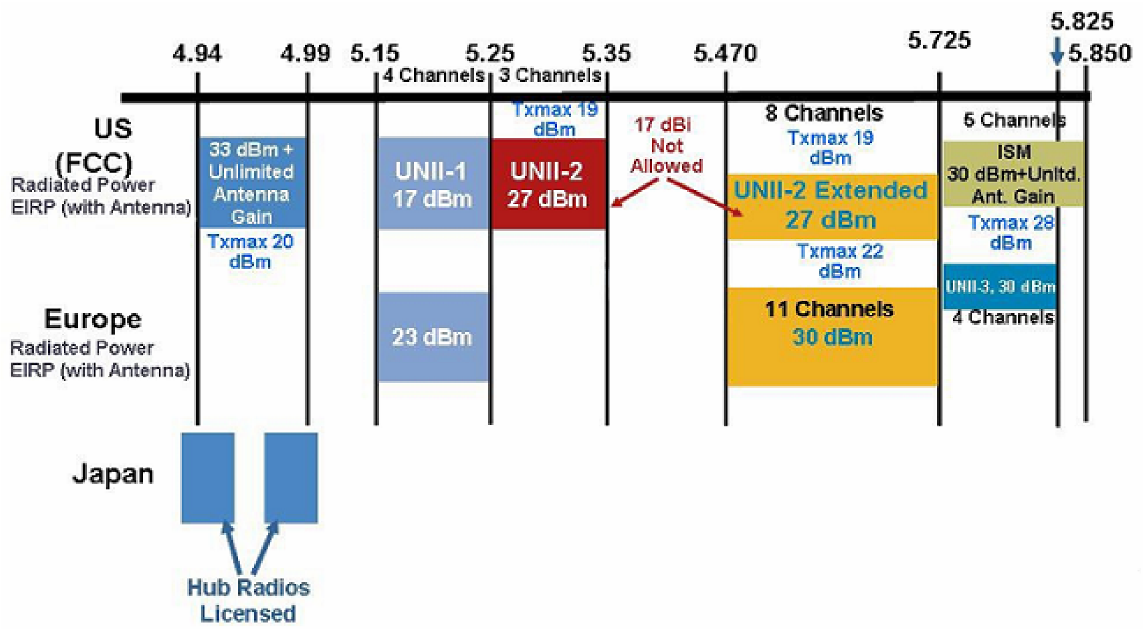
For more information, please refer the following guides:

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

Frequency Bands

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

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



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

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

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

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

Table 8-4 lists the frequency band.

Table 8-4 Frequency Band

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

[1] UNII refers to the Unlicensed National Information Infrastructure.

[2] ISM refers to Industrial, Scientific and Medical.

Note For regulatory information, see Wireless LAN Compliance Status.

Dynamic Frequency Selection

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

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

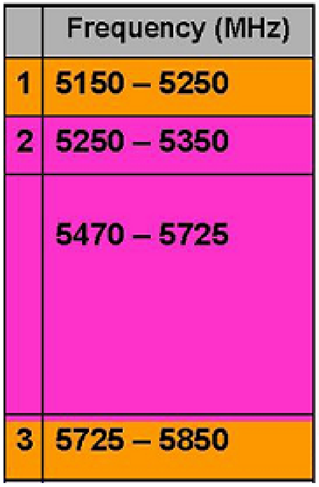
The AP performs a DFS scan on the new DFS channel for 60 seconds. However, if a neighboring AP is already using that new DFS channel, the AP does not perform the DFS scan.

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

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

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

Figure 8-7 DFS and TPC Band Requirements



	Frequency (MHz)
1	5150 – 5250
2	5250 – 5350
	5470 – 5725
3	5725 – 5850

Antennas

Overview

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

- Directional
- Omni-directional

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

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

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

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

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

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

Antenna Options

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

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

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

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

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

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

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

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

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

Table 8-6 Horizontal and Vertical Beamwidth for Cisco Antennas

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

N-Connectors

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

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

Antenna Configurations for 1552

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

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

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

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

Figure 8-8 1552C Cable Mount

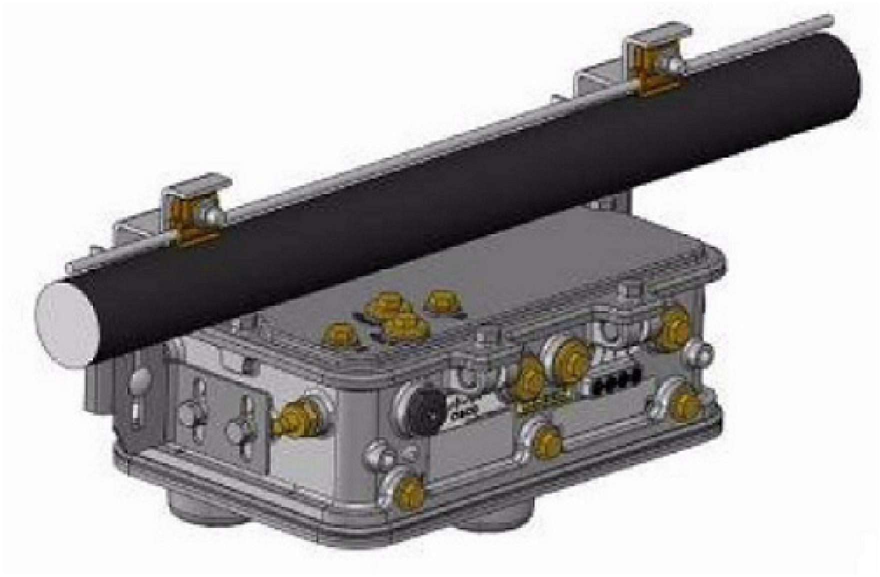
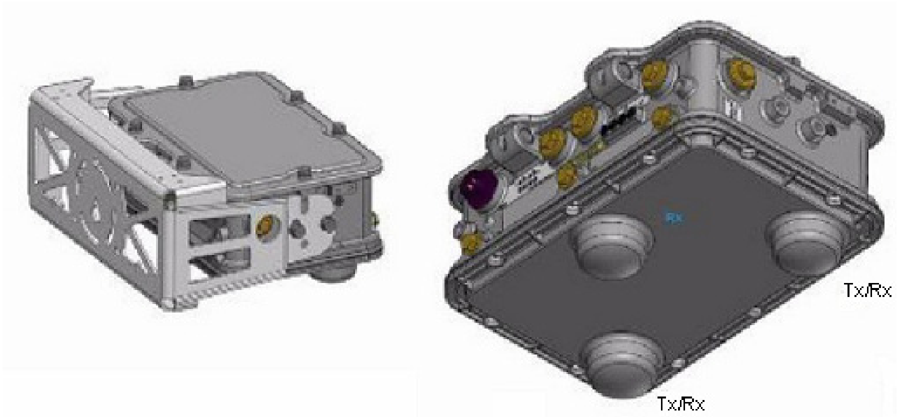


Figure 8-9 1552I Pole/Wall Mount



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

Figure 8-10 1552 E Pole/Wall Mount

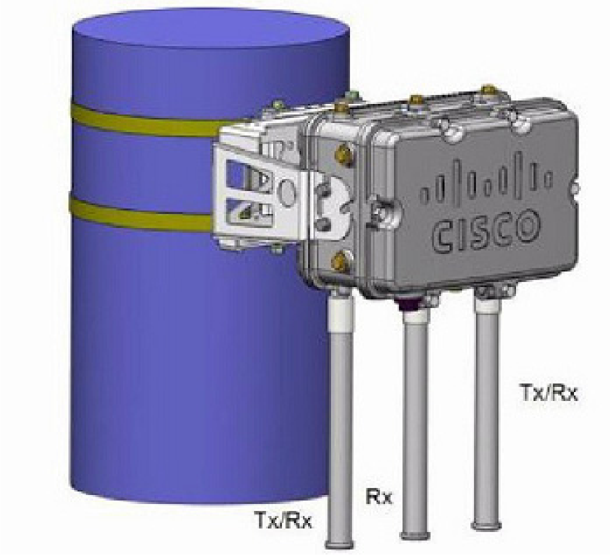
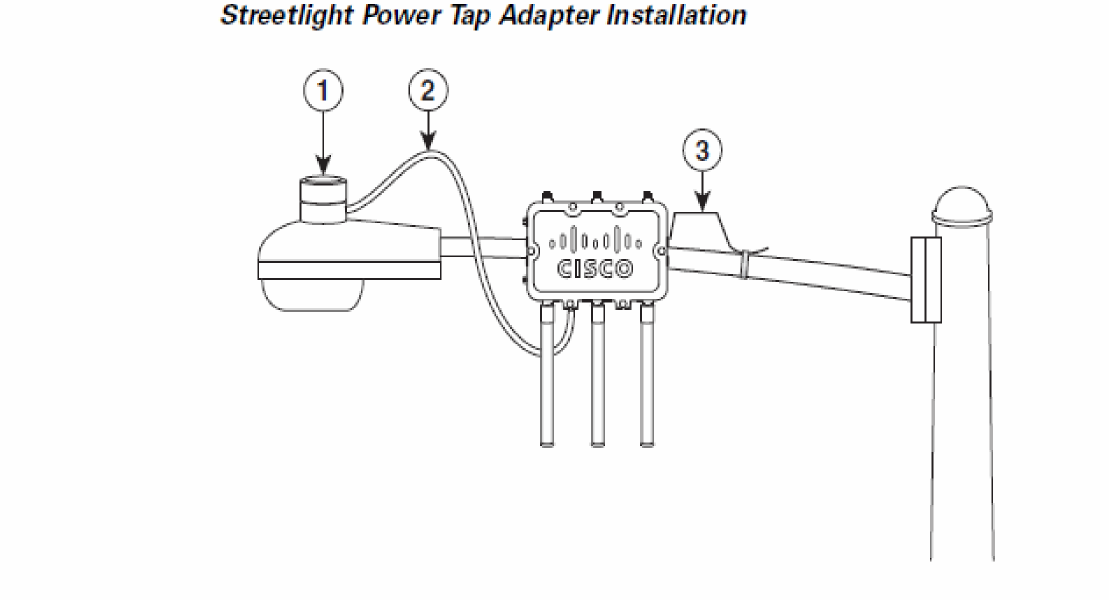


Figure 8-11 shows one of the recommended installations of an outdoor AP1500.

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



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

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

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

Client Access Certified Antennas (Third-Party Antennas)

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

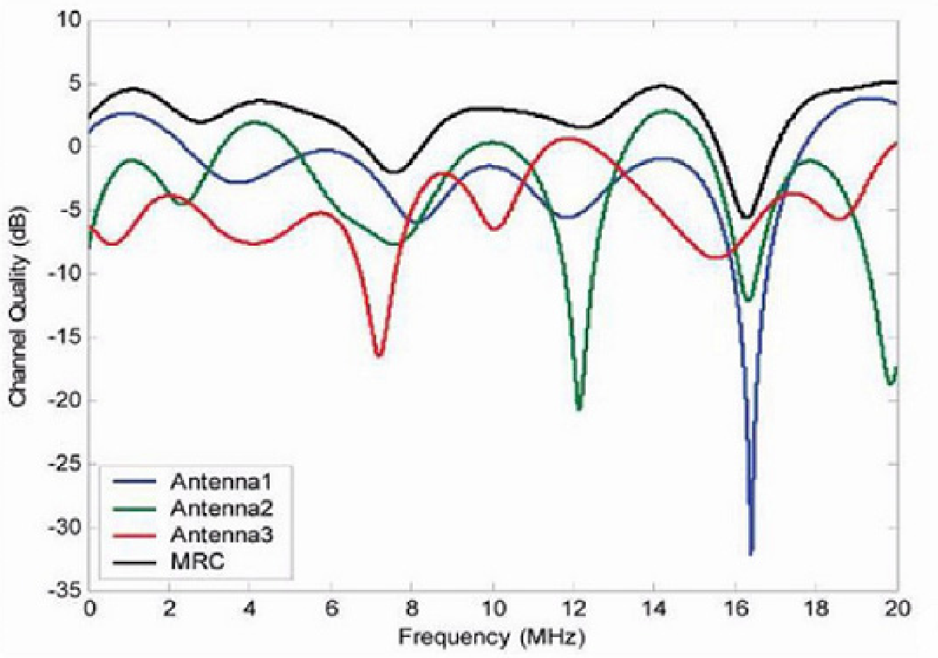
- Cisco does not track or maintain information about the quality, performance, or reliability of the non-certified antennas and cables.
- RF connectivity and compliance is the customer's responsibility.
- Compliance is only guaranteed with Cisco antennas or antennas that are of the same design and gain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

Maximum Ratio Combining

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

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

Figure 8-12 Reinforcement of Received Signal via MRC Algorithm



For the 1550 Series

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

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

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

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

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

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

Table 8-7 AP1552 11a/g MRC Gain

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

Table 8-8 AP1552 11n MRC Gain

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

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

Cisco 1500 Hazardous Location Certification

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

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

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

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

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

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

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

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

Table 8-9 TerraWave Enclosures

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

For more information, see Terrawave Enclosures.

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

Table 8-10 Hardware Features at a Glance

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

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

Cisco Wireless LAN Controllers

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

Cisco Prime Infrastructure

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

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

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

Architecture

Control and Provisioning of Wireless Access Points

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

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

CAPWAP Discovery on a Mesh Network

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

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

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

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

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

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

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

Dynamic MTU Detection

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

XML Configuration File

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

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

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

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

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

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

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

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

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

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

```
show invalid-config
```

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

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

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

Adaptive Wireless Path Protocol

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

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

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

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

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

Traffic Flow

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

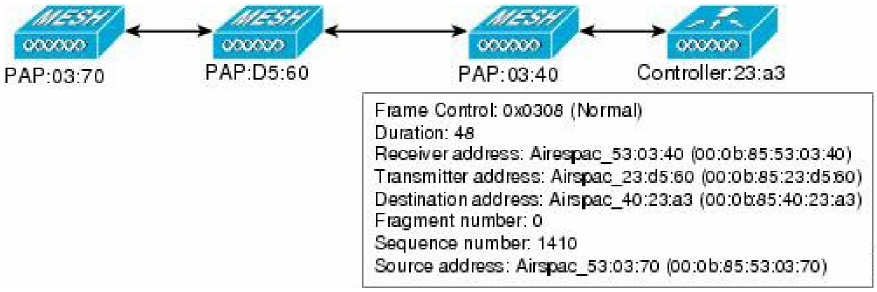
- Overlay CAPWAP traffic that flows within a standard CAPWAP access point deployment; that is, CAPWAP traffic between the CAPWAP access point and the CAPWAP controller.
- Wireless mesh data frame flow.
- AWPP exchanges.

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

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

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

Figure 8-13 Wireless Mesh Frame



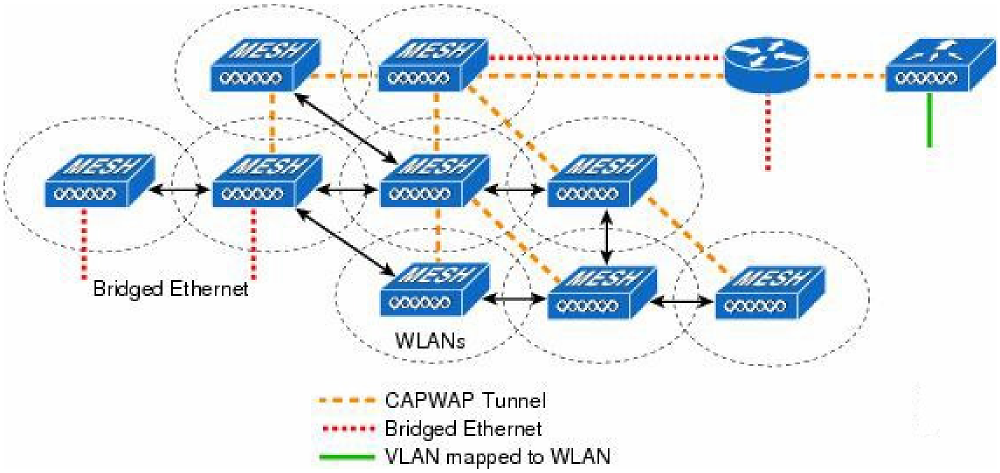
Frame Control: 0x0308 (Normal)
Duration: 48
Receiver address: Airespac_53:03:40 (00:0b:85:53:03:40)
Transmitter address: Airspac_23:d5:60 (00:0b:85:23:d5:60)
Destination address: Airspac_40:23:a3 (00:0b:85:40:23:a3)
Fragment number: 0
Sequence number: 1410
Source address: Airspac_53:03:70 (00:0b:85:53:03:70)

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

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

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

Figure 8-14 Logical Bridge and WLAN Mapping

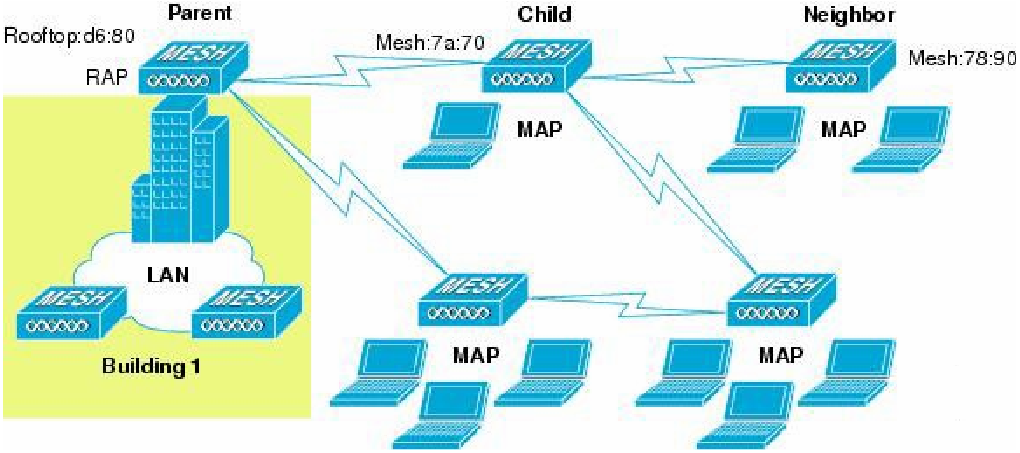


Mesh Neighbors, Parents, and Children

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

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

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



Criteria to Choose the Best Parent

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

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

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

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

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

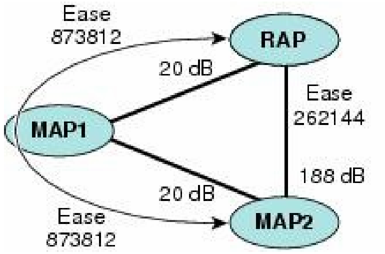
A parent mesh access point provides the best path back to a RAP. AWPP uses Ease to determine the best path. Ease can be considered the opposite of cost, and the preferred path is the path with the higher ease.

Ease Calculation

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

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

Figure 8-16 Parent Path Selection



Parent Decision

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

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

SNR Smoothing

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

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

Loop Prevention

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

Mesh Deployment Modes

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

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

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

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

Wireless Backhaul

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

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

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

Universal Access

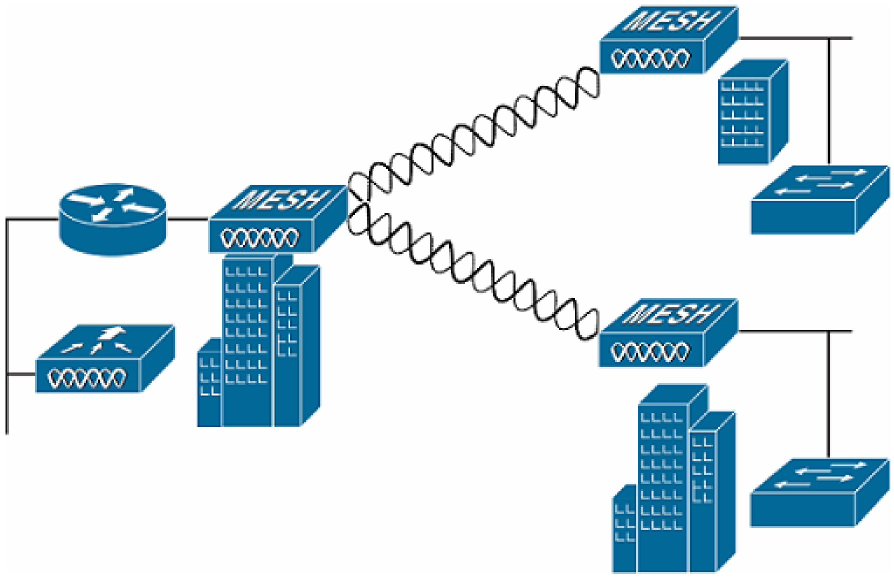
You can configure the backhaul on mesh APs to accept client traffic over its 802.11a radio. This feature is identified as Backhaul Client Access in the controller GUI (**Monitor > Wireless**). When this feature is disabled, backhaul traffic is transmitted only over the 802.11a or 802.11a/n radio and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

Point-to-Multipoint Wireless Bridging

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

Figure 8-17 shows a simple deployment with one RAP and two MAPs, but this configuration is fundamentally a wireless mesh with no WLAN clients. Client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access.

Figure 8-17 Point-to-Multipoint Bridging Example



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

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

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

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

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

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

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

Wireless Backhaul Data Rate

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

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

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

A lower bit rate might allow a greater distance between MAPs, but there are likely to be gaps in the WLAN client coverage, and the capacity of the backhaul network is reduced. An increased bit rate for the backhaul network either requires more MAPs or results in a reduced SNR between MAPs, limiting mesh reliability and interconnection.

ClientLink Technology

Many networks still support a mix of 802.11a/g and 802.11n clients. Because 802.11a/g clients (legacy clients) operate at lower data rates, the older clients can reduce the capacity of the entire network.

Cisco ClientLink technology can help to solve problems related to adoption of 802.11n in mixed-client networks by ensuring that 802.11a/g clients operate at the best possible rates, especially when they are near cell boundaries.

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

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

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

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

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

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

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

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

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

Controller Planning

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

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

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

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

Table 8-11 Mesh AP Support by Controller Model

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

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

[2] For 5508, controllers, the number of MAPs is equal to (local AP support - number of RAPs).

[3] For 2504, controllers, the number of MAPs is equal to (local AP support - number of RAPs).

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

Wireless Mesh Network Coverage Considerations

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

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

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

Cell Planning and Distance

For the Cisco 1520 Series Access Points

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

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

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

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

Collocating Mesh Access Points

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

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

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

Collocating AP1500s on Adjacent Channels

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

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

Collocating AP1500s on Alternate Adjacent Channels

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

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

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

CleanAir

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

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

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

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

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

CleanAir Advisor

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

Wireless Mesh Mobility Groups

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

Multiple Controllers

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

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

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

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

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

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

Increasing Mesh Availability

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

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

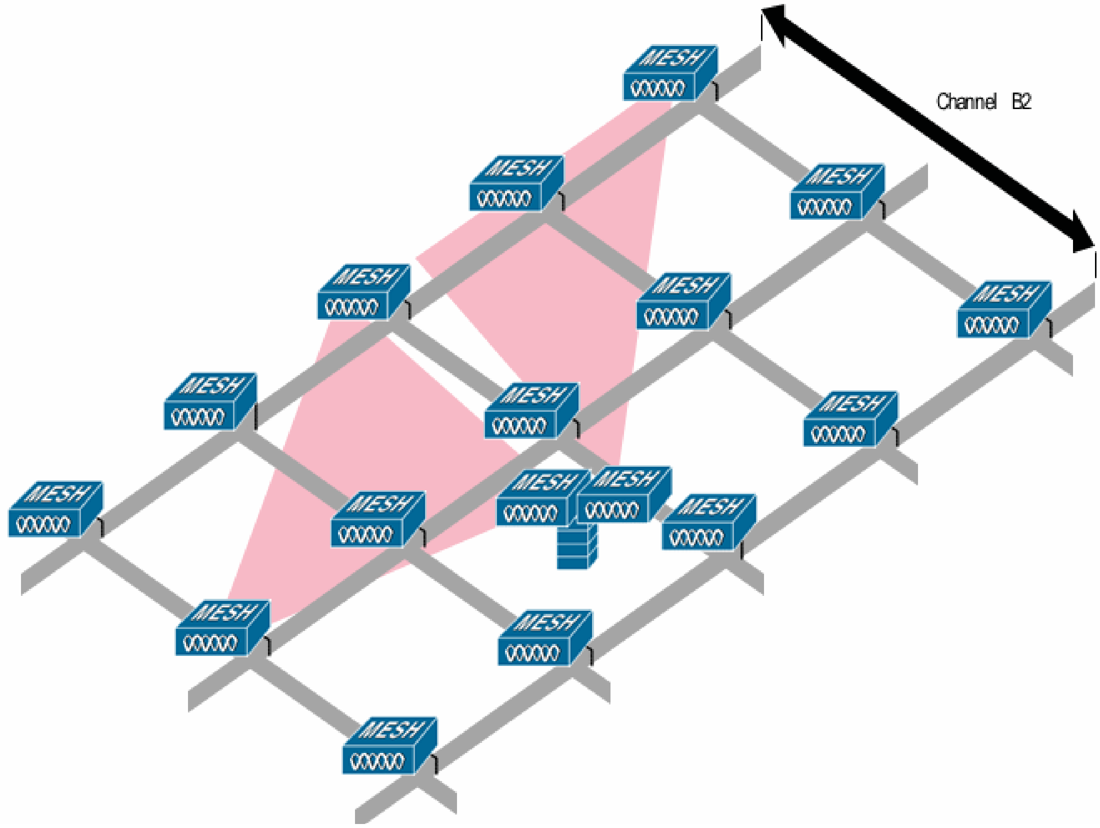
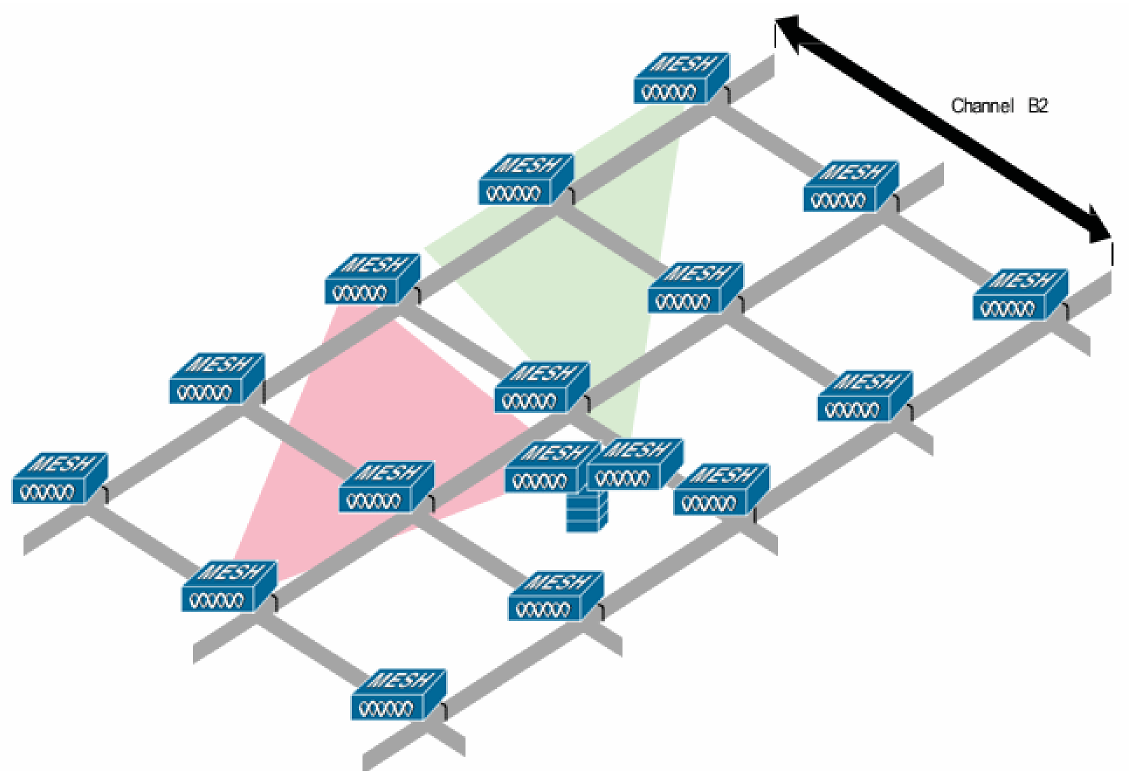


Figure 8-19 Two RAPs per Cell on Different Channels



Multiple RAPs

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

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

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

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

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

Indoor Mesh Interoperability with Outdoor Mesh

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

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

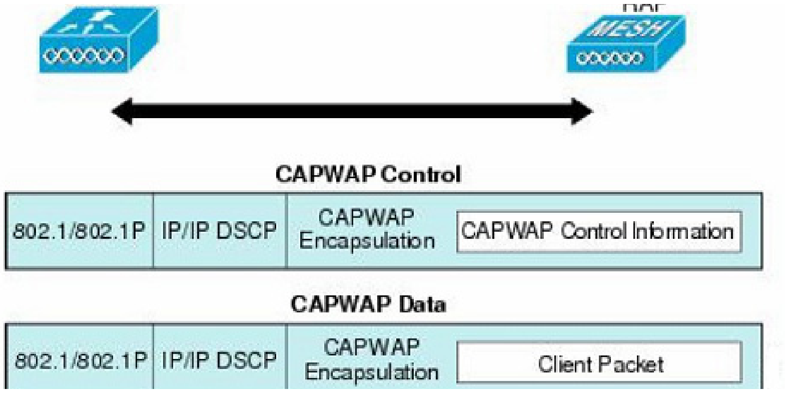
Mobility groups can be shared between outdoor mesh networks and indoor WLAN networks. It is also possible for a single controller to control indoor and outdoor mesh APs simultaneously. The same WLANs are broadcast out of both indoor and outdoor mesh APs.

Connecting the Cisco 1500 Series Mesh APs to the Network

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

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

Figure 8-20 Mesh Network Traffic Termination



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

Adding Mesh APs to the Mesh Network

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

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

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

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

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

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

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

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

Step 6 Configure global mesh parameters.

Step 7 Configure universal client access.

Step 8 Configure local mesh parameters.

Step 9 Configure antenna parameters.

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

Step 11 Configure the DCA channels for the mesh APs.

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

Step 13 Configure Ethernet bridging (if desired).

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

CHAPTER 9

VoWLAN Design Recommendations

This chapter provides additional design considerations for deploying voice over WLAN (VoWLAN) solutions. WLAN configuration specifics can vary depending on the VoWLAN device being used and the WLAN design. This chapter provides details about key RF and site survey considerations that are generally applicable to VoWLAN deployments, which were introduced in .Chapter 3, “WLAN RF Design Considerations”

Softphone applications are key VoWLAN solutions and they are available on a number of hardware and operating systems platforms. The Cisco JabberTM, application lets you access presence, instant messaging (IM), audio, video, voice messaging, desktop sharing, and conferencing. Jabber downloads for smartphones, tablets, and laptops along with information on design guides for each of the variants can be referred at Cisco Jabber.

Antenna Considerations

The more demanding network requirements of VoWLAN impacts WLAN planning at all levels, including the choice of antenna. Key antenna considerations are as follows:

- Access point (AP) antenna selection
- Antenna placement
- Handset antenna characteristics

AP Antenna Selection

Cisco recommends a ceiling-mounted antenna solution for VoWLAN applications. Ceiling mounted antennas and APs with internal antennas are quick and easy to install. More importantly, they place the radiating portion of the antenna in open space, which allows the most efficient signal propagation and reception. Cisco APs with internal antennas offer the easiest installation solution, plus the internal antennas provide a downward signal propagation pattern that is well suited for the majority of installations. The internal antenna solution is particularly well suited to the open spaces of enterprise environments.

Cisco offers a variety of multiple-input and multiple-output (MIMO) dual band, dual radiating element Omni-directional and Directional (patch style) antennas. These multiple element antennas are designed to take advantage of IEEE 802.11n and .11ac technologies such as Maximum Ratio Combining (MRC) and unique Cisco performance features such as ClientLink. These technologies combine client phone packets, (as they are captured on the multiple antennas of the APs) into a single, combined signal that is stronger. The combined signal provides a better signal-to-noise ratio (SNR) between the phone's transmitted packet and the general 2.4 or 5 GHz band noise. An important feature of MRC is that it reduces the upstream packet error rate. Cisco APs use the multiple antennas and 802.11 ClientLink logic to deliver a higher energy packet to the client phone, which reduces the downstream packet error rate. These two features improve the mean opinion score (MOS) value of individual VoWLAN calls and the overall capacity of the Wi-Fi channel of the APs.

Cisco recommends that all antennas be placed 1 to 2 wavelengths away from highly reflective surfaces such as metal. The length of the 2.4 GHz waves is 4.92 inches (12.5 cm), and the length of the 5 GHz waves is 2.36 inches (6 cm). The separation of one or more wavelengths between the antenna and reflective surfaces allows the AP radio a better opportunity to receive a transmission and reduces the creation of nulls when the radio transmits. Orthogonal frequency-division multiplexing (OFDM), used by the 802.11g/n and 802.11a/n/ac specifications, helps to mitigate problems with reflections, nulls, and multipath. However, good antenna placement and the use of the appropriate antenna types provide a superior solution. The ceiling tile itself is a good absorber of signals transmitted into the area above the ceiling and reflected back into the coverage area.

For information on MRC, see the IEEE Report.

For more information on ClientLink, refer the following:

- Cisco Wireless ClientLink 3.0 Technology
- Cisco Aironet 3700 Series White Paper

Antennas come in a variety of types and form factors; no single type is best for all applications and locations. For additional information on the performance and part numbers of various antenna types, see the Cisco Aironet Antennas and Accessories Reference Guide.

Cisco recommends using the Cisco Aironet dipole dual band AIR-ANT2524D series antenna when attaching dipole antennas to an AP with dual (2.4 GHz and 5 GHz) band support from the same external antenna port.

The Aironet dipole dual band antennas provide the advantages of:

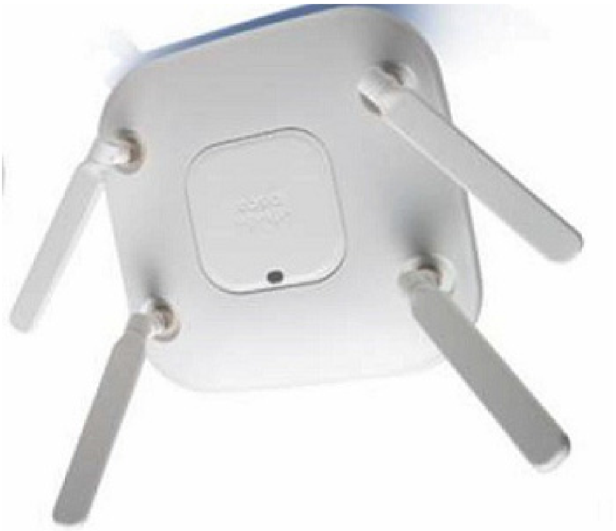
- Support for simultaneous 2.4 and 5 GHz dual band transmission and reception (the same as the dual band omni and patch antennas). The gain on the Aironet dipole dual band antennas is 2.2 dBi for the 2.4 GHz band and 4 dBi for the 5 GHz band.
- Being small and coming in neutral colors of black, grey and white.
- Having an articulating and rotating base.

Antenna Orientation

Cisco recommends that, **for APs with multiple antennas, all the antennas be oriented in the same direction**.

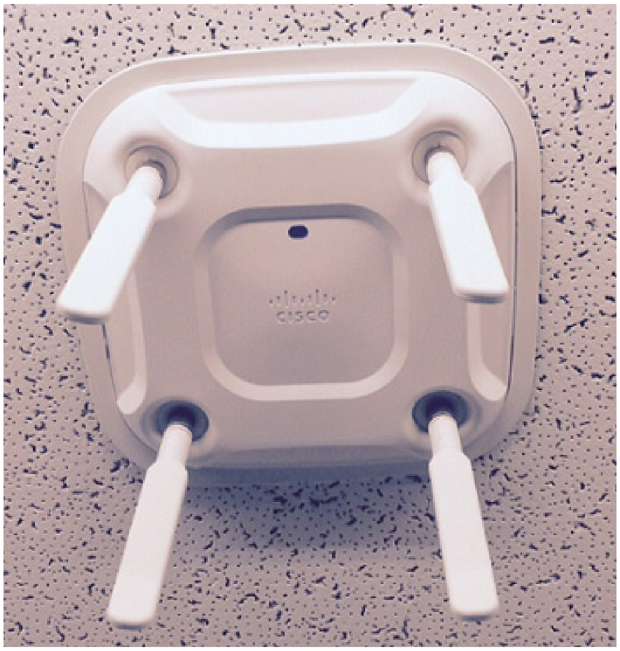
Note While APs are often depicted in marketing material showing the antennas arranged in multiple directions, as shown in Figure 9-1, Cisco does not recommended this practice.

Figure 9-1 AP With Antennas Arranged (incorrectly) in Different Directions



The best MRC and ClientLink performance is obtained when all antennas of an AP are arranged in the same orientation, as shown in Figure 9-2.

Figure 9-2 AP With Antennas Arranged (correctly) in Same Orientation



Having all four antennas of the AP in a flat, straight out position increases the overall throughput of the coverage cell by 2 Mbps when using single spatial stream 802.11n smartphones.

General Recommendations

Cisco recommends for optimum Wi-Fi coverage cell bandwidth and client application performance (for dipole antenna types of all forms) that:

- Each AP antenna port be populated with an antenna.
- Each port must have the same antenna model.
- Each antenna has the same orientation.

The APs and the protocols they operate with are designed around MRC and ClientLink. Use an antenna system that follows these recommendations to capitalize on that technology and your AP hardware investment.

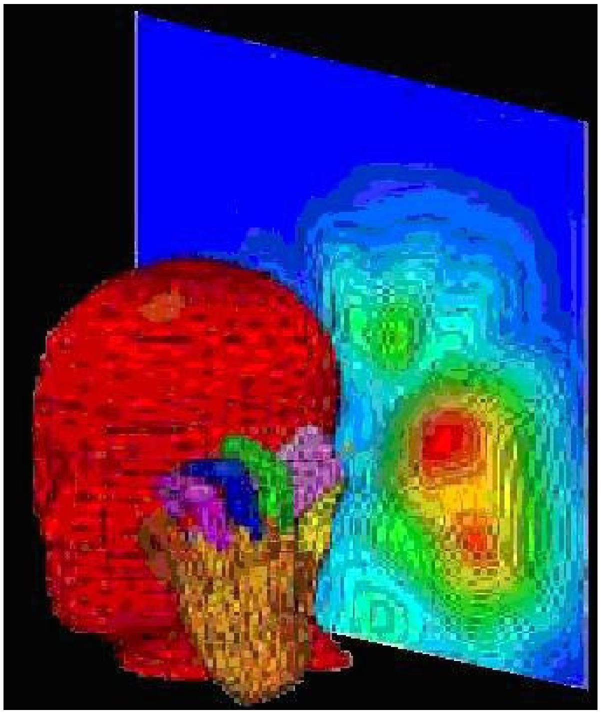
Higher gain antennas may spread the signal further on the horizontal plane, which creates a larger cell that could also pick up additional noise. This results in a lower SNR that increases the packet error ratio. SNR is defined by the following criteria:

- Signal—The radiated energy transmitted from one radio that can be received uninterrupted by another radio. For Wi-Fi this means that the transmitting radio is sending 802.11 protocol packets that the receiving radio is able to decode.
- Noise—Transmitted energy in the frequency range of the receiving radio that cannot be decoded by that radio.

The larger the difference in energy between the protocol packet and the background noise, the better the reception of the protocol packet and the lower the packet error rate and bit error rate. Coverage area design involves using channels to create the lowest possible packet error rate while maintaining a high audio call capacity.

Higher gain antennas can also reduce the number of calls on a Wi-Fi channel because of the increased coverage area. For audio, a ceiling-mounted antenna is preferred over a wall-mounted patch because the human head and body attenuate 5 dB of the signal (see Figure 9-3). Ceiling mounted antennas are better positioned to avoid more of this head and body attenuation than most wall-mounted antennas.

Figure 9-3 Head and Hand Attenuation



Antenna Positioning

Ceiling-mounted antennas typically have better signal paths to handheld phones. The recommended coverage cell size takes into consideration the signal loss because of the attenuation of human heads and other obstacles. It is important to understand that the gain of antennas is reciprocal; gain applies equally to reception and transmission. Antenna gain is not an increase in transmitted power because the radio produces the transmitted power. The antenna is only a passive device. Gain is derived by focusing the signal of the radio into a direction, plane, and beam width, much in the same way a flashlight reflector focuses the light emanating from its bulb.

For further information on WLAN RF planning, see Chapter 3, “WLAN RF Design Considerations”.

Handset Antennas

For phones that integrate the antenna inside the body of the phone, the way the user holds the phone in their hand can influence signal attenuation by 4 dB. In some cases, a phone held against the head with the hand covering the antenna can result in a signal drop of 9 dB. The general rule for indoor deployments is that every 9 dB of signal loss reduces the coverage area in half. Figure 9-3 shows an example of the difference in radiating power from a handset when held to the head.

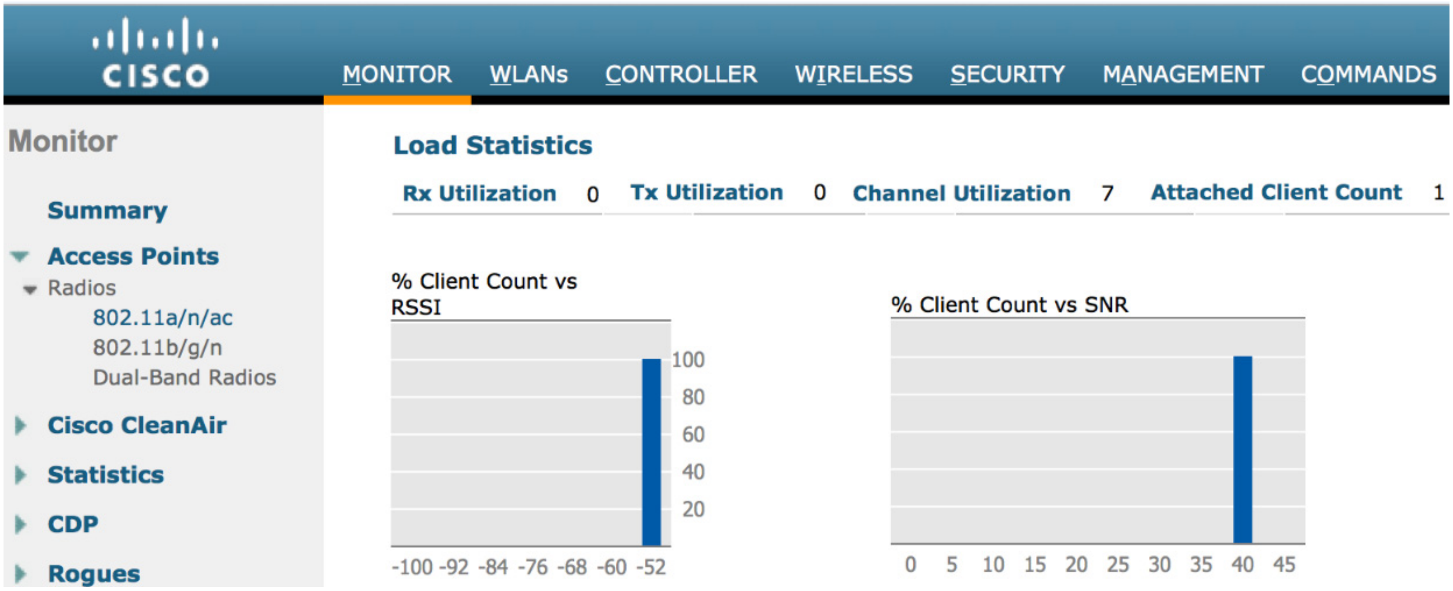
The typical smartphone and tablet computer have a Wi-Fi antenna system with negative dB gain. The typical smartphone antenna is -3 or -4 dBi. The typical laptop has a positive gain from 0 to 2 dBi. This difference in antenna gain reflects in a difference in coverage range between smartphones, tablets and laptops at the same AP. For a smartphone or tablet to obtain the best application performance, the AP channel coverage should be designed to the Wi-Fi capabilities of the smartphones or tablets themselves.

To provide optimum link quality between the smartphone, tablet or laptop and the AP, the AP should operate with ClientLink enabled. ClientLink is enabled by default with the Cisco wireless LAN controller (WLC).

Channel Utilization

The 802.11, 802.11b, 802.11g and 802.11n protocol specifications use the same 2.4 GHz band and therefore they must be able to interoperate with each other. This interoperability introduces additional 802.11 protection protocol logic overhead that reduces channel throughput. Many sites already have devices using the Wi-Fi frequencies of the 2.4 GHz band, but there are a number of foreign devices that can use these same frequencies. These foreign devices include Bluetooth, cordless phones, video game controllers, surveillance cameras, and even microwave ovens. Because the 2.4 GHz band is so crowded, and coupled with constraints on its channel allocation, Cisco recommends using the 5 GHz Wi-Fi band for new VoWLAN deployments. The channels available in the 5 GHz band are generally not as heavily used at most sites (see Figure 9-4). It is important to note that use of the 5 GHz UNII-2 channels for VoWLAN traffic requires the absence of radar. Cisco therefore recommends that there should be additional testing at any new site to determine whether a particular UNII-2 channel should be configured to be blocked. The reason is that if an AP detects radar on a channel during normal use, it must leave that channel until the radar signal is no longer present.

Figure 9-4 Channel Utilization for 2.4 GHz Reporting



Load Statistics

Rx Utilization 0
Tx Utilization 0
Channel Utilization 7
Attached Client Count 1

Before the installation of a Cisco Unified Wireless Network, the site can be tested for channel interference and utilization with tools from AirMagnet, Wild Packets, Cognio, and others. To aid in the design process, the AP On-Demand Statistics Display report generated by the Cisco Prime Infrastructure provides a spectrum review of:

- Client count versus RSSI
- Client count versus SNR
- Channel utilization

The ALOHAnet protocol defines a radio channel as full when channel utilization reaches 33 percent. This means the channel is busy enough that packets must wait for an open time slot before they are transmitted. The 46 percent channel utilization, as shown in Figure 9-4, is above the channel utilization wireless packetized Aloha standard.

To reduce channel utilization in the 2.4 GHz band, Cisco recommends moving clients to 5 GHz and removing the legacy 1 Mbps and 2 Mbps data rates from the 2.4 GHz configuration when legacy devices are not part of the client makeup.

Dynamic Frequency Selection and 802.11h Requirements of the APs

The Federal Communications Commission (FCC) of the United States, the European Telecommunications Standards Institute (ETSI), and other regulatory agencies have their own requirements regarding the use of radio frequencies. Portions of the 5 GHz band have been and are currently being used for such things as weather radars. Although most 5 GHz radar systems generally use higher frequencies with shorter wavelengths, there are still systems in place that overlap with some Wi-Fi frequencies in the 5 GHz UNII-2 bands. In 2006, the FCC opened the frequencies in the 5.470 to 5.725 MHz range to unlicensed use. With these additional frequencies came a requirement to maintain an *interference-free* AP configuration. The AP must constantly monitor for radar pulses (typically from military, satellite, or weather stations) and use dynamic frequency selection (DFS) to automatically switch to a *clean* channel if radar is detected.

When radar is detected, the system must carry out the following:

- Stop packet transmission within 200 ms
- Stop control transmissions within 10 seconds
- Avoid transmission on the channel for 30 minutes
- Scan a new channel for 60 seconds before transmission

Because the radar avoidance requirements in the UNII-2 band can impact audio call quality, you should conduct a test for radar before going live with audio applications. Cisco Spectrum Expert is an excellent tool to test for the presence of radar on certain channels. If radar is detected during a Spectrum Expert test, the APs can then be configured to block use of those channels.

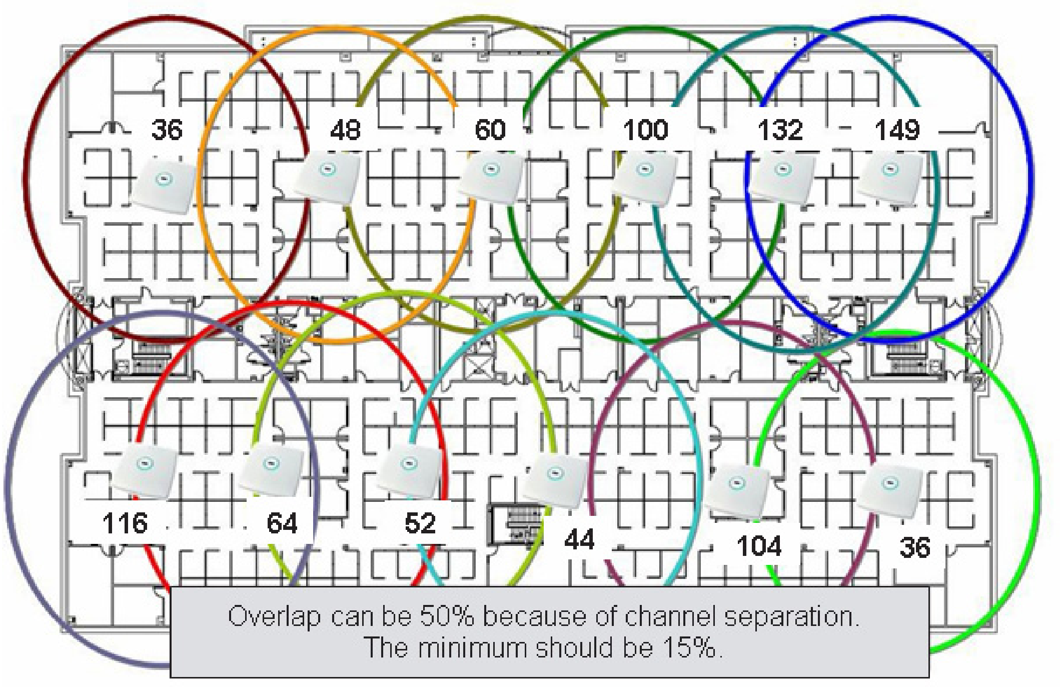
5 GHz Band Channels

The DFS requirement includes the four original UNII-2 channels (52-64) and the new eight channels (100-116 and 132-140), while the 5 GHz band now has 20 channels. All of these channels are non-overlapping channels so all can be co-located. 2.4 GHz has only three non-overlapping channels. A design allowing co-located channels in a coverage area aggregates the number calls obtainable in a coverage area.

Note See the Cisco website for current compliance information and also check with your local regulatory authority to find out what is permitted within your country.

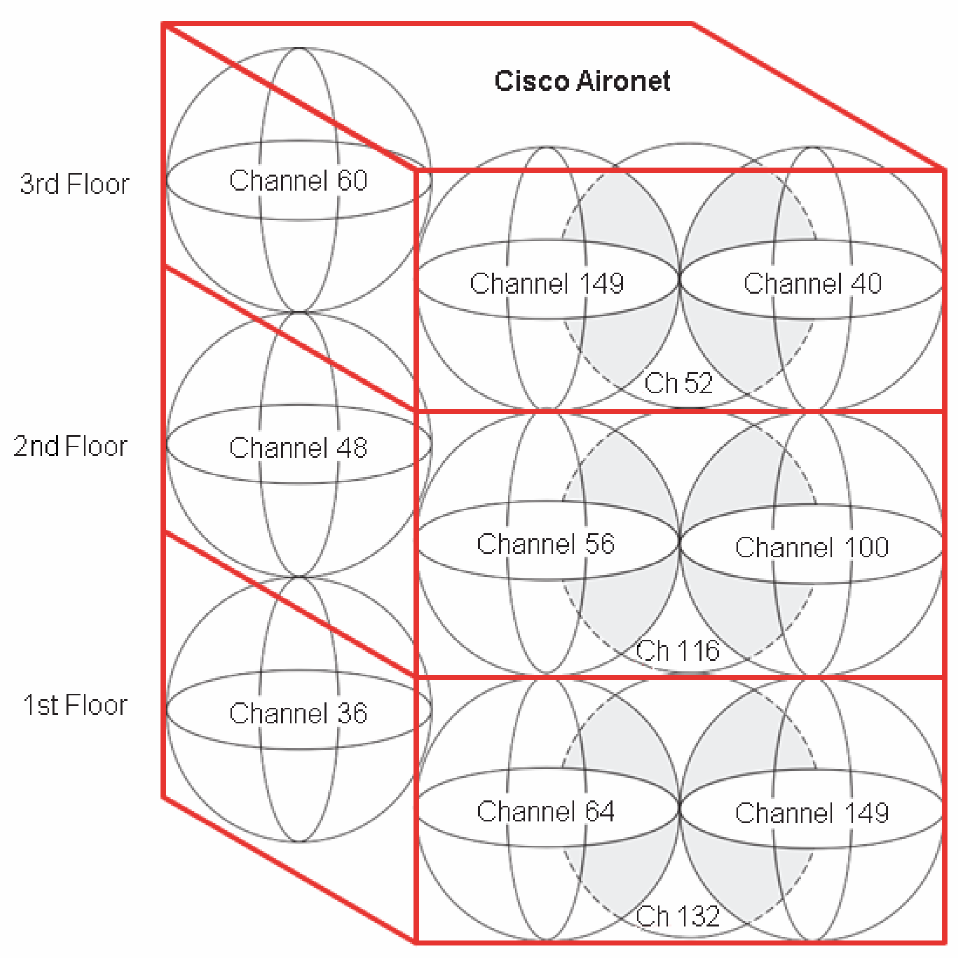
A channel-based design can be implemented horizontally on a single floor, as shown in Figure 9-5.

Figure 9-5 Single Floor Channel Design


36
48
60
100
132
149
116
64
52
44
104
36
Overlap can be 50% because of channel separation.
The minimum should be 15%.

In a multi-floor design, the channels can be separated vertically between floors to reduce the possibility of co-channel interference, as shown in Figure 9-6.

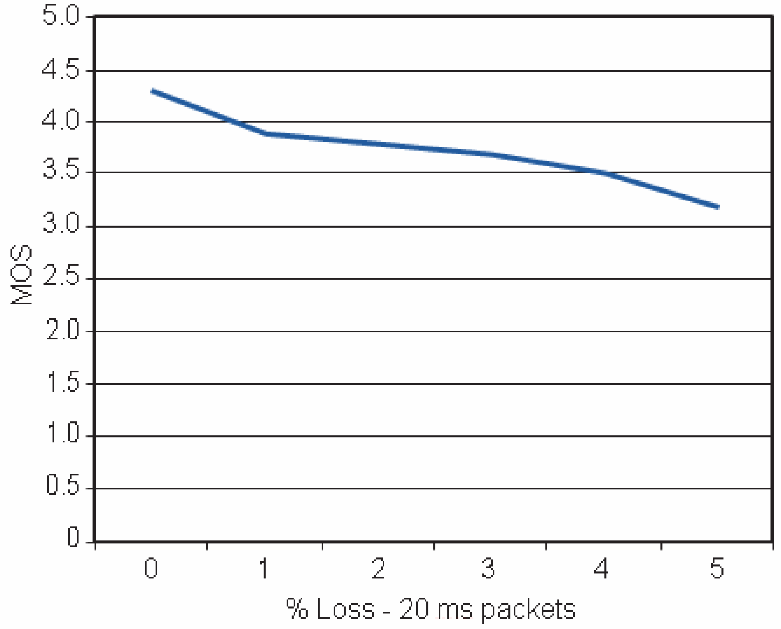
Figure 9-6 Vertical Channel Separation



Call Capacity

The number of calls on a Wi-Fi channel is limited by a number of factors. First, the RF spectrum used by the AP and VoWLAN clients cannot be shielded from electromagnetic interference as shielded twisted-pair CAT 5 cable can. The closest Wi-Fi comes to segmentation is channel separation. The open, shared RF spectrum of 802.11 creates the possibility for high packet loss. Most of the packet loss is addressed through retransmission of 802.11 frames, which in turn causes jitter. Figure 9-7 illustrates the packet loss relationship as a mean opinion score (MOS).

Figure 9-7 Effective Packet Loss Graphic



In the 802.11a specification as well as in 802.11g, the highest coverage range is achieved by the lowest data rate, which is 6 Mbps. For any given power level the lowest packet error rate is also 6 Mbps.

An acceptable coverage area for audio is an area that maintains a packet error rate of 5 percent or less. The MOS scores are ranked as follows:

- 4.4—Highest MOS score
- 4.3-4.0—*Very satisfied* to *Satisfied*
- 4.0-3.6—*Some users satisfied*

Figure 9-7 above shows that a packet error rate of 5 percent reduces the MOS to a level of *Some users satisfied* quality of speech.

The coverage area edge for a phone is the point in the coverage area that lowers the MOS rating to the *Very satisfied* category. This coverage area edge is referred to as a *cell edge* in this design guide. A cell edge with a 1 percent packet error rate is needed for audio because of the likelihood of multiple phone clients, data clients, co-channel interference, and other un-accounted for interferers. Cell edge and coverage design are defined in detail in other sections of this chapter.

If 802.11 and 802.11b are not required to support legacy 2.4 GHz Wi-Fi clients, Cisco recommends disabling the data rates of 1, 2, 5.5, and 11 MHz.

If these rates are disabled, one or more 802.11g data rates must be set to *required*. Cisco recommends that the 6 MHz data rate be set to required, but this depends on the cell size design requirements, which might require using a higher bit rate. If possible, an 802.11g-only network is recommended rather than a combined 802.11b/g network. Most data clients and phone clients recognize the data rates advertised by the AP in its beacons and probe response. Therefore, clients send their management, control, multicast, and broadcast packets at the required data rates as advertised by the AP, while they can send their unicast packets at any of the data rates advertised by the AP. Generally, unicast packets are sent at a data rate that provides the highest reliable rate for the link between the AP and client. Cisco APs are capable of sending unicast packets at a data rate that is unique for each ClientLink.

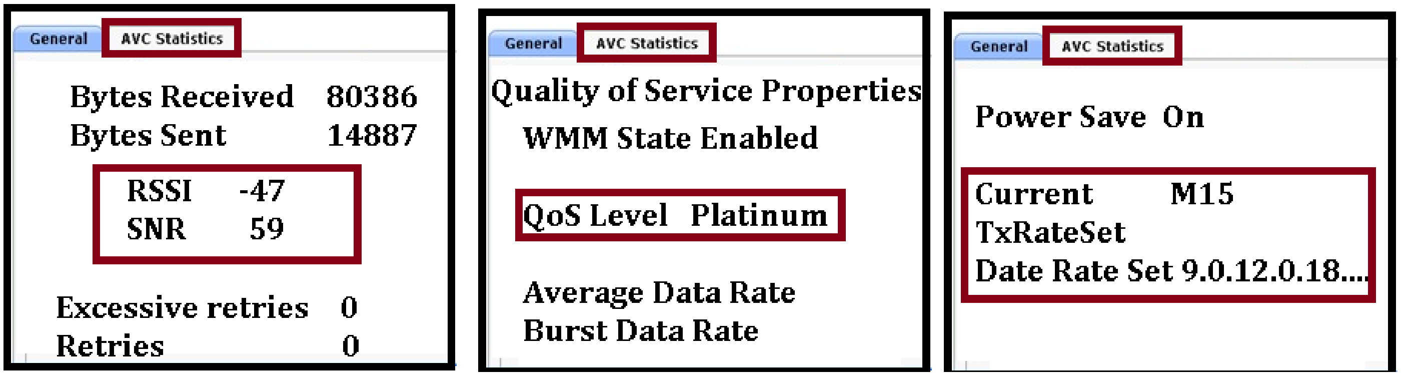
SNR is an important consideration for packet reception. The receiving radio is either the AP radio or the phone radio. The SNR is not likely to be the same at both radios of the link. SNR and multipath interference must be considered at the AP and at the cell edge. Path loss can be assumed to be the same at both ends of the link.

Cisco recommends that for audio applications the cell edge be determined by using the actual phone at the desired data rate. The audio packets sent between the AP and the phone in Wi-Fi applications are generally unicast real-time transport protocol (RTP) G.711 packets with a typical size of 236 bytes. The RTP packet is based on UDP and IP protocols, and therefore RTP is connectionless. The signal strength, SNR, data rate, and error rates of the phone call can be seen from the AP statistics, either on the autonomous AP or the controller-based CAPWAP AP.

Cisco also recommends that coverage testing be done with active calls. The two-way call provides the downstream (AP to client) packet size and the unicast packet type for ClientLink. The upstream (client to AP) provides the packets size and unicast packet type for MRC processing on the AP. When doing the client cell edge range testing, Cisco recommends testing a combination of smartphone, tablet and laptop models to the same AP from the same location and that the same square feet of space be used for all clients. This then means that the phones are not tested simultaneously because they could not all share the same space.

Figure 9-8 shows a sample of the client cell edge dBm values of a phone for 2.4 GHz and 5 GHz.

Figure 9-8 Client Edge RSSI -67 dBm with an SNR of 59 dB



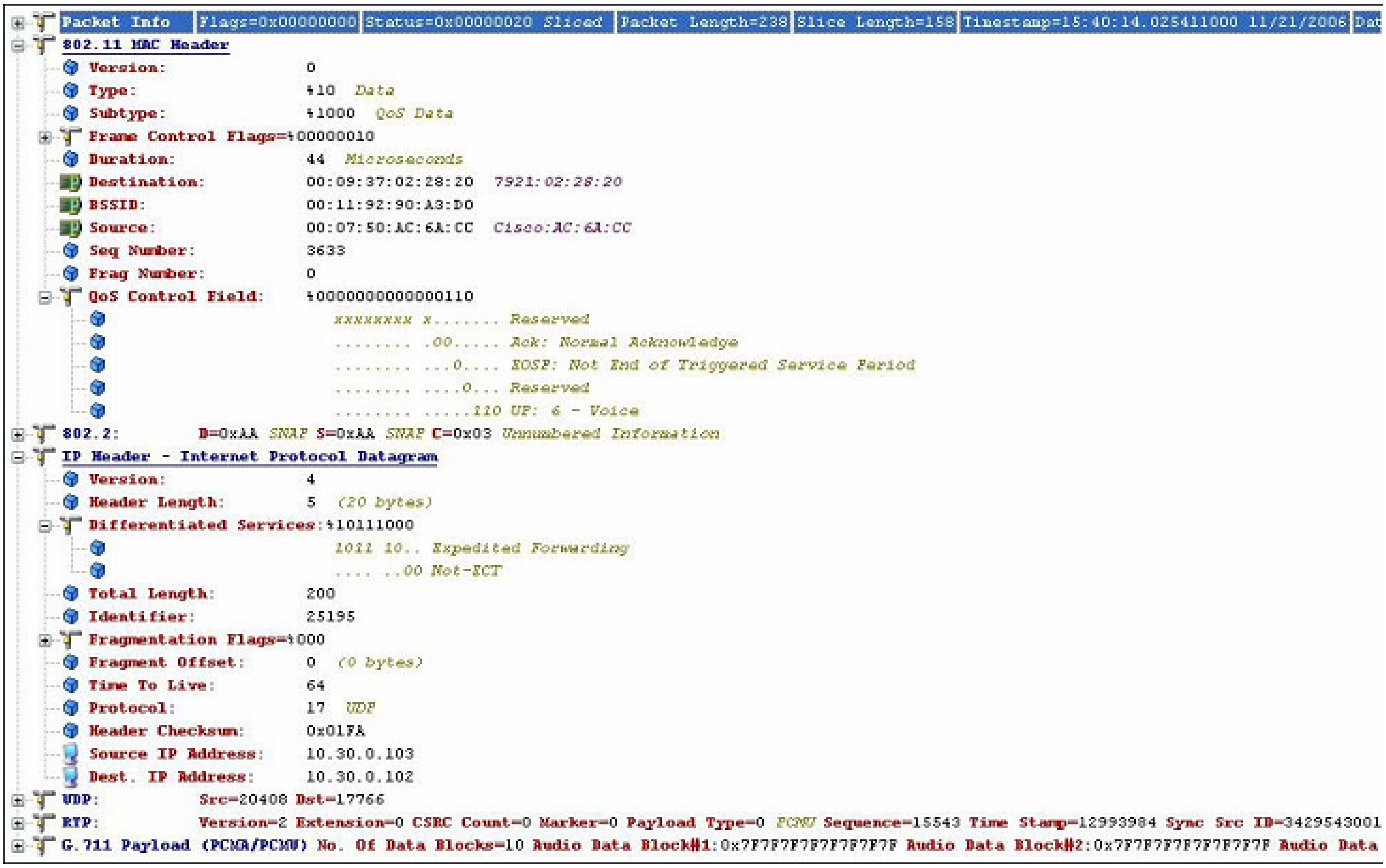
Bytes Received 80386
Bytes Sent 14887
RSSI -47
SNR 59
Excessive retries 0
Retries 0

Quality of Service Properties
WMM State Enabled
QoS Level Platinum
Average Data Rate
Burst Data Rate

Power Save On
Current TxRateSet M15
Date Rate Set 9.0.12.0.18....

Figure 9-9 shows a decoded audio G.711 RTP packet. The packet, which originated on a Cisco 7960 desk phone, is downstream from the AP to a VoWLAN end-point. The over-the-air QoS marking is changed from the QoS baseline marking of 5 to a user priority of 6, which follows the 802.11e specification. Call statistics on the Cisco phone can be viewed on the phone or by browsing into the phone using the IP address of the phone. After that the cell edge dBm value can then be the benchmark value for tools that are better suited for surveying. A automated survey tool will expedite the coverage design of the site.

Figure 9-9 Sample VoWLAN Capture



```
Packet Info  Flags=0x00000000 Status=0x00000020 Sliced  Packet Length=238 Slice Length=158 Timestamp=15:40:14.025411000 11/21/2006 Dat
802.11 MAC Header
    Version:                 0
    Type:                    %10  Data
    Subtype:                 %1000  QoS Data
    Frame Control Flags=%00000010
    Duration:                44  Microseconds
    Destination:             00:09:37:02:28:20  7921:02:28:20
    BSSID:                   00:11:92:90:A3:D0
    Source:                  00:07:50:AC:6A:CC  Cisco:AC:6A:CC
    Seq Number:              3633
    Frag Number:             0
    QoS Control Field:       %0000000000000110
                                xxxxxxxx x....... Reserved
                                ........ .00..... Ack: Normal Acknowledge
                                ........ ...0.... EOSP: Not End of Triggered Service Period
                                ........ ....0... Reserved
                                ........ .....110 UP: 6 - Voice
802.2:          D=0xAA SNAP S=0xAA SNAP C=0x03 Unnumbered Information
IP Header - Internet Protocol Datagram
    Version:                 4
    Header Length:           5  (20 bytes)
    Differentiated Services:%10111000
                                1011 10.. Expedited Forwarding
                                .... ..00 Not-ECT
    Total Length:            200
    Identifier:              25195
    Fragmentation Flags=%000
    Fragment Offset:         0  (0 bytes)
    Time To Live:            64
    Protocol:                17  UDP
    Header Checksum:         0x01FA
    Source IP Address:       10.30.0.103
    Dest. IP Address:        10.30.0.102
UDP:            Src=20408 Dst=17766
RTP:            Version=2 Extension=0 CSRC Count=0 Marker=0 Payload Type=0 PCMU Sequence=15543 Time Stamp=12993984 Sync Src ID=3429543001
G.711 Payload (PCMA/PCMU) No. Of Data Blocks=10 Audio Data Block#1:0x7F7F7F7F7F7F7F7F Audio Data Block#2:0x7F7F7F7F7F7F7F7F Audio Data
```

When multipath interference is present at a location where signal level measurements are being taken, it is quite likely that the reported values will fluctuate from packet to packet. A packet can be as much as 5 dB higher or lower than the previous packet. It may take several minutes to obtain an average value for a given measurement location.

AP Call Capacity

A key part of the planning process for a VoWLAN deployment is to plan the number of simultaneous audio streams per AP.

Note A call between two phones associated to the same AP is considered as two active audio streams.

When planning the audio stream capacity of the AP, consider the following points:

- The utilization of an unlicensed (shared) 802.11 channel is the real determinant for the number of simultaneous audio streams an AP can carry.
- Because the channel utilization and AP performance determine the number of audio streams, same channel and next channel separation are very important. Two APs in the same location, operating on the same channel, do not provide twice the number of audio streams. In fact, there can be fewer audio streams than a single AP would provide.

- Cell capacity or bandwidth determines the number of audio streams that can be simultaneously conducted.
- The QoS features supported in the handsets and VoWLAN deployment should be considered.
- Various handsets have different WLAN QoS features and capabilities that impact the features that are enabled in the WLAN deployment, and ultimately determine the per-AP audio call capacity of the AP. Most VoWLAN handsets provide guidance on the number of calls per AP supported by that phone; this should be considered a best-case figure for situations where the handset is able to use its optimal QoS features and has full access to the channel capacity.

The actual number of audio streams a channel can support is highly dependent on a number of issues, including environmental factors and client compliance to Wi-Fi Multimedia (WMM).

The Table 9-1 in lists how Cisco Compatible Extensions benefit VoWLAN call quality.

Table 9-1 Cisco Compatible Extensions Benefit VoWLAN Quality

How Cisco Compatible Extension Benefits VoWLAN Quality	
Feature	**Benefit**
CCKM Support for EAP-Types	Locally Cached Credentials Means Faster Roams
Unscheduled Automatic Power Save Delivery (U-APSD)	More Channel Capacity and Better Battery Life
TSPEC-Based Call Admission Control (CAC)	Managed Call Capacity for Roaming and Emergency Calls
Voice Metrics	Better and More Informed Troubleshooting
Neighbor List	Reduced Client Channel Scanning
Load Balancing	Calls Balanced Between APs
Dynamic Transmit Power Control (DTPC)	Clients Learn a Power to Transmit At
Assisted Roaming	Faster Layer 2 Roams

From Table 9-1 it can be seen that:

- Cisco Centralized Key Management (CCKM) provides faster client roaming for Extensible Authentication Protocol (EAP)-authenticated clients, which benefits audio call quality.
- Call Admission Control (CAC) also benefits audio call quality and can create bandwidth reservation for E911 and roaming calls.
- Assisted Roaming and Neighbor List benefit audio call quality and battery life.
- Voice metrics can benefit management.
- Unscheduled automatic power save delivery (U-APSD) and dynamic transmit power control (DTPC) benefit battery life.
- Load balancing and DTPC benefit audio call quality.

The Cisco Compatible Extensions Program provides third-party verification of Cisco Aironet wireless infrastructure products and wireless client devices from third-party companies. Several of the Cisco Compatible Extensions features have more than one benefit.

The amount of buffer memory, CPU speed, and radio quality are key factors of the performance of an AP radio. QoS features prioritize the audio and data traffic in the channel. For a further discussion of QoS, see Chapter 5, "Cisco Unified Wireless QoS and AVC".

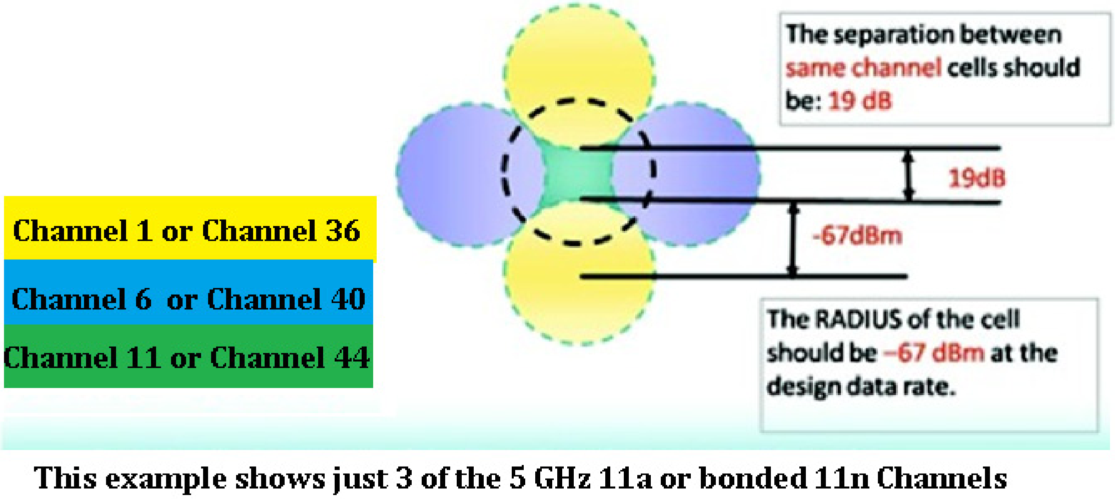
The 802.11e, WMM, and Cisco Compatible Extension specifications help balance and prevent the overloading of a cell with audio streams. CAC determines whether there is enough channel capacity to start a call; if not, the phone can scan for another channel. The primary benefit of U-ASPD is the preservation of WLAN client power by allowing the transmission of frames from the WLAN client to trigger the forwarding of client data frames that are being buffered at the AP for power saving purposes. The Neighbor List option provides the phone with a list that includes channel numbers and channel capacity of neighboring APs. This is done to improve audio call quality, provide faster roams, and improve battery life.

Cell Edge Design

Cisco guidelines for deploying 802.11b/g/a VoWLAN handsets recommend a design where a minimum power of -67 dBm is present at the cell boundary (see Figure 9-10). This practice creates cell sizes that are smaller than those used in data WLAN designs of the past. The -67 dBm threshold is a general recommendation for achieving a packet error of one percent, which requires an SNR value of 25 dB or greater (local noise conditions impact this requirement). Therefore, when determining the likely channel coverage area for a particular phone type, both signal strength and noise measured at the phone must be verified using the client statistics offered through the AP. See Table 9-1 for determining these values on the autonomous and CAPWAP APs.

The -67 dBm signal strength measurement has been used by 802.11b phone vendors for a number of years, and tests indicate that this same general rule of measurement also works well for 802.11g/n and 802.11a/n/ac phone clients.

Figure 9-10 Cell Edge Measurements


The separation between same channel cells should be: 19 dB
19dB
-67dBm
Channel 1 or Channel 36
Channel 6 or Channel 40
Channel 11 or Channel 44
The RADIUS of the cell should be -67 dBm at the design data rate.
This example shows just 3 of the 5 GHz 11a or bonded 11n Channels

Note The -86 dBm separations shown in Figure 9-10 are simplified and are considered ideal. It is not likely that this 19 dBm of separation can be achieved in most deployments. The most important RF design criteria are the -67 dBm cell radius and the 20 percent recommended overlap between cells. Designing to these constraints optimizes channel separation.

For 5 GHz cells, there is less concern about same channel separation because of the number of available non-overlapping channels. There are 20 channels in the 802.11a 5 GHz band so a two-channel separation is almost always possible. In contrast, the 2.4 GHz band has only three channels that do not overlap in frequency.

For both the 5 GHz and 2.4 GHz bands the cell edge must be at the floor level where a packet error rate of 1 percent is maintained at the highest data rate desired for a given channel. The data rate is 72 Mbps for an 802.11n on 2.4 GHz with a one spatial stream client.

The data rate is 150 Mbps for an 802.11n client on the 5 GHz band with a 40 MHz wide channel and with a one spatial stream client. A laptop running a softphone application such as Jabber can support three spatial streams and have a date rate to 450 Mbps on a 5 GHz, 40 MHz wide channel. Both an 802.11a client and an 802.11n client that is only 20 MHz wide and supporting one spatial stream can share Wi-Fi channel access on a 40 MHz wide channel with an 802.11ac three spatial stream client on a 80 MHz wide channel.

This type of client mixture and protocol mixture is part of the 802.11 specification. The compatibility for this type of client mixture on the same Wi-Fi frequencies is part of the 802.11n and 802.11ac specifications.

The major design question is how to define the coverage area for bandwidth and call capacity. Audio call capacity is about the same for 802.11n and 802.11ac as it was for 802.11g and 802.11a. This is because of the packet size of the audio G.711 or G.722 frame, which with AES encryption is less than 300 bytes. The small packet size and the ACK logic of the 802.11 specification creates a large overhead compared to large streaming applications. A video call generates both small audio packets and large video packets. The video packets are highly compressed and therefore spaced out in comparison to the audio. Cisco recommends as a guideline to establish the cell edge of coverage. Measure the distance from the AP that the phone is when the RSSI value of phone on the AP is -67 dBm.

802.11g and 802.11a phone clients can be capable of rates up to 54 Mbps. Current chip sets support many rates, but transmit power capabilities differ. Cisco highly recommends that all links between phone clients and APs be established using matching transmit power levels (see Dynamic Transmit Power Control).

Coverage cells can be created for specific data rates. For a high density deployment or a deployment where a large number of calls are required within a small floor space, 802.11a is recommended because of the number of channels and the 54 Mbps data rate. The lower data rates in 802.11a can be disabled, the 24 Mbps data rate can be set to *required*, while the 36 to 54 Mbps data rates can be left enabled.

After setting the cell edge of -67 dBm, determine where the error rate of 1 percent occurs, and then examine the SNR value.

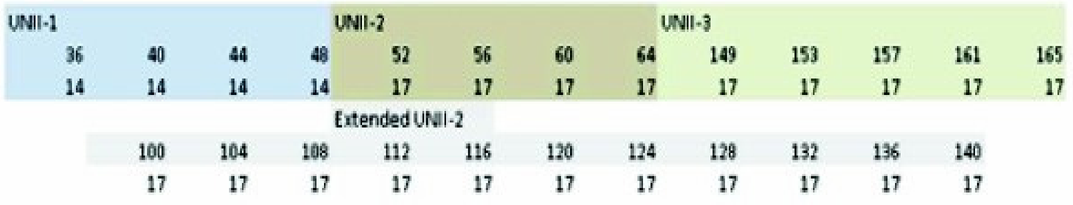
The -67 dBm cell edge can be determined as follows:

- Set the phone to its desired transmit power.
- Set the AP to a matching transmit power.
- Place the AP and the desired antenna in the location where the phone will be used.
- With an active call, or while sending and receiving packets equal in size to the G711 codec, measure the signal level out to the -67 dBm cell edge.

Carefully examine the data sheets of the particular phone device to determine the transmit power levels and data rates supported by the phone device in a particular Wi-Fi band. For more information, refer the Data Sheets for Cisco Unified Wireless IP Phones.

The 2.4 GHz maximum transmit power levels vary on different channels and with different AP models. The 5 GHz maximum transmit power levels vary by model. The Cisco Aironet AP data sheets should be carefully reviewed to determine which AP model supports which data rates. Figure 9-11 shows an example of the maximum 5 GHz transmit power in dBm by channel.

Figure 9-11 Channel Power Assignment



UNII-1				UNII-2				UNII-3				
36	40	44	48	52	56	60	64	149	153	157	161	165
14	14	14	14	17	17	17	17	17	17	17	17	17

Extended UNII-2										
100	104	108	112	116	120	124	128	132	136	140
17	17	17	17	17	17	17	17	17	17	17

The maximum permissible transmit power across the 5 GHz band varies by as much as 6 dB. This means that when using the maximum allowed transmit power throughout a site that allows all channels, there will not be equal cell coverage on all channels. It also means that if dynamic channel selection is used, the cell coverage edge can change based on the channel number. However, dynamic channel selection can be tuned. The default mode of dynamic channel selection accounts for the difference of maximum transmit power level by channel.

Cell transmit power on all APs should not exceed the maximum or desired transmit power of the phones. If the phone's maximum or set transmit power is 13 dBm, Cisco recommends that all APs have a maximum transmit power of 13 dBm. Therefore, the maximum transmit power on the AP should be set to an equal level or, if that is not possible, the next higher transmit power level. Equal transmit power is recommended to avoid one-way audio problems. The AP generally has better receiver sensitivity and diversity support than the phone, so it should be able to receive the slightly lower strength phone signal. See Dynamic Transmit Power Control for more information on equal transmit powers.

Dual Band Coverage Cells

Chapter 3, “WLAN RF Design Considerations” describes 2.4 GHz and 5 GHz channel coverage design. For a dual mode AP to provide equal cell coverage on both the 2.4 GHz and 5 GHz channels, the 2.4 GHz channel must have an equal (or usually lower) transmit power than the 5 GHz channel. At most sites the noise level in the SNR formula is lower by up to 10 dB. The receiver sensitivity of 802.11g radios is generally 2 dBm better than the same data rate on 802.11a radios. For example, the Cisco 7921G phone data sheet lists the receive sensitivity of -78 dBm at the data rate of 36 Mbps for 802.11g, and -76 dBm for 802.11a. Therefore, given the anticipated better noise floor of 10 dB, the 802.11a cell can do better by 8 dBm. Other details such as the difference in path loss between 802.11g and 802.11a keep this from being a direct ratio. However, if the same coverage cells are desired, reducing the 802.11g network by one or two power levels from the 802.11a network power levels should accomplish this goal.

Dynamic Transmit Power Control

By default, Cisco Aironet APs have dynamic transmit power control (DTPC) enabled. DTPC is automatic with Cisco WLCs but must be configured on autonomous APs.

The objective of DTPC is to reduce the chance of one-way audio because of an imbalance of transmit power between the AP and the Wi-Fi radio of the client. DTPC accomplishes this by:

- Setting the phones transmit power to match the transmit power of the APs.
- Having APs advertise their transmit power for the clients to learn.

DTPC allows phones to automatically adjust their transmit power to that of the APs. In the example shown in Figure 9-12, this means that the phone changes its transmit power level from 5 mW to 100 mW.

Figure 9-12 Client and AP Power Matching

The licensing requirements of 802.11 do not require clients to have a minimum transmit power and few if any Wi-Fi devices use the maximum transmit powers allowed by regulations. With a typical Wi-Fi device, the maximum transmit power capability is at or below 100 mW. This is because Wi-Fi specifications do not require APs and clients to have matching power levels during associated connections between themselves. There will always be the possibility that for a short period of time, while associated, they might not be in the coverage range of each other but still be associated. If this happens during an active call there is a loss of audio. If the transmit power levels are not equal during an active call then there is audio loss. Several 802.11 mechanisms help to maintain the connection between the AP and the phone, one being that they can negotiate a slower data rate. Slower data rates generally have higher transmit powers than higher data rates. The slower data rates should be avoided in dense deployments. This is because when a coverage cell needs high throughput and capacity, the slower data rates for the high packet count phone calls lowers the throughput for all clients on that Wi-Fi channel and AP.

Cisco highly recommends that the maximum configured transmit power on APs be no higher than the maximum transmit power the client phones support. Because the current Cisco APs support ClientLink, Cisco highly recommends that ClientLink be configured. ClientLink dynamically creates a directed signal towards selected clients. The ClientLink logic changes the signal prorogation on directed packets but not on broadcast or multicast packets. ClientLink removes the typically omni antenna horizontal signal prorogation with equal signal energy in all directions. Signal energy is increased in the direction for the selected clients. The directed signal increases the signal energy at the selected client, improving downstream signal quality at the phone. This improves the MOS value of the call. Improving the MOS value reduces retries and improves the throughput in the coverage area for all clients. Because this is a shaped signal that is directed to a specific location, there is reduced signal in the remaining coverage areas of the AP. This improves the performance of the channel in areas where there is channel overlap with broadcast and multicast packets with other APs.

Cisco recommends that each model of phone be tested for its Wi-Fi coverage range. The WLC reports the receive signal strength indicator (RSSI) of each client at the AP to which the phone is associated. The value shown in the RSSI field is the signal strength of a packet transmitted from the phone to the AP. The value indicates how strong the packet transmitted by the phone was at when it was received at the AP. It is recommended to check the coverage range of the phones and that the phones be placed at the estimated coverage edge of the AP. Then check the RSSI when a phone is on an active call. The goal is that at the cell edge (recommended -67dBm RSSI) the packets are sent at a high data rate. See Figure 9-10 for a reference to the cell edge for VoWLAN Wi-Fi coverage area range. The value of -39 shown in the figure is a very strong signal that is seen when the client phone or device is within a few feet of the AP.

Testing the phone's coverage has become more important with the advent of smartphones and tablets. Because the Wi-Fi feature sets of these devices are typically for the consumer market, these devices typically have few 802.11 features that are considered to support enterprise. The consumer orientation of most smartphones and tablets does not support DTPC. Therefore, Cisco recommends that the maximum transmit power for 2.4 GHz and 5 GHz be a dBm value that matches the 2.4 GHz and 5 GHz band maximum transmit power of your weakest smartphone or tablet. This WLC field value limits the transmit signal power of the APs, thereby helping to maintain a balance in range of the phone to the AP.

802.11r and 802.11k Features

IEEE 802.11k and 802.11r are key industry standards that enable seamless Basic Service Set (BSS) transitions in the WLAN environment. With WLAN 7.2 release, Cisco supports the 802.11r secure authentication Fast Transition protocol. The IEEE 802.11k specification was ratified in June 2008. The IEEE 802.11r specification was ratified in July 2008. 802.11r specification follows the 802.11e security specification of June 2004.

See a brief description of the 802.11k Specification.

See the 802.11k Specifications.

See a brief description of the 802.11r Specifications.

802.11k and 802.11k-enabled client devices send a request for a list of neighbor APs (a *Neighbor List*) from the APs they are currently associated with. The request is in the form of an 802.11 management frame known as an *action packet*. The AP responds with an action packet that contains a Neighbor List of APs on the same WLAN along with their Wi-Fi channel numbers.

From the response action packet the 802.11k client learns which APs are candidates for the next roam. The use of 802.11k radio resource management (RRM) algorithms allows smartphones to roam efficiently and quickly: a requirement for good call quality in an enterprise environment where on-call roams are common.

Cisco recommends that the 802.11k be configured in the WLC to enable radio resource management (RRM) to provide both 2.4 GHz and 5 GHz AP channel numbers in the Neighbor List response packets. Cisco also recommends the use of 5 GHz band Wi-Fi channels for not only VoWLAN calls but for all applications and devices.

With information from the Neighbor List, 802.11k clients do not need to probe all of the 2.4 GHz and 5 GHz channels to find an AP they can roam to. Not having to probe all of the channels reduces channel utilization on all channels, thereby increasing bandwidth on all channels. It also reduces roam times and improves the decisions made by the client. Additionally, it increases battery life of the device because it is neither changing the radio configuration for each channel nor sending probe requests on each channel. This prevents the devices from having to process all of the probe response frames.

The 802.11r and 802.11e specifications both support the same authentication types: EAP-FAST, LEAP, EAP-TLS, EAP-TTLS, EAP-SIM, and PEAP versions 1 and 2. This security feature allows an 802.11r-enabled client to authenticate securely to an AP in an exchange of only four packets. Two of the packets are sent over the Ethernet wires that connect the APs to each other. The other two packets are sent on the Wi-Fi channels of each AP. This allows the 802.11r client to be authenticated securely to the AP that it is going to roam to before it actually roams. The result is the 802.11r client can be sending and receiving data, video, and audio packets after the roam without the delay of the authentication process. Because the 802.11 header is changed by the addition of the 802.11r parameters, the WLAN for 802.11r clients cannot be shared with clients that are not 802.11r-aware. This means that all clients that have the SSID assigned by the WLAN with 802.11r enabled must have Wi-Fi radio firmware that is aware of the 802.11r element in association packets. Limitations to 802.11r fast roaming are:

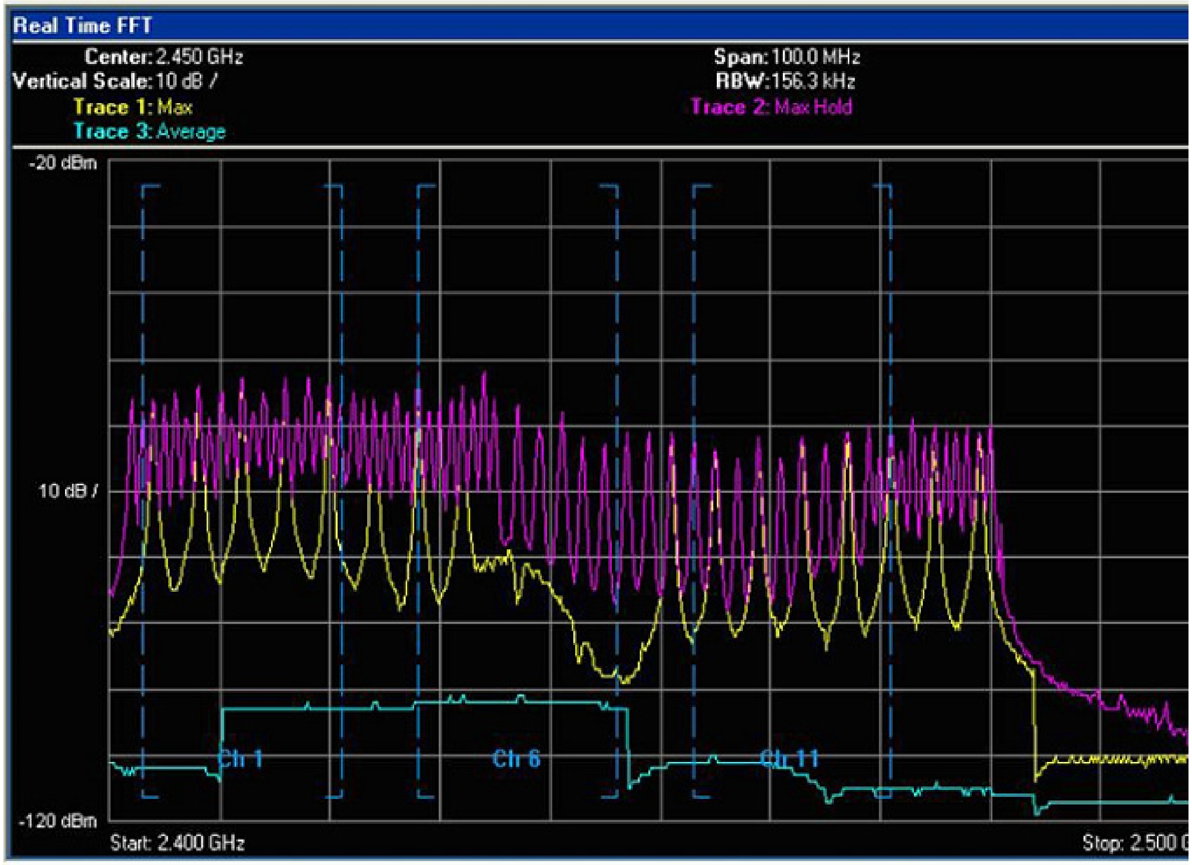
- Is supported on APs in autonomous mode but requires Wireless Domain Services (WDS).
- Roaming between local authentication and central authentication WLAN is not supported.

Cisco recommends that you use the 802.11r specification as it improves roam times because of a reduction in the number of packets sent over the Wi-Fi channel between a client that is already authenticated to the WLAN.

Interference Sources Local to the User

Interference can be local to the user but it is also likely to affect nearby users. Bluetooth is a popular RF protocol used in personal area networks that interferes with 2.4 GHz Wi-Fi channels. Figure 9-13 shows that the actual Bluetooth signal does span all of the 2.4 GHz channels used by 802.11b/g clients. This graphic is taken from an 802.11g audio call with a Bluetooth headset linked to the phone. Figure 9-14 also shows the jitter caused by the Bluetooth headset.

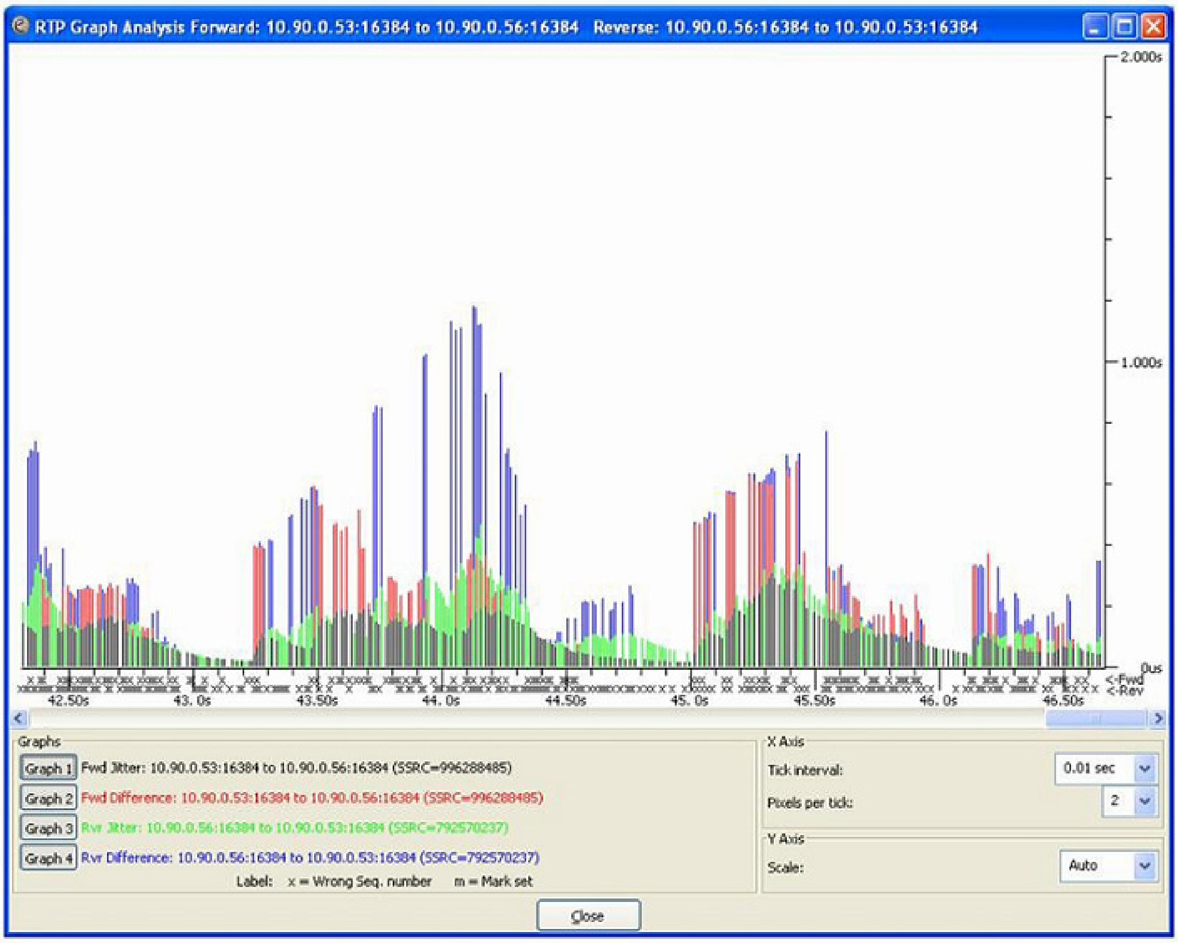
Figure 9-13 Signal Pattern in the 802.11b/g 2.4 GHz Spectrum of a Typical Bluetooth Earpiece



In Figure 9-13 the purple line shows the Max Hold, the maximum transmit power that was reached during the test. The yellow line shows the maximum transmit power in the last sample period of ten seconds. The turquoise line shows the average transmit power over the period of the test. The vertical dashed blue lines separate the three non-overlapping 802.11b/g channels (Ch1, Ch6, and Ch11). The charting is from 2.400 GHz on the left to 2.500 GHz on the right. From the right edge of the Ch11 vertical blue line is the part of the 802.11 spectrum used in Europe and Japan. This capture was done with the AP and clients configured for the North American regulatory domain. This graph shows that the Bluetooth earpiece was easily transmitting outside of FCC regulations.

Notice that the Bluetooth signal is very narrow. Bluetooth transmits data on a single MHz of frequency, stops the transmission, moves to another frequency in the 802.11 2.4 GHz band, and then transmits data. This is repeated continually. The 802.11b and 802.11g signals are sent with a combined 22 MHz of frequency. The radio remains on that 22 MHz of frequency. This grouping of 22 MHz is referred to as the channel. The Max Hold line shows how strong the Bluetooth is while in search mode. The signal level is above that of a 50 mW (17 dBm) OFDM 802.11g radio. A signal of this strength and duration causes 802.11b/g phones to drop the VoWLAN call. Lesser strength Bluetooth signals cause jitter, resulting in a lower MOS value. Figure 9-14 shows an example of an Ethereal jitter analysis of three simultaneous phone calls, each using a Bluetooth earpiece.

Figure 9-14 Jitter Analysis Example



RTP Graph Analysis Forward: 10.90.0.53:16384 to 10.90.0.56:16384 Reverse: 10.90.0.56:16384 to 10.90.0.53:16384

Graphs

Graph 1 Fwd Jitter: 10.90.0.53:16384 to 10.90.0.56:16384 (SSRC=996288485)

Graph 2 Fwd Difference: 10.90.0.53:16384 to 10.90.0.56:16384 (SSRC=996288485)

Graph 3 Rvr Jitter: 10.90.0.56:16384 to 10.90.0.53:16384 (SSRC=792570237)

Graph 4 Rvr Difference: 10.90.0.56:16384 to 10.90.0.53:16384 (SSRC=792570237)

Label: x = Wrong Seq. number m = Mark set

X Axis

Tick interval: 0.01 sec

Pixels per tick: 2

Y Axis

Scale: Auto

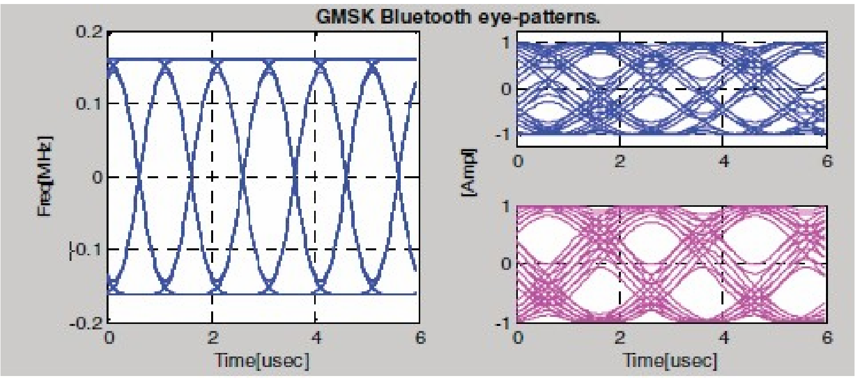
All three calls were on the same AP and were to three other phones also on the same AP. For information on interference with Wi-Fi and Bluetooth, see the IEEE Report.

The factors that affect the impairments introduced to a Bluetooth TDM packet when colliding with Wi-Fi OFDM include:

- Relative power
- Bandwidth
- Mutual overlap
- Number of colliding OFDM signals

Simulations were performed on the effects of interference between a sample Wi-Fi OFDM packet and Bluetooth signals, as shown in Figure 9-15. The figure shows the Normal GMSK Bluetooth undistorted signal TDM characteristics. On the left is frequency versus time (MHz), and on the right is I/Q amplitudes.

Figure 9-15 IEEE Waveform Simulations



As shown above in the Figure 9-15, the 625-second long hopping Bluetooth packet can interfere with more than one OFDM packet at a time, especially whenever high-rate OFDM mode packets (where the length of the packet is much shorter than that of Bluetooth) are subject to the collision.

CHAPTER 10

Cisco Unified Wireless Network Guest Access Services

The introduction of wireless LAN (WLAN) technologies in the enterprise has changed the way corporations and small-to-medium businesses function by freeing staff and network resources from the constraints of fixed network connectivity.

WLAN has also changed how individuals access the Internet and their corporate networks from public locations. The advent of public WLAN hotspots has caused mobile workers to become accustomed to being able to access their corporate network from practically anywhere.

Introduction

The paradigm of public access has extended to the enterprise itself. Our highly mobile, information-on-demand culture requires on-demand network connectivity. For this reason, enterprise guest access services are becoming increasingly important and a necessity in the corporate environment.

While there is broad recognition that guest networking is becoming increasingly important, there is also well-founded apprehension over how to safeguard internal corporate information and infrastructure assets. When implemented correctly, an enterprise that implements a guest access solution will most likely improve their overall security posture as a result of the network audits associated with the implementation process.

In addition to overall improved security, implementing a guest access network offers these additional general benefits.

- Authentication and authorization control of guests based on variables including date, duration, and bandwidth.
- An audit mechanism to track who is currently using, or has used, the network.

Additional benefits of a wireless-based guest access include the following:

- It provides wider coverage by including areas such as lobbies and other common areas that otherwise might not have been wired for network connectivity.
- It removes the need for designated guest access areas or rooms.

Scope

Several architectures can be implemented to offer guest access in the enterprise. It is not the goal of this chapter to cover all possible solutions. Instead, this chapter focuses on the implementation of wireless guest networking using the Cisco Unified Wireless Network solution. For more information on deploying wired and wireless Guest Access services in other topology scenarios, see:

Network Virtualization--Guest and Partner Access Deployment Guide

Wireless Guest Access Overview

Ideally, the implementation of a wireless guest network uses as much of an enterprise's existing wireless and wired infrastructure as possible to avoid the cost and complexity of building a physical overlay network. Assuming this is the case, the following additional elements and functions are needed:

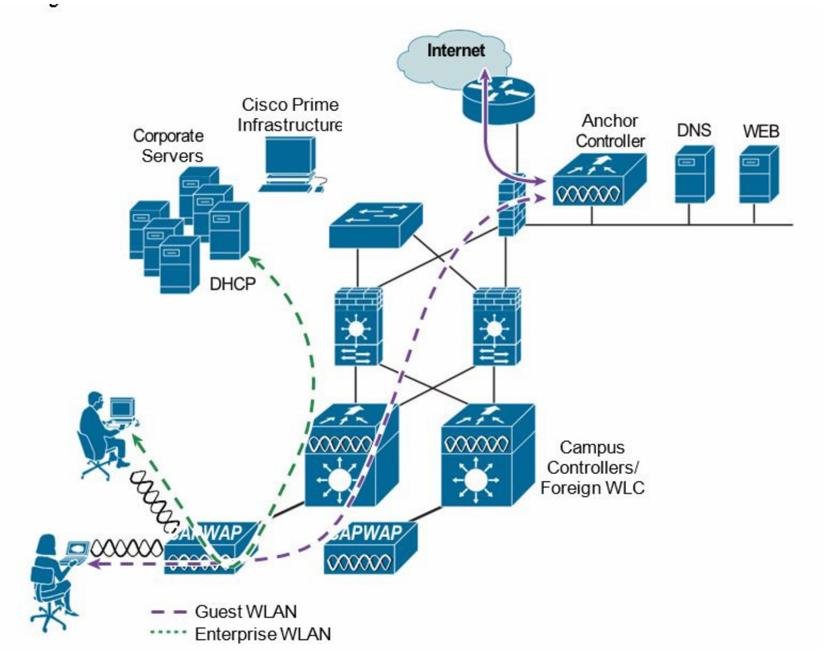
- A dedicated guest WLAN/SSID—Implemented throughout the campus wireless network wherever guest access is required.
- Guest traffic segregation—Requires implementing Layer 2 or Layer 3 techniques across the campus network to restrict where guests are allowed to go.
- Access control—Involves using imbedded access control functionality within the campus network or implementing an external platform to control guest access to the Internet from the enterprise network.
- Guest user credential management—A process by which a sponsor or lobby administrator can create temporary credentials in behalf of a guest. This function might be resident within an access control platform or it might be a component of AAA or some other management system.

Guest Access using the Cisco Unified Wireless Network Solution

The Cisco Unified WLAN solution offers a flexible, easy-to-implement method for deploying wireless guest access by using Ethernet in IP (RFC3378) within the centralized architecture. Ethernet in IP is used to create a tunnel across a Layer 3 topology between two WLC endpoints. The benefit of this approach is that there are no additional protocols or segmentation techniques that must be implemented to isolate guest traffic from the enterprise.

See Figure 10-1 for an example of guest access topology using a centralized WLAN architecture.

Figure 10-1 Centralized Controller Guest Access



As illustrated in Figure 10-1 the anchor controller is located in the enterprise DMZ where it performs an "anchor" function. The anchor controller is responsible for terminating EoIP tunnels that originate from other campus controller throughout the network. These "foreign" controllers are responsible for termination, management, and standard operation of the various WLANs provisioned throughout the enterprise, including one or more guest WLANs. Guest WLANs are transported via an EoIP tunnel to the anchor controller. Specifically, guest WLAN data frames are encapsulated using CAPWAP from the AP to the foreign controller and then encapsulated in EoIP from the foreign management system to a guest VLAN defined on the anchor WLC. In this way, guest user traffic is forwarded to the Internet transparently, with no visibility by, or interaction with, other traffic in the enterprise.

WLAN Controller Guest Access

The Guest Access solution is self-contained and does not require any external platforms to perform access control, web portal, or AAA services. All these functions are configured and run within the anchor controller. However, the option exists to implement one or all of these functions externally and is discussed later in the chapter.

Supported Platforms

The anchor function, which includes tunnel termination, web authentication, and access control is supported on the following WLC platforms (using version 8.1 or later):

- WLC 2504
- WLC 5508
- WLC 5520

- WiSM-2
- WLC 8510
- WLC 8540

The following WLC platforms cannot be used for anchor functions, but can be used for standard controller deployments and guest mobility tunnel origination (foreign WLC) to a designated anchor controller(s):

- Cisco WLAN Controller Module for Integrated Service Routers (ISR-SM)
- WLC 7500
- Virtual WLC

Auto Anchor Mobility to Support Wireless Guest Access

Auto anchor mobility, or guest WLAN mobility, is a key feature of the Cisco Unified Wireless Network solution. It offers the ability to map a provisioned guest WLAN to one or more (anchor) WLCs by using an EoIP tunnel. Auto anchor mobility allows a guest WLAN and all associated guest traffic to be transported transparently across an enterprise network to an anchor controller that resides in the Internet DMZ (see Figure 10-2).

Figure 10-2 Auto Anchor EoIP Tunnels

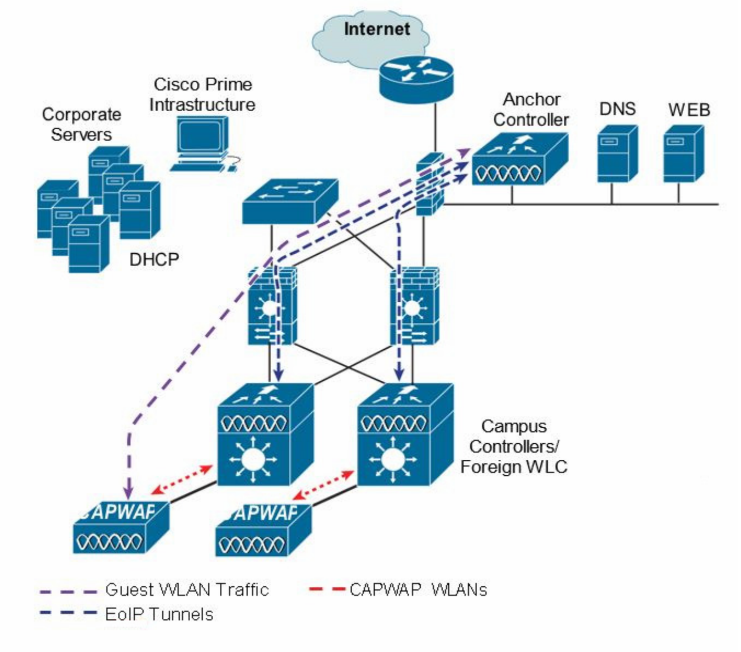
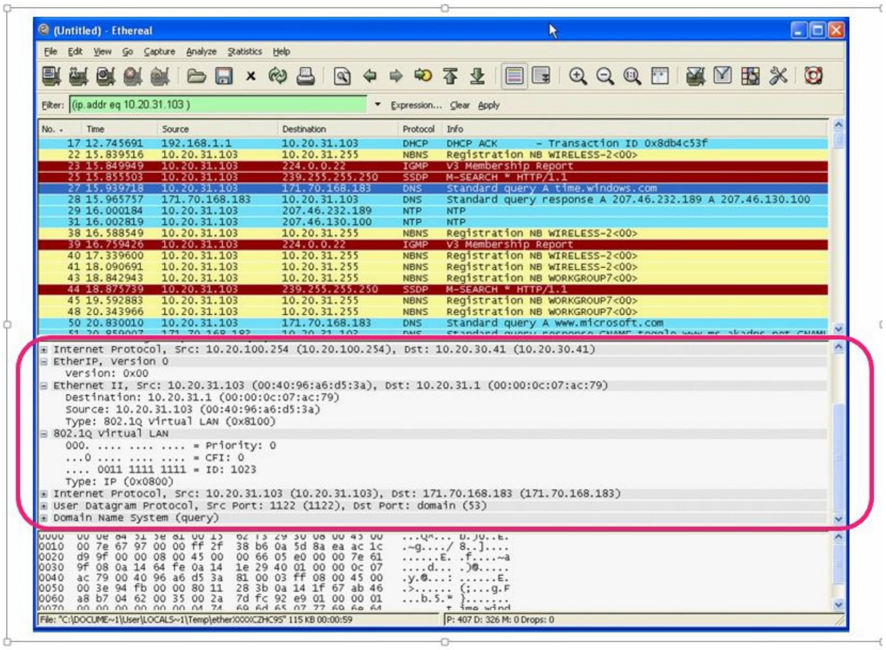


Figure 10-3 shows a sniffer trace of an Ethernet in IP tunnel (highlighted) between a foreign controller with a guest WLAN provisioned and an anchor controller that is performing local web authentication. The first IP detail shown represents the Ethernet in IP tunnel between the foreign and anchor controllers. The second IP detail is that of guest traffic (in this case, a DNS query).

Figure 10-3 Sample Ethernet in IP Sniffer Trace


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: (ip.addr eq 10.20.31.103)
Expression... Clear Apply

```
No. .  Time        Source          Destination      Protocol  Info
    17 12.745691   192.168.1.1     10.20.31.103     DHCP      DHCP ACK      - Transaction ID 0x8db4c53f
    22 15.839516   10.20.31.103    10.20.31.255     NBNS      Registration NB WIRELESS-2<00>
    23 15.849949   10.20.31.103    224.0.0.22       IGMP      V3 Membership Report
    25 15.855503   10.20.31.103    239.255.255.250  SSDP      M-SEARCH * HTTP/1.1
    27 15.939718   10.20.31.103    171.70.168.183   DNS       Standard query A time.windows.com
    28 15.965757   171.70.168.183  10.20.31.103     DNS       Standard query response A 207.46.232.189 A 207.46.130.100
    29 16.000184   10.20.31.103    207.46.232.189   NTP       NTP
    31 16.002819   10.20.31.103    207.46.130.100   NTP       NTP
    38 16.588549   10.20.31.103    10.20.31.255     NBNS      Registration NB WIRELESS-2<00>
    39 16.759426   10.20.31.103    224.0.0.22       IGMP      V3 Membership Report
    40 17.339600   10.20.31.103    10.20.31.255     NBNS      Registration NB WIRELESS-2<00>
    41 18.090691   10.20.31.103    10.20.31.255     NBNS      Registration NB WIRELESS-2<00>
    43 18.842943   10.20.31.103    10.20.31.255     NBNS      Registration NB WORKGROUP7<00>
    44 18.875739   10.20.31.103    239.255.255.250  SSDP      M-SEARCH * HTTP/1.1
    45 19.592883   10.20.31.103    10.20.31.255     NBNS      Registration NB WORKGROUP7<00>
    48 20.343966   10.20.31.103    10.20.31.255     NBNS      Registration NB WORKGROUP7<00>
    50 20.830010   10.20.31.103    171.70.168.183   DNS       Standard query A www.microsoft.com
```

```
⊞ Internet Protocol, Src: 10.20.100.254 (10.20.100.254), Dst: 10.20.30.41 (10.20.30.41)
⊟ EtherIP, Version 0
    Version: 0x00
⊟ Ethernet II, Src: 10.20.31.103 (00:40:96:a6:d5:3a), Dst: 10.20.31.1 (00:00:0c:07:ac:79)
    Destination: 10.20.31.1 (00:00:0c:07:ac:79)
    Source: 10.20.31.103 (00:40:96:a6:d5:3a)
    Type: 802.1Q Virtual LAN (0x8100)
⊟ 802.1Q Virtual LAN
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0011 1111 1111 = ID: 1023
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 10.20.31.103 (10.20.31.103), Dst: 171.70.168.183 (171.70.168.183)
⊞ User Datagram Protocol, Src Port: 1122 (1122), Dst Port: domain (53)
⊞ Domain Name System (query)
```

```
0010  00 7e 67 97 00 00 ff 2f  38 b6 0a 5d 8a ea ac 1c   .~g..../ 8..]....
0020  d9 9f 00 00 08 00 45 00  00 66 05 e0 00 00 7e 61   ......E. .f....~a
0030  9f 08 0a 14 64 fe 0a 14  1e 29 40 01 00 00 0c 07   ....d... .)@.....
0040  ac 79 00 40 96 a6 d5 3a  81 00 03 ff 08 00 45 00   .y.@...: ......E.
0050  00 3e 94 fb 00 00 80 11  28 3b 0a 14 1f 67 ab 46   .>...... (;...g.F
0060  a8 b7 04 62 00 35 00 2a  7d fc 92 e9 01 00 00 01   ...b.5.* }.......
```

```
File: "C:\DOCUME~1\User\LOCALS~1\Temp\etherXXXXCZHC9S" 115 KB 00:00:59    P: 407 D: 326 M: 0 Drops: 0
```

Anchor Controller Deployment Guidelines

This section provides guidelines for deploying an anchor controller to support wireless guest access.

Anchor Controller Positioning

Because the anchor controller is responsible for termination of guest WLAN traffic and subsequent access to the Internet, it is typically positioned in the enterprise Internet DMZ. In doing so, rules can be established within the firewall to precisely manage communications between authorized controllers throughout the enterprise and the anchor controller. Such rules might include filtering on source or destination controller addresses, UDP port 16666 for inter-WLC communication, and IP protocol ID 97 Ethernet in IP for client traffic. Other rules that might be needed include the following:

- UDP 161 and 162 for SNMP
- UDP 69 for TFTP
- TCP 80, 443 and 8443 for HTTP, or HTTPS for GUI access
- TCP 23 or 22 for Telnet, or SSH for CLI access
- UDP 123 for NTP
- TCP 514 for Syslog
- UDP 1812 and 1813 RADIUS

Depending on the topology, the firewall can be used to protect the anchor controller from outside threats.

For the best possible performance and because of its suggested positioning in the network, it is strongly recommended that the guest anchor controller be dedicated to supporting guest access functions only. In other words, the anchor controller should not be used to support guest access in addition to controlling and managing other CAPWAP APs in the enterprise.

DHCP Services

As previously described, guest traffic is transported at Layer 2 via EoIP. Therefore, the first point at which DHCP services can be implemented is either locally on the anchor controller or the controller can relay client DHCP requests to an external server. See Guest Access Configuration, for configuration examples.

Routing

Guest traffic egress occurs at the anchor controller. Guest WLANs are mapped to a dynamic interface/VLAN on the anchor. Depending on the topology, this interface might connect to an interface on a firewall, or directly to an Internet border router. Therefore, a client's default gateway IP is either that of the firewall or the address of a VLAN/interface on the first hop router. For ingress routing, it is assumed the guest VLAN is directly connected to a DMZ interface on a firewall or to an interface on a border router. In either case, the guest (VLAN) subnet is known as a directly connected network and advertised accordingly.

Anchor Controller Sizing and Scaling

The most cost-effective platform to support guest networking, in most enterprise deployments is the Cisco 2504 Series controller. Assuming the controller is being deployed to support guest access with EoIP tunnel termination only, the 2504 with support for 12 APs is sufficient because it is assumed the controller is not going to be used to manage APs in the network.

A single wireless LAN controller can support EoIP tunnels from up to 71 foreign controllers within the enterprise.

The selection of the guest anchor controller is a function of the amount of guest traffic, as defined by the number of active guest client sessions, or as defined by the uplink interface capacity on the controller, or both.

Total throughput and client limitations per guest anchor controller are as follows:

- 2504 WLC = 1 Gbps and 1000 guest clients
- 5508 WLC = 8 Gbps and 7,000 guest clients
- 5520 WLC = 20Gbps and 20,000 guest clients
- Catalyst 6K WiSM-2 = 20G bps and 15,000 guest clients
- WLC 7500 = 10 Gbps and 20,000 guest clients
- 8510 WLC = 10 Gbps and 20,000 guest clients
- 8540 WLC = 40 Gbps and 64,000 guest clients

Anchor Controller Redundancy N+1

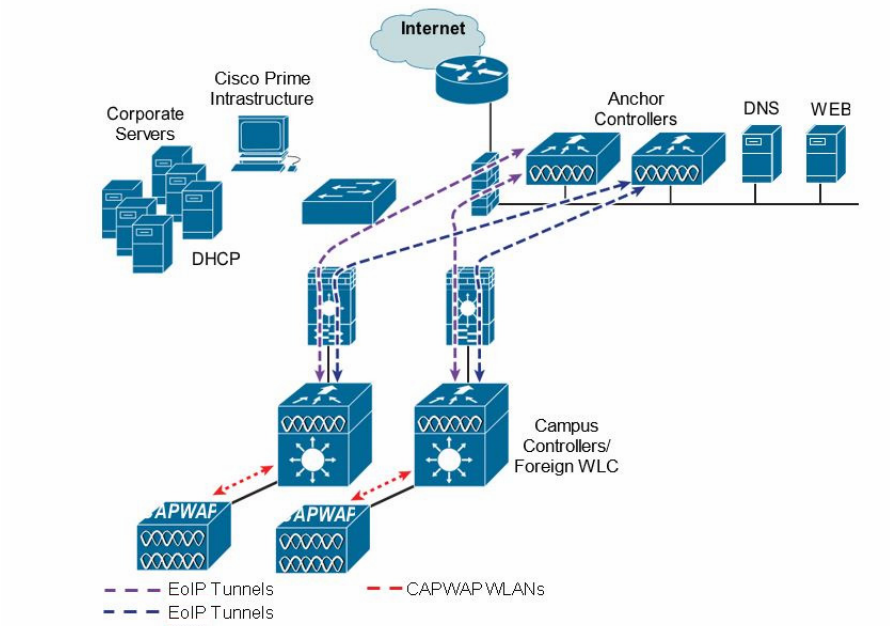
Beginning with Release 4.1 of Cisco Unified Wireless Network solution software, a "guest N+1" redundancy capability was added to the auto anchor/mobility functionality. This feature introduced an automatic ping function that enables a foreign controller to proactively ping anchor controllers to verity control and data path connectivity. In the event of failure or an active anchor becomes unreachable, the foreign controller does the following:

- Automatically detects that the anchor has become unreachable.
- Automatically disassociates any wireless clients that were previously associated with the unreachable anchor.
- Automatically re-associates wireless client(s) to an alternate anchor WLC.

With guest N+1 redundancy, two or more anchor WLCs can be defined for a given guest WLAN.

Figure 10-4 shows a generic guest access topology with anchor controller redundancy.

Figure 10-4 Guest Access Topology with Guest Anchor N+1 Redundancy



Keep in mind the following in regards to guest N+1 redundancy:

- A given foreign controller load balances wireless client connections across the list of anchor controllers configured for the guest WLAN. There is currently no method to designate one anchor as primary with one or more secondary anchors.
- Wireless clients that are associated with an anchor WLC that becomes unreachable are re-associated with another anchor defined for the WLAN. When this happens, assuming web authentication is being used, the client is redirected to the web portal authentication page and required to re-submit their credentials.

Note Multicast traffic is not supported over guest tunnels, even if multicast is enabled on the Cisco Unified Wireless Network.

Anchor Controller Redundancy Priority

The guest anchor priority feature provides a mechanism that gives "active/standby" load distribution amongst the anchor WLCs. This is achieved by assigning a fixed priority to each anchor WLC, by distributing the load to highest priority WLC and in round-robin fashion if they have the same priority value.

Releases Prior to 8.1	With Release 8.1
All guest clients are load balanced in round robin fashion amongst anchor WLCs.	All guest clients are sent to anchor controller with highest priority in relation to local internal WLC.
If an anchor fails, guest clients will be load balanced amongst remaining anchor WLCs.	If an anchor fails, guest clients will be sent to the next highest priority or round robin if remaining anchors have same priority value.

You can configure a priority to the guest anchor when you configure a WLAN. Priority values range from 1 (high) to 3 (low) or primary, secondary or tertiary and defined priority is displayed with guest anchor. Only one priority value is allowed per anchor WLC. Selection of guest anchor is round-robin based on a single priority value. If a guest anchor is down, the fallback would be on guest anchors with equal priority. If all guest anchors with same priority value are down, the selection would be on a round-robin basis on next highest priority and so on. Default priority value is 3. If WLC is upgraded to Release 8.1, it will be marked with priority 3. Priority configurations are retained across reboots. The priority configuration would be synchronized on HA pair for seamless switchover. Same set of rules apply in determining the anchor WLC regardless of IPv4 and/or IPv6 addressing. That is, highest priority value is determinant and not addressing including dual stack case.

Restrictions

- No hard limit on the number of times a priority value is used.
- Feature applies only to wireless and "old" mobility model.
- Maximum supported anchor per WLAN is 24 (same as maximum anchor per WLAN in releases prior to 8.1).
- Downgrading from Release 8.1 would void this feature since it is not supported on earlier images.
- If a guest anchor with higher priority comes up, the existing connections will not shift to the new high priority anchor and only the new connections will go to it.
- This feature is applicable when all internal and anchor WLCs are using Release 8.1.
- There should not be a local address with priority of zero at the Internal/Foreign controller. Priority 0 in the output indicates a local IP address. For example at the anchor WLC on DMZ with tunnel termination.

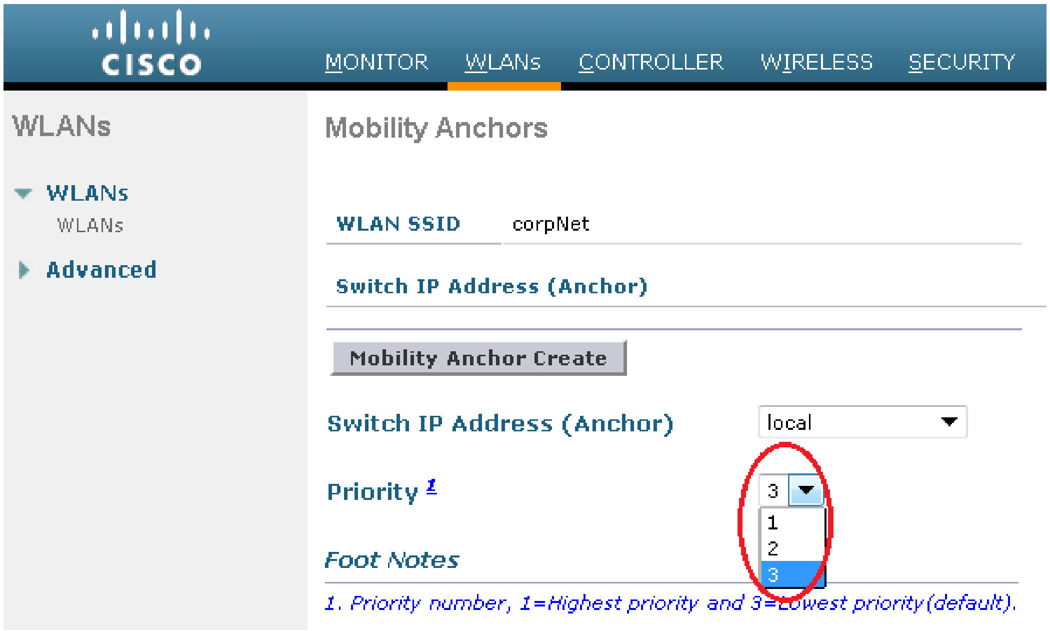
Deployment Considerations

- Priority configuration should only be done on foreign controller WLAN. On the mobility list if you are seeing value zero and non-zero that means the same controller is acting as Anchor for few WLANs and foreign controller for few WLAN, if you have WLC in DMZ and there is no APs connected to it, then we should not see any non-zero priority for any of its WLANs, as this should be the terminating point for all the clients on the network.

- Ideally we should not see priority zero on foreign WLC and non-zero on anchor WLC. Example: 10.10.10.10(Site A) and 20.20.20.20(Site B) should not have any priority with zero and DMZ controller 172.10.10.10(Site A) and 172.20.20.20(Site B) should not have any priority with non-zero values.
- Here priority values zero is not configurable when we select the controller own IP Address as anchor. It will automatically set the priority zero if controller own IP address is selected as anchor.

Examples

- Local anchor WLCs may be grouped together with higher priority value than group of remote anchor WLCs.
- Guest client traffic goes to Anchor WLC(s) that is/are local to internal WLC rather than remote one(s) due to having higher priority value.
- Guest client traffic will be load balanced in round-robin across local anchor WLCs since local anchors have same priority value.
- If all local anchor WLCs fail then traffic will be load balanced in round-robin across remote anchor WLC with next priority level.



Mobility Anchors

WLAN SSID corpNet

Switch IP Address (Anchor)

Switch IP Address (Anchor) local

Priority[1] 3

1
2
3

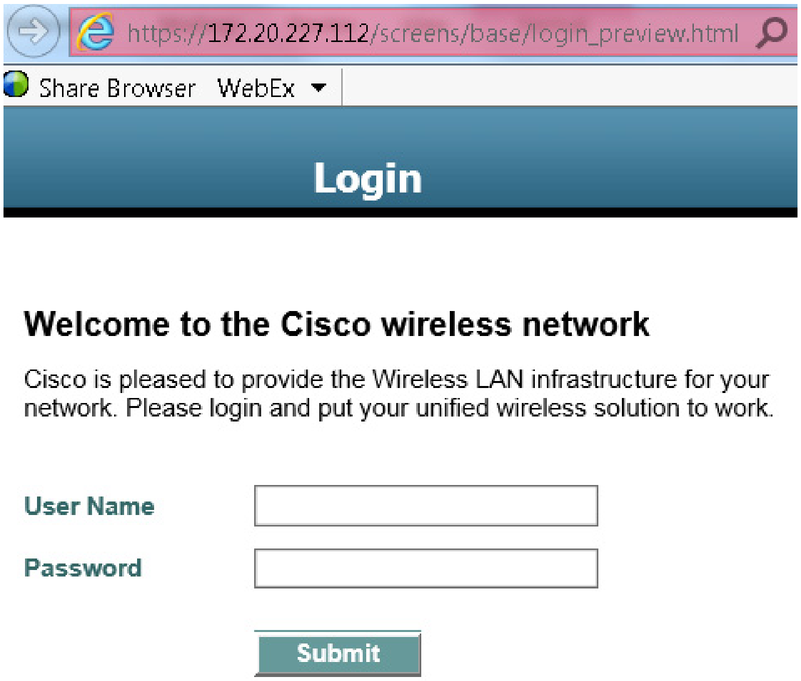
Foot Notes

1. Priority number, 1=Highest priority and 3=Lowest priority(default).

Web Portal Authentication

The Cisco Centralized Guest Access solution offers a built-in web portal that is used to solicit guest credentials for authentication and offers simple branding capabilities, along with the ability to display disclaimer or acceptable use policy information (see Figure 10-5).

Figure 10-5 Controller Web Authentication Page



https://172.20.227.112/screens/base/login_preview.html

Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

The web portal page is available on all Cisco WLAN controller platforms and is invoked by default when a WLAN is configured for Layer 3 web policy-based authentication.

If a more customized page is required, administrators have the option of importing and locally storing a customized page. Additionally, if an enterprise wants to use an external web server, the controller can be configured to redirect to it in place of using the internal server. See Guest Access Configuration, for web page configuration guidelines.

User Redirection

As is typical for most web-based authentication systems, in order for guest clients to be redirected to the WLC web authentication page, they must launch a web browser session and attempt to open a destination URL. For redirection to work correctly, the following conditions must be met:

- DNS resolution—The guest access topology must ensure that valid DNS servers are assigned via DHCP and those DNS servers are reachable to users prior to authentication. When a client associates to a web policy WLAN for authentication, all traffic is blocked except DHCP and DNS. Therefore, the DNS servers must be reachable from the anchor controller. Depending on the topology, this might require opening up conduits through a firewall to permit DNS or modifying ACLs on an Internet border router.

Note Clients with static DNS configurations might not work depending on whether their configured DNS servers are reachable from the guest network.

- Resolvable Home Page URL—The home page URL of a guest user must be globally resolvable by DNS. If a user home page is, for example, an internal company home page that cannot be resolved outside of their company intranet, that user is not redirected. In this case, the user must open a URL to a public site such as www.yahoo.com or www.google.com.

- HTTP Port 80—If the home page of a user is resolvable, but connects to a web server on a port other than port 80, they are not redirected. Again, the user is required to open a URL that uses port 80 to be redirected to the WLC web authentication page.

Note In addition to port 80, there is an option to configure one additional port number that the controller can monitor for redirection. The setting is available only through the CLI of the controller:

```
<controller_name> config> networkweb-auth-port <port>
```

Guest Credentials Management

Guest credentials can be created and managed centrally using the management system beginning with release 4.0 and later. A network administrator can create a limited privilege account within the management system that permits lobby ambassador access for the purpose of creating guest credentials. With such an account, the only function a lobby ambassador is permitted to do is create and assign guest credentials to controllers that have web-policy configured WLANs.

As with many configuration tasks within the management system, guest credentials are created using templates. Some of the newer guest user template options and capabilities are:

- There are two types of guest templates: one for scheduling immediate guest access with limited or unlimited lifetime, and the other permits administrators to schedule "future" guest access and offers time of day as well as day of week access restrictions.
- The solution offers administrators the ability to e-mail credentials to guest users. Additionally, when the "schedule" guest template is used, the system automatically e-mails credentials for each new day (interval) that access is offered.
- Guest credentials can be applied to the WLC(s) based on a (guest) WLAN SSID and the management system mapping information: campus/building/floor location or based on a WLAN SSID and a specific controller or list of controllers. The latter method is used when deploying guest access using the guest mobility anchor method as discussed in this chapter.

After a lobby ambassador has created a guest template, it is applied to one or more controllers depending on the guest access topology. Only controllers with a *"web" policy-configured* WLAN are listed as a candidate controller to which the template can be applied. This is also true when applying guest templates to controllers based on the management system map location criteria.

Guest credentials, once applied, are stored locally on the (anchor) WLC (under Security > Local Net Users) and remain there until expiration of the "Lifetime" variable as defined in the guest template. If a wireless guest is associated and active when their credentials expire, the WLC stops forwarding traffic and returns to the WEBAUTH_REQD policy state for that user. Unless the guest credentials are re-applied (to the controller), the user is no longer able to access the network.

Note The Lifetime variable associated with guest credentials is independent of the WLAN session timeout variable. If a user remains connected beyond the WLAN session timeout interval, they are de-authenticated. The user is then redirected to the web portal and, assuming their credentials have not expired, must log back in to regain access. To avoid annoying redirects for authentication, the guest WLAN session timeout variable should be set appropriately.

Local Controller Lobby Admin Access

In the event that a centralized management system is not deployed or unavailable, a network administrator can establish a local admin account on the anchor controller, which has only lobby admin privileges. A person who logs in to the controller using the lobby admin account has access to guest user management functions. Configuration options available for local guest management are limited in contrast to the capabilities available through the management system, and include:

- User name
- Generate password
- Administrator assigned password
- Confirm the password
- Lifetime-days:hours:minutes:seconds
- SSID
- Guest Role Profile
- Only WLANs configured for Layer 3 web policy authentication are displayed
- Description

Any credentials that may have been applied to the controller by the management system are shown when an admin logs into the controller. A local lobby admin account has privileges to modify or delete any guest credentials that were previously created by the management system. Guest credentials that are created locally on the WLC do not automatically appear in the management system unless the controller's configuration is updated/refreshed in the management system. Locally created guest credentials that are imported into the management system as a result of a WLC configuration refresh appear as a new guest template that can be edited and re-applied to the WLC.

Guest User Authentication

As previously discussed in Guest Credentials Management, when an administrator uses the management system or a local account on a controller to create guest user credentials, those credentials are stored locally on the controller, which in the case of a centralized guest access topology, would be the anchor controller.

When a wireless guest logs in through the web portal, the controller handles the authentication in the following order:

1. The controller checks its local database for username and password and, if present, grants access.

If no user credentials are found, then:

2. The controller checks to see if an external RADIUS server has been configured for the guest WLAN (under WLAN configuration settings). If so, then the controller creates a RADIUS access-request packet with the user name and password and forwards it to the selected RADIUS server for authentication.

If no specific RADIUS servers have been configured for the guest WLAN:

3. The controller checks its global RADIUS server configuration settings. Any external RADIUS servers configured with the option to authenticate "network" users are queried with the guest user credentials. Otherwise, if no RADIUS servers have "network user" checked, and the user has not authenticated as a result of 1 or 2 above, authentication fails.

Note A RADIUS server can still be used to support network user authentication even if the **Network User** check box is cleared under the **WLC Security > AAA > RADIUS** settings. However, to do so, a server must then be explicitly selected under the **Security > AAA Servers** settings of a given WLAN.

External Authentication

WLC and the guest account management (lobby ambassador) capabilities can be used only to create and apply guest user credentials for local authentication on the WLC. However, there may be cases where an enterprise already has an existing guest management /authentication solution deployed as part of a wired guest access or NAC solution. If this is the case, the anchor controller/guest WLAN can be configured to forward web portal authentication to an external RADIUS server, as described in Guest User Authentication.

The default protocol used by the controller to authenticate web users is Password Authentication Protocol (PAP). In the event you are authenticating web users to an external AAA server, be sure to verify the protocols supported by that server. The anchor controller can also be configured to use CHAP or MD5-CHAP for web authentication. The web auth protocol type is configured under the Controller configuration settings of the WLC.

External Authentication using ISE or Cisco Secure ACS and Microsoft User Databases

If a guest access deployment is planning to use ISE or a Microsoft user database in conjunction with Cisco ACS to authenticate guest users, see the following additional Cisco ACS configuration caveats:

Cisco Secure Access Control System

See specifically the following:

Installation and Upgrade Guide for Cisco Secure Access Control System

Active directory integration with ISE:

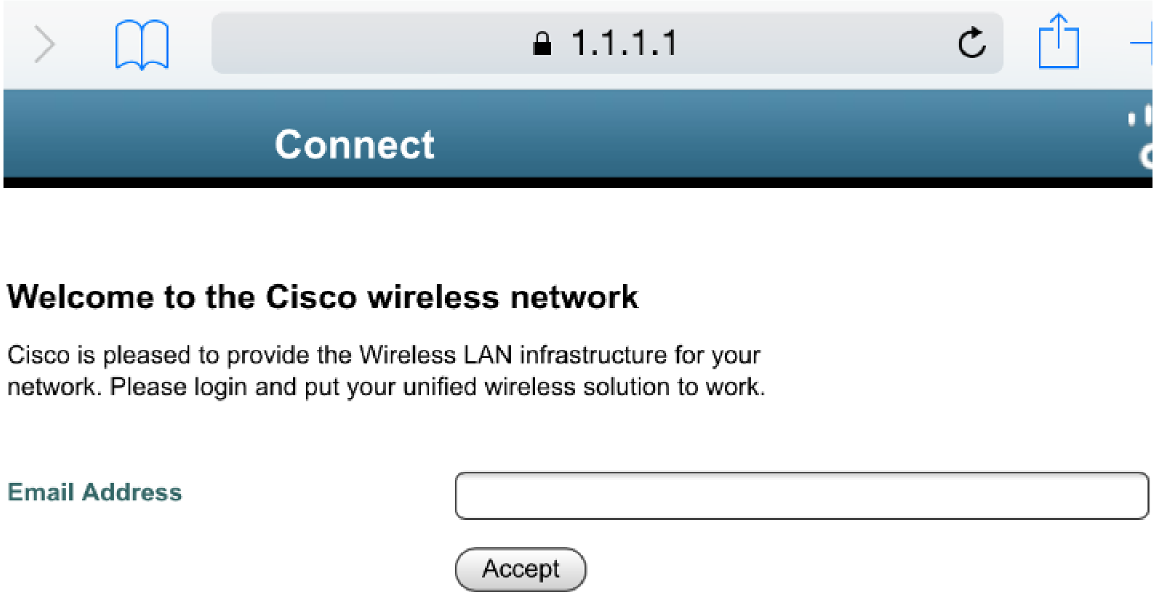
Active Directory Integration with Cisco ISE

Guest Pass-through

Another variation of wireless guest access is to bypass user authentication altogether and allow open access. However, an enterprise may still need to present an acceptable use policy or disclaimer page to users before granting access. If this is the case, then a guest WLAN can be configured for web policy pass through. In this scenario, a guest user is redirected to a portal page containing disclaimer information.

Pass through mode also has an option for a user to enter an e-mail address before connecting (see Figure 10-6 and Figure 10-7 for sample pages). See Guest Access Configuration, for configuration examples.

Figure 10-6 Pass-through Welcome AUP Page

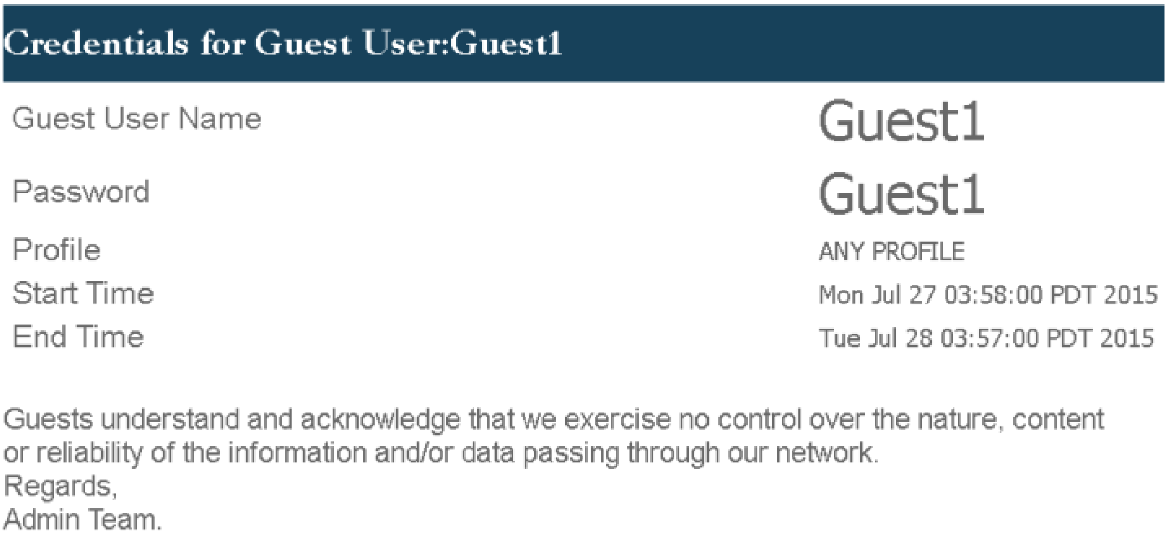


Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

Email Address:

Figure 10-7 Pass-through Page with E-mail



Credentials for Guest User:Guest1

Guest User Name	Guest1
Password	Guest1
Profile	ANY PROFILE
Start Time	Mon Jul 27 03:58:00 PDT 2015
End Time	Tue Jul 28 03:57:00 PDT 2015

Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.
Regards,
Admin Team.

Guest Access Configuration

This section describes how to enable a wireless guest access service within the Cisco Unified Wireless Network solution. The configuration tasks require the use of a web browser. A web session is established with the controller by opening an HTTPS session to the controller management IP address: **https://***management_IP* or optionally to a controller service port IP address.

The following procedures assume there is already a deployed infrastructure of controllers and LAPs with the possible exception of the anchor WLC(s). For more information, see Anchor Controller Deployment Guidelines.

Note Cisco recommends that the configuration steps outlined in this section be followed in the order in which they are presented.

The following references are used throughout the configuration sections:

- Foreign WLC—Refers to the one or more WLCs deployed throughout an enterprise campus or at branch location that are used for managing and controlling a group of APs. Foreign controllers map a guest WLAN into a guest mobility EoIP tunnel.
- Anchor WLC—Refers to one or more WLCs deployed in the enterprise DMZ that are used to perform guest mobility EoIP tunnel termination, web redirection, and user authentication.

Note Only the relevant portion of a given configuration screen capture is shown in this section.

The implementation of the Cisco Unified Wireless Network Guest Access solution can be broken into the following configuration categories:

- Anchor WLC Installation and Interface configuration—This section briefly discusses installation requirements, steps and caveats associated with implementing one or more anchor WLCs. When implementing guest access for the first time in an existing Cisco Unified Wireless Network deployment, the anchor WLC is usually a new platform that is installed at the Internet edge of an Enterprise network.
- Mobility Group Configuration—This section outlines the parameters that must be configured in order for the foreign WLCs to be able to initiate EoIP tunnels to one or more guest anchor WLCs. The mobility group configuration does not itself create the EoIP tunnels, but rather establishes peer relationships between the foreign and anchor WLCs in order to support a guest access WLAN service.
- Guest WLAN Configuration—Highlights WLAN specific configuration parameters that are required to map the guest WLAN (originating from a foreign WLC) to the anchor WLC. It is during this portion of the guest access solution configuration that EoIP tunnels are created between the foreign and anchor WLCs. This section also covers the settings required to invoke Layer 3 redirection for web-based authentication.
- Guest Account Management—This section outlines how to configure and apply guest user credentials locally on the anchor WLC using controllers the anchor WLC's lobby admin interface.
- Other Features and Solution Options—Discusses other features that may be configured including, but not limited to:
  - Web-portal page configuration and management
  - Support for external web redirection
  - Pre-authentication ACLs
  - Anchor WLC DHCP configuration
  - External radius authentication
  - External access control

Anchor WLC Installation and Interface Configuration

As described in Anchor Controller Positioning, Cisco recommends that the anchor WLC be dedicated solely to guest access functions and not be used to control and manage LAPs in the enterprise.

This section does not address all aspects of interface configuration on the anchor WLC. It is assumed the reader is familiar with the WLC initialization and configuration process required upon initial bootup using the serial console interface.

This section offers specific information and caveats as they pertain to configuring interfaces on a WLC being deployed as an anchor in a guest access topology.

As part of the initial configuration (using the serial console interface), you are required to define the following three static interfaces:

- Controller management—This interface/IP is used for communications with other controllers in the network. It is also the interface used to terminate EoIP tunnels that originate from the foreign controllers.
- AP manager interface—Even though the controller is not used to manage APs, you are still required to configure this interface. Cisco recommends the AP manager interface be configured on the same VLAN and subnet as the management interface.
- Virtual interface—The controller quickstart installation documentation recommends defining the virtual IP with an address, such as 192.0.2.1. This address needs to be the same for all controllers that are members of the same mobility group name. The virtual interface is also used as the source IP address when the controller redirects clients for web authentication.

Guest VLAN Interface Configuration

The interfaces previously described are for operations and administrative functions associated with the controller. To implement a guest access service, another interface must be defined. This is the interface through which guest traffic is forwarded for routing to the Internet. As previously described in Anchor Controller Positioning, the guest interface will likely connect to a port on a firewall or be switched to an interface on an Internet border router.

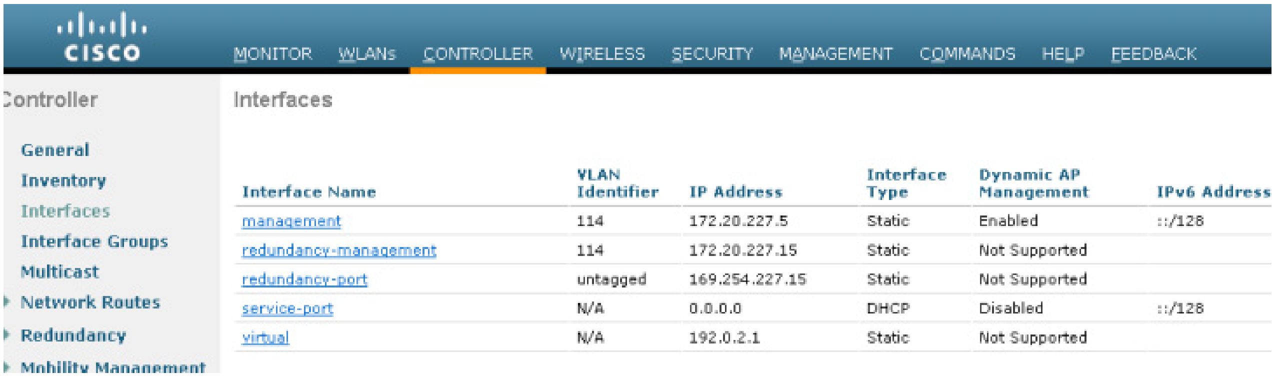
Defining a New Interface

Perform the following to define and configure an interface to support guest traffic:

Step 1 Click the **Controller** tab.

Step 2 In the left pane, click **Interfaces** (See Figure 10-8).

Figure 10-8 Controller Interfaces



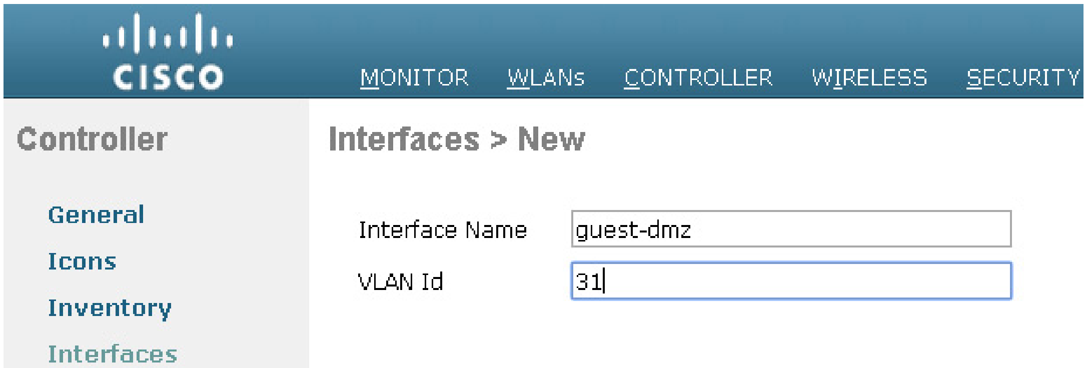
Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	114	172.20.227.5	Static	Enabled	::/128
redundancy-management	114	172.20.227.15	Static	Not Supported	
redundancy-port	untagged	169.254.227.15	Static	Not Supported	
service-port	N/A	0.0.0.0	DHCP	Disabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

Step 3 Click **New**.

Step 4 Enter an interface name and VLAN ID. (See Figure 10-9).

Figure 10-9 Interface Name and VLAN ID



Interfaces > New

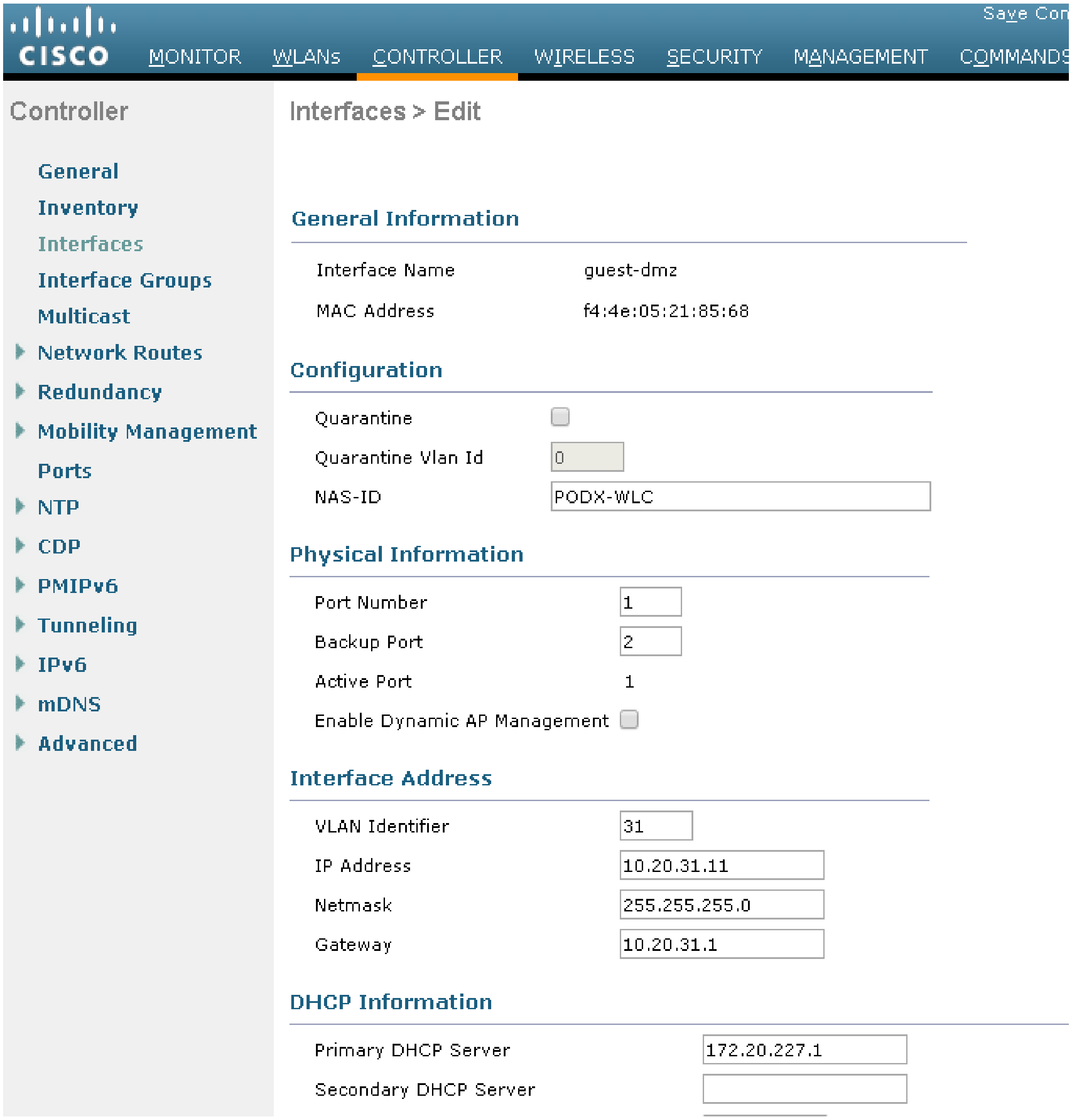
Interface Name: guest-dmz

VLAN Id: 31

Step 5 Define the following properties:

- Interface IP
- Mask
- Gateway (for the firewall or next hop router connected to the anchor controller)
- DHCP Server IP (If using an external DHCP server, use the IP address of that server in the Primary DHCP Server field.). See Figure 10-10.

Figure 10-10 Defining Interface Properties



Interfaces > Edit

General Information

Interface Name guest-dmz
MAC Address f4:4e:05:21:85:68

Configuration

Quarantine ☐
Quarantine Vlan Id 0
NAS-ID PODX-WLC

Physical Information

Port Number 1
Backup Port 2
Active Port 1
Enable Dynamic AP Management ☐

Interface Address

VLAN Identifier 31
IP Address 10.20.31.11
Netmask 255.255.255.0
Gateway 10.20.31.1

DHCP Information

Primary DHCP Server 172.20.227.1
Secondary DHCP Server

Note Internal DHCP server is not recommended but if DHCP services are to be implemented locally on the anchor controller, populate the primary DHCP server field with the management IP address of the controller. Review if internal DHCP server support is present on the controller platform. If guest N+1 redundancy is being implemented in the DMZ, repeat the above interface configuration for each additional anchor WLC being deployed.

Mobility Group Configuration

The following default mobility group parameters should already be defined on the foreign WLC(s) as part of a standard centralized WLAN deployment. To support auto-anchor mobility for guest access, the anchor WLC(s) must also be configured with a mobility group domain name.

Defining the Default Mobility Domain Name for the Anchor WLC

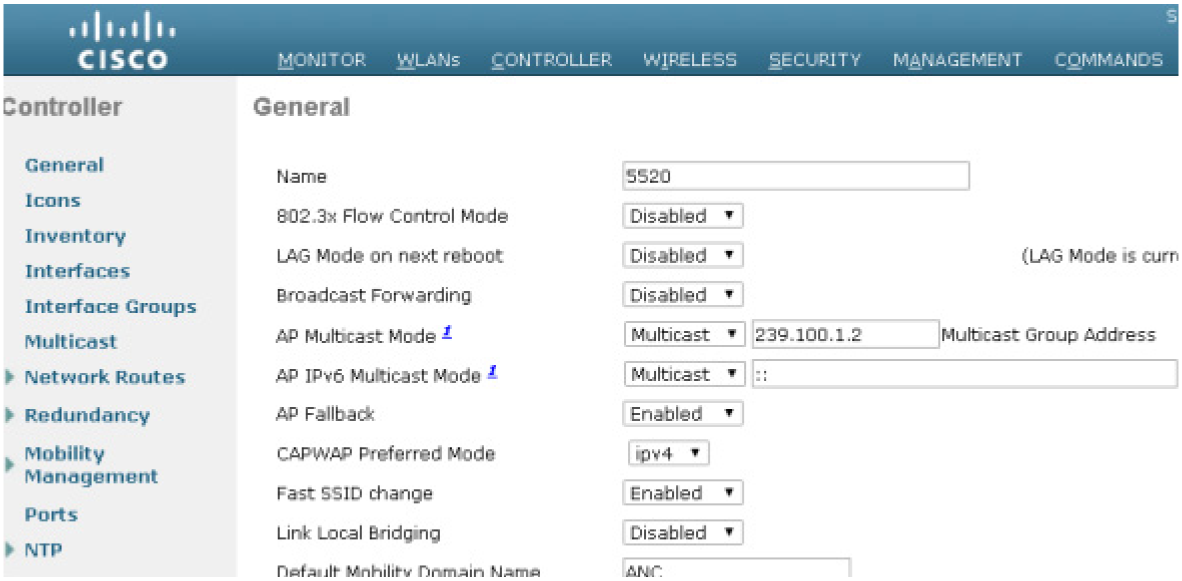
Configure a default mobility domain name for the anchor WLC. The anchor's mobility domain name should be different than what is configured for the foreign WLCs. In the examples below, the WLCs (foreign controllers) associated with the enterprise wireless deployment are all members of mobility group 'SRND'. The guest anchor WLC on the other hand, is configured with a different mobility group name: "ANC". This is done to keep the anchor WLC logically separate from the primary mobility domain associated with the enterprise wireless deployment.

Step 1 Click the **Controller** tab.

Step 2 Enter a name in the **Default Mobility Domain Name** field.

Step 3 Click **Apply**. (See Figure 10-11.)

Figure 10-11 Defining a Default Mobility Domain Name on the Anchor WLC



General

Name	5520	
802.3x Flow Control Mode	Disabled	
LAG Mode on next reboot	Disabled	(LAG Mode is curr
Broadcast Forwarding	Disabled	
AP Multicast Mode [1]	Multicast	239.100.1.2 Multicast Group Address
AP IPv6 Multicast Mode [1]	Multicast	::
AP Fallback	Enabled	
CAPWAP Preferred Mode	ipv4	
Fast SSID change	Enabled	
Link Local Bridging	Disabled	
Default Mobility Domain Name	ANC	

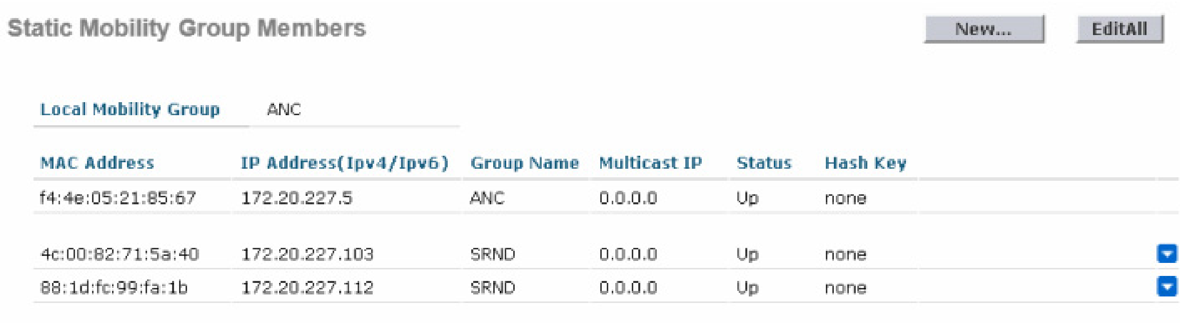
Defining Mobility Group Members of the Anchor WLC

Every foreign WLC within the enterprise deployment that is going to support the guest WLAN must be defined as a mobility group member in the guest anchor WLC(s).

Step 1 Click the **Controller** tab.

Step 2 In the left pane, click **Mobility Management** and then **Mobility Groups**. (See Figure 10-12.)

Figure 10-12 Defining Mobility Group Members



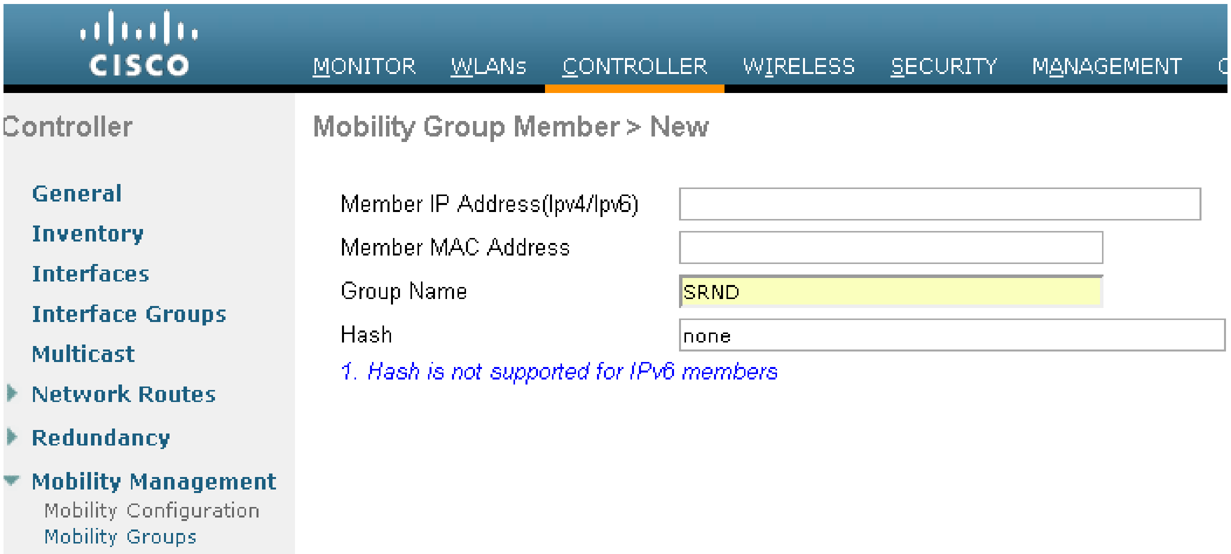
Static Mobility Group Members

Local Mobility Group: ANC

MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key
f4:4e:05:21:85:67	172.20.227.5	ANC	0.0.0.0	Up	none
4c:00:82:71:5a:40	172.20.227.103	SRND	0.0.0.0	Up	none
88:1d:fc:99:fa:1b	172.20.227.112	SRND	0.0.0.0	Up	none

Step 3 Click **New** to define a MAC and IP address for each foreign controller that will support the guest access WLAN. (See Figure 10-13.)

Figure 10-13 Adding Foreign Controllers to Anchor WLC



Mobility Group Member > New

Member IP Address(Ipv4/Ipv6):
Member MAC Address:
Group Name: SRND
Hash: none

1. Hash is not supported for IPv6 members

Note The "Group Name" in Figure 10-13 above is the name configured under the foreign WLC's 'Default Mobility Domain Name', which should be different than the name used by the anchor WLC. The member IP and MAC address are those addresses associated with the management interface of the foreign WLCs. Repeat the above steps for each additional foreign WLC that will support the guest WLAN. If more than one anchor is being deployed (guest anchor redundancy), then repeat the steps in Defining the Default Mobility Domain Name for the Anchor WLC and Defining Mobility Group Members of the Anchor WLC.

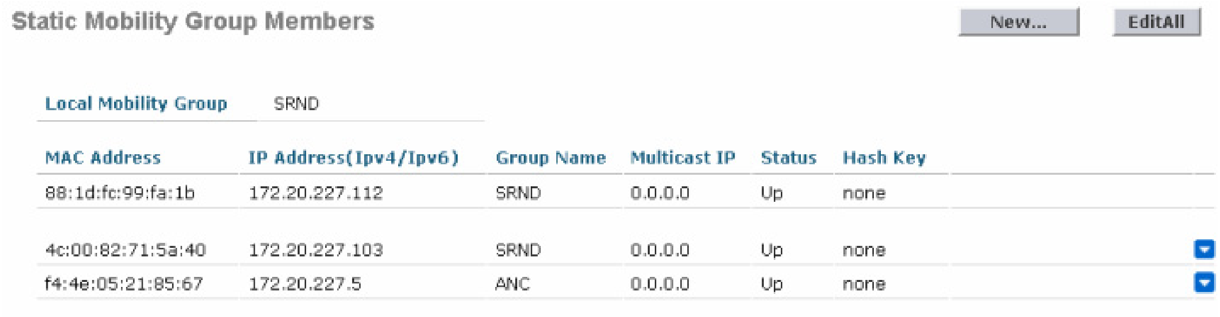
Adding the Anchor WLC as a Mobility Group Member of a Foreign WLC

As described in Auto Anchor Mobility to Support Wireless Guest Access, each foreign WLC maps the guest WLAN into an EoIP tunnel that terminates on the anchor WLC. Therefore, the anchor WLC(s) must be defined as a mobility group member in each foreign controller. In the example below, note that the group name entry for the anchor WLC is 'ANC' (see Defining Mobility Group Members of the Anchor WLC) whereas the other WLCs that comprise the enterprise wireless deployment are members of the mobility group: 'SRND'.

Step 1 Click **New** to add the anchor WLC's IP, MAC address, and Group Name to the mobility members table.

Step 2 Repeat these steps for each additional foreign controller. (See Figure 10-14.)

Figure 10-14 Adding Anchor Controller(s) to Foreign WLC



Local Mobility Group SRND

MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key
88:1d:fc:99:fa:1b	172.20.227.112	SRND	0.0.0.0	Up	none
4c:00:82:71:5a:40	172.20.227.103	SRND	0.0.0.0	Up	none
f4:4e:05:21:85:67	172.20.227.5	ANC	0.0.0.0	Up	none

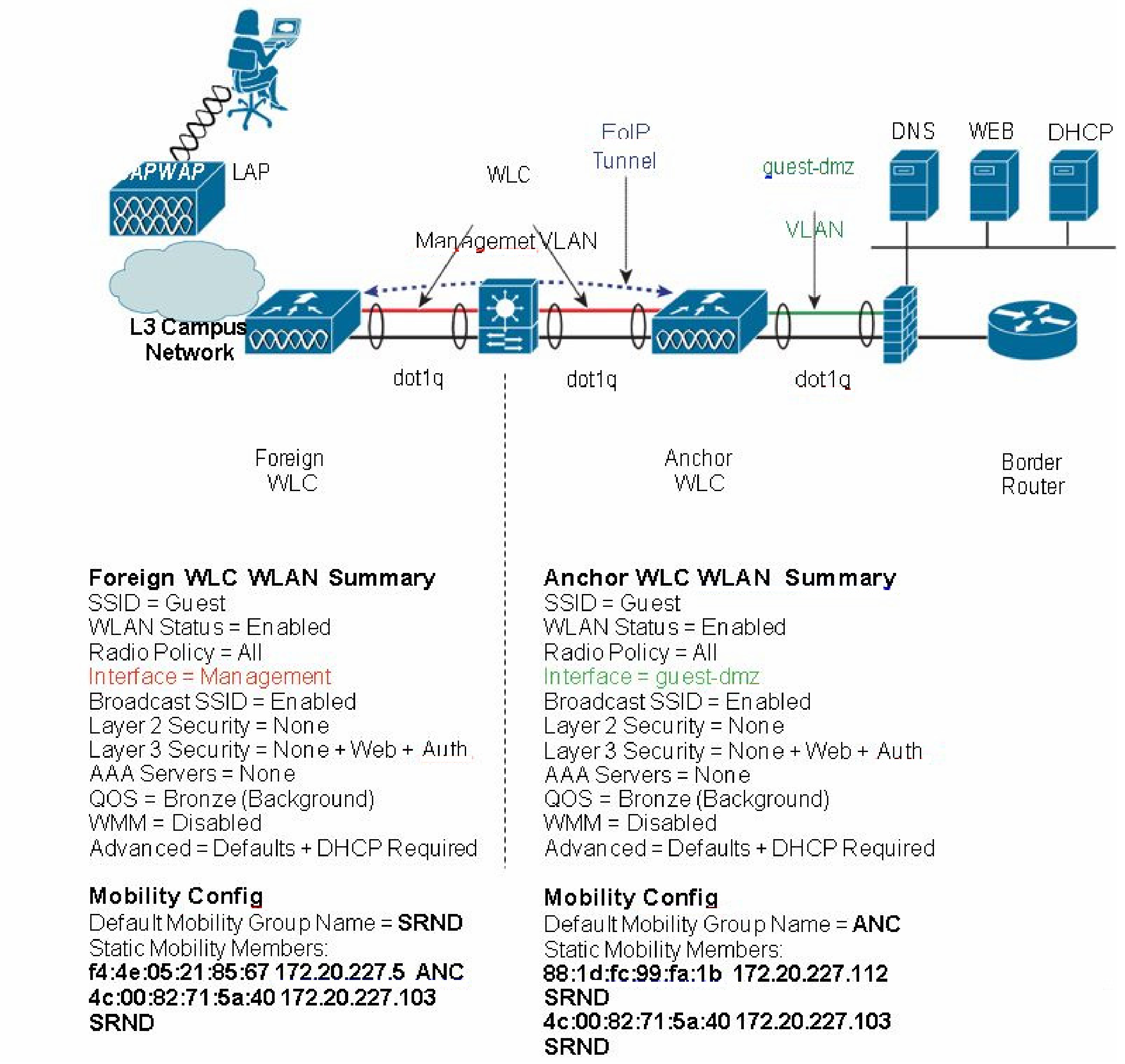
Note If guest anchor redundancy capability is being deployed, two or more anchor WLC entries are added to each foreign WLC's Mobility Group Members list.

Guest WLAN Configuration

The following section describes how to configure a single guest WLAN. The guest WLAN is configured on every foreign WLC that manages APs where guest access is required. Even though the anchor WLC(s) is not specifically used to manage LAPs associated with a guest WLAN, it must also be configured with the guest WLAN because the anchor WLC is a logical extension of the WLAN where user traffic is ultimately bridged (using CAPWAP between the AP and the foreign controller, and EoIP between the foreign controller and the anchor controller) to an interface/VLAN on the anchor WLC.

Note It is extremely important to note that all parameters defined in the WLAN Security, QoS, and Advanced settings tabs, must be configured identically in both the anchor and foreign WLC(s). Figure 10-15 shows a high level diagram illustrating the WLAN configuration discussed below.

Figure 10-15 WLAN Configuration



Foreign WLC WLAN Summary
SSID = Guest
WLAN Status = Enabled
Radio Policy = All
Interface = Management
Broadcast SSID = Enabled
Layer 2 Security = None
Layer 3 Security = None + Web + Auth
AAA Servers = None
QOS = Bronze (Background)
WMM = Disabled
Advanced = Defaults + DHCP Required

Mobility Config
Default Mobility Group Name = **SRND**
Static Mobility Members:
f4:4e:05:21:85:67 172.20.227.5 ANC
4c:00:82:71:5a:40 172.20.227.103
SRND

Anchor WLC WLAN Summary
SSID = Guest
WLAN Status = Enabled
Radio Policy = All
Interface = guest-dmz
Broadcast SSID = Enabled
Layer 2 Security = None
Layer 3 Security = None + Web + Auth
AAA Servers = None
QOS = Bronze (Background)
WMM = Disabled
Advanced = Defaults + DHCP Required

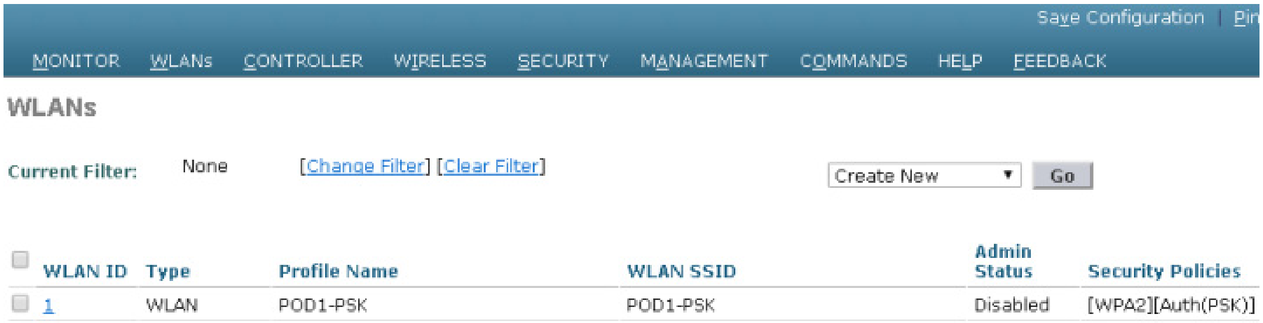
Mobility Config
Default Mobility Group Name = **ANC**
Static Mobility Members:
88:1d:fc:99:fa:1b 172.20.227.112
SRND
4c:00:82:71:5a:40 172.20.227.103
SRND

Note The parameters defined in the WLAN Security, QoS, and Advanced settings tabs, must be configured identically in both the anchor and foreign controller(s).

Foreign WLC-Guest WLAN Configuration

Step 1 Click the **WLANs** tab and then click **New**. (See Figure 10-16.)

Figure 10-16 Guest WLAN Configuration


Save Configuration | Pin
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
Current Filter: None [Change Filter] [Clear Filter]
Create New
Go

☐	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
☐	1	WLAN	POD1-PSK	POD1-PSK	Disabled	[WPA2][Auth(PSK)]

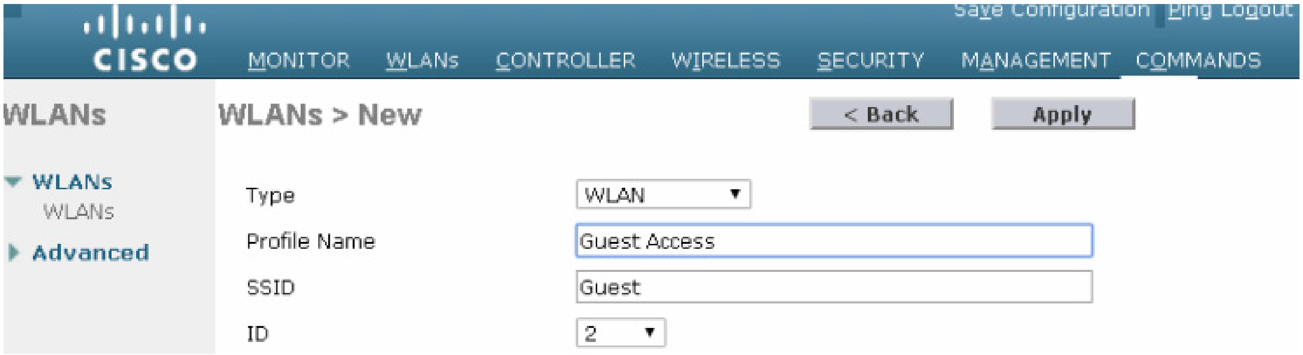
Step 2 Define an SSID that is intuitive or easily recognized by potential guest users.

The controller automatically assigns a VLAN ID. Administrators have the option of selecting 1 - 16, as long as the ID is not already in use by another SSID/ WLAN.

Step 3 Define a Profile Name.

Step 4 Click **Apply**. (See Figure 10-17.)

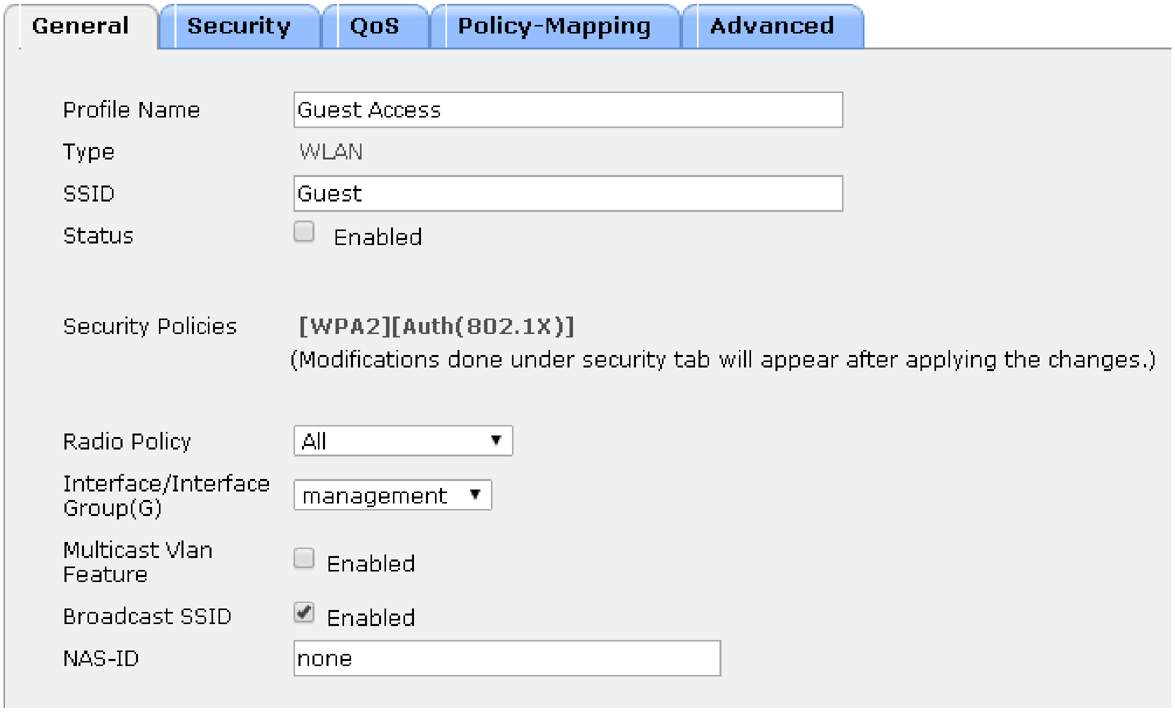
Figure 10-17 Defining a Guest WLAN SSID


Save Configuration Ping Logout
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS
WLANs
WLANs > New
< Back
Apply
WLANs
WLANs
Advanced

Type: WLAN
Profile Name: Guest Access
SSID: Guest
ID: 2

After creation of the new WLAN, the configuration page appears, as shown in Figure 10-18.

Figure 10-18 WLAN Configuration Page



Profile Name: Guest Access
Type: WLAN
SSID: Guest
Status: ☐ Enabled
Security Policies: [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy: All
Interface/Interface Group(G): management
Multicast Vlan Feature: ☐ Enabled
Broadcast SSID: ☑ Enabled
NAS-ID: none

Note The default interface used by the foreign WLC for the guest WLAN is the management interface. If the EoIP tunnel cannot be established with the anchor, the foreign controller will disassociate any wireless clients that were previously associated with the unreachable anchor and then assign new clients and reassociate clients to the interface configured under the guest WLAN of the foreign itself. Therefore, it is recommended to link the guest WLAN on the foreign to a non-routable network, or alternatively configure the DHCP server of the management interface with an unreachable IP address. If the anchor becomes unreachable, this prevents the guest clients to gain access to the management network.

Defining Guest WLAN Parameters and Policies

Under the **General Configuration** tab, perform the following steps:

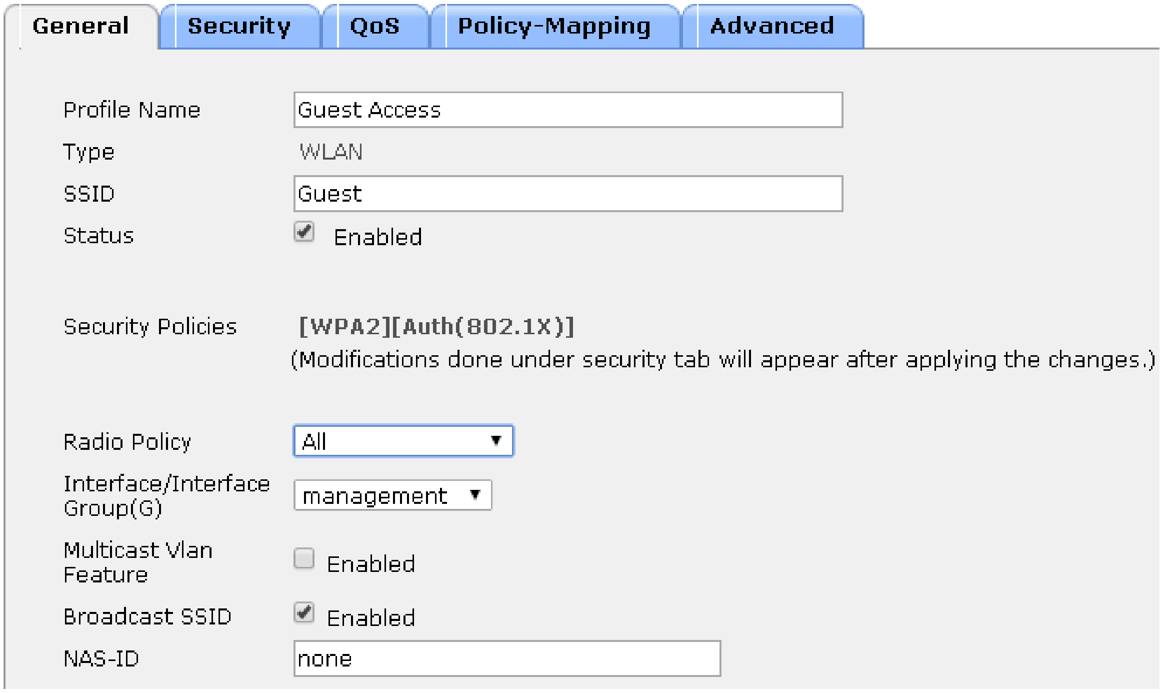
Step 1 Enable the WLAN by clicking the box next to **WLAN Status**.

Step 2 Optionally, set the radio policy if you wish to restrict which bands support the guest access.

- Broadcast SSID is enabled by default; leave enabled.
- By default, the WLAN is assigned to the "management" interface of the WLC. Do not change this.

Step 3 Click the **Security** tab. (See Figure 10-19.)

Figure 10-19 Defining Guest WLAN General Policies



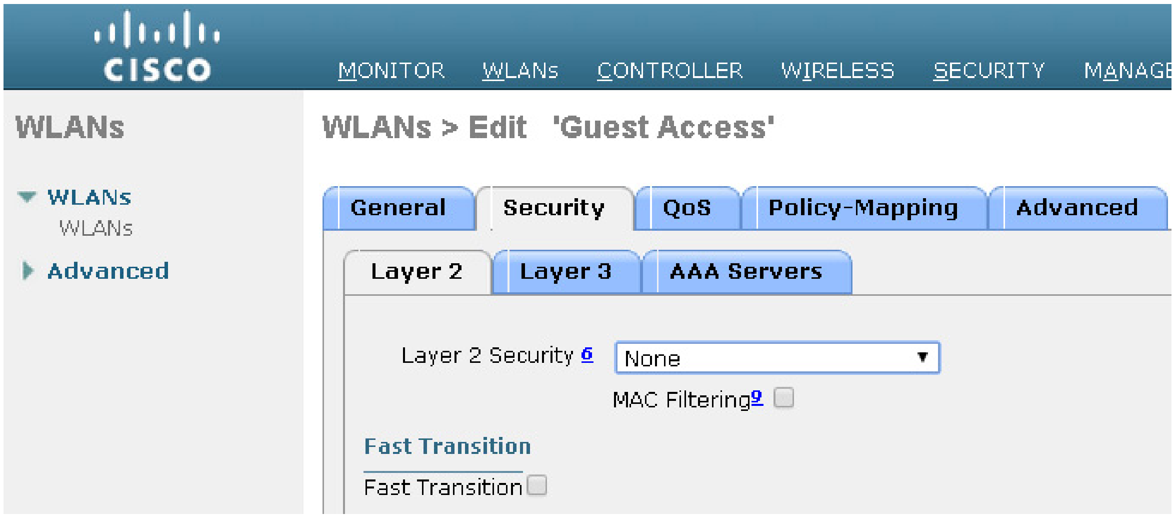
Profile Name: Guest Access
Type: WLAN
SSID: Guest
Status: ☑ Enabled

Security Policies: [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All
Interface/Interface Group(G): management
Multicast Vlan Feature: ☐ Enabled
Broadcast SSID: ☑ Enabled
NAS-ID: none

Step 4 Set the Layer 2 Security to **none** from its default setting (802.1x WPA/WPA2). (See Figure 10-20.)

Figure 10-20 WLAN Layer 2 Security Configuration



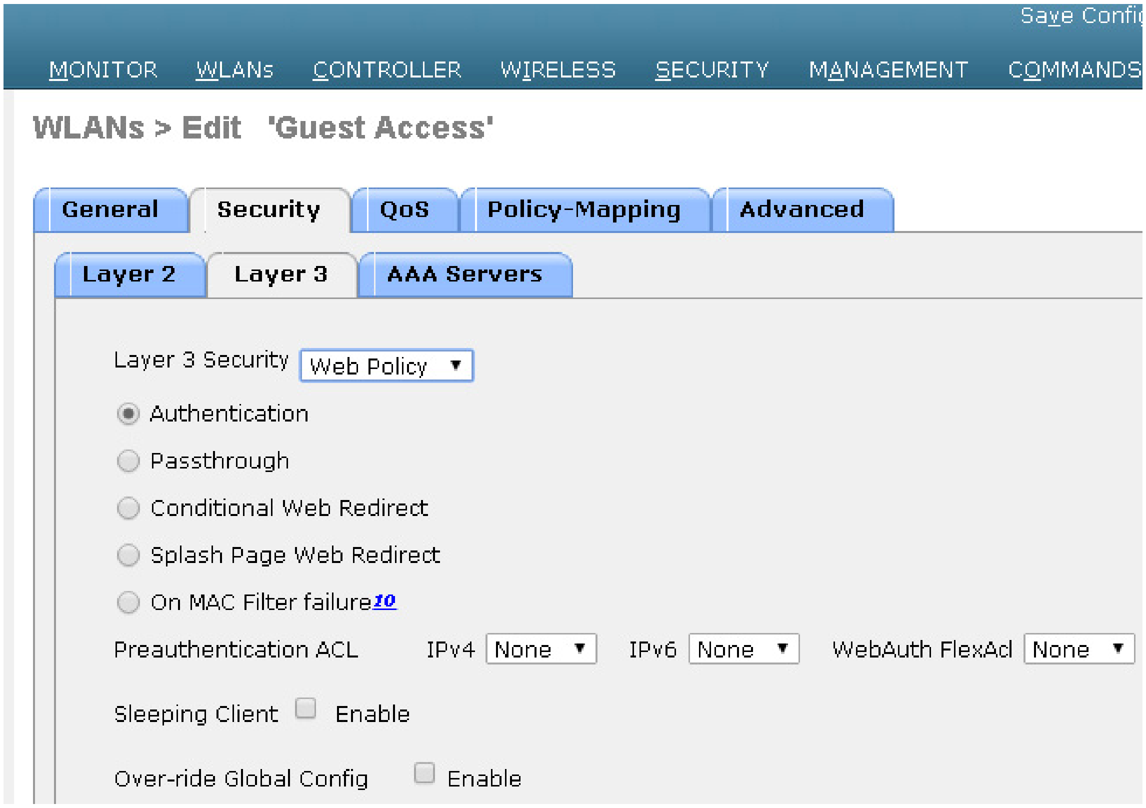
WLANs > Edit 'Guest Access'

Layer 2 Security 6: None
MAC Filtering9 ☐

Fast Transition
Fast Transition ☐

Step 5 Click the **Layer 3** tab. (See Figure 10-22.)

Figure 10-21 WLAN Layer 2 Security Configuration



WLANs > Edit 'Guest Access'

Layer 3 Security: Web Policy

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

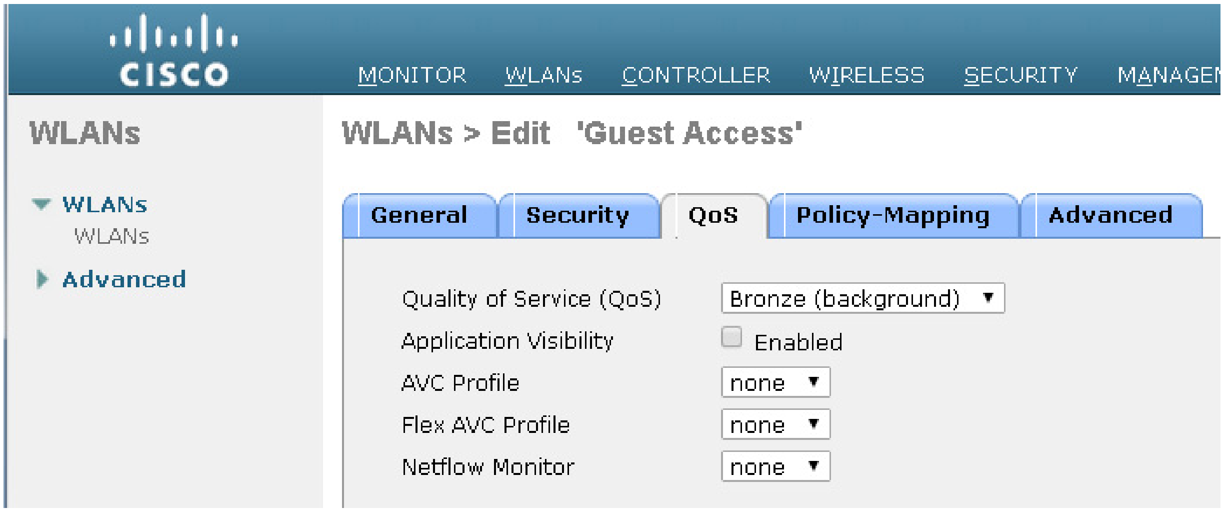
○ On MAC Filter failure10

Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None

Sleeping Client ☐ Enable

Over-ride Global Config ☐ Enable

Figure 10-22 Guest WLAN Layer 3 Security Configuration



WLANs > Edit 'Guest Access'

Quality of Service (QoS): Bronze (background)

Application Visibility ☐ Enabled

AVC Profile: none

Flex AVC Profile: none

Netflow Monitor: none

Step 6 Click the **Web Policy** check box (a list of additional options will be presented).

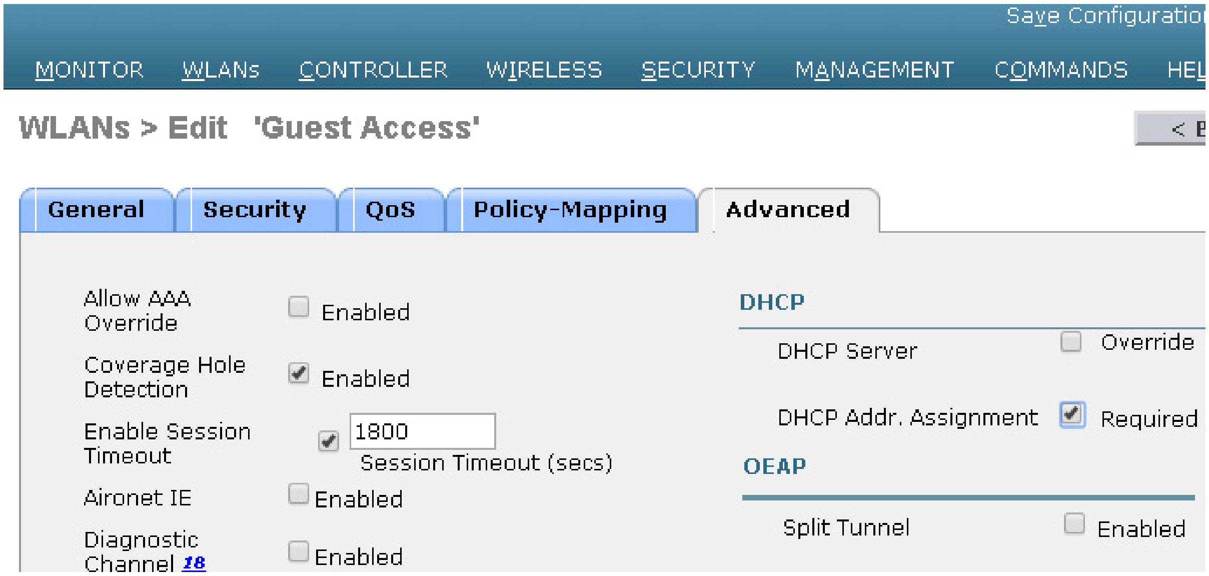
A dialog warning box appears, indicating that the WLC will pass DNS traffic to and from clients prior to authentication.

Step 7 Select **Authentication** or **Pass-through** for the web policy. (See Guest User Authentication).

Note A pre-authentication ACL can be used to apply an ACL that allows un-authenticated clients to connect to specific hosts or URL destinations before authentication. The ACL is configured under Security > Access Control Lists. If a pre-authentication ACL is used in conjunction with the web auth policy, it must include a rule to permit DNS requests; otherwise, the client will be unable to resolve and connect to a destination host/URL that would otherwise be allowed by the ACL.

Step 8 Select the **QoS** tab, as shown in Figure 10-23.

Figure 10-23 Guest WLAN QoS Configuration



WLANs > Edit 'Guest Access'

Allow AAA Override ☐ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE ☐ Enabled

Diagnostic Channel 18 ☐ Enabled

DHCP

DHCP Server ☐ Override

DHCP Addr. Assignment ☑ Required

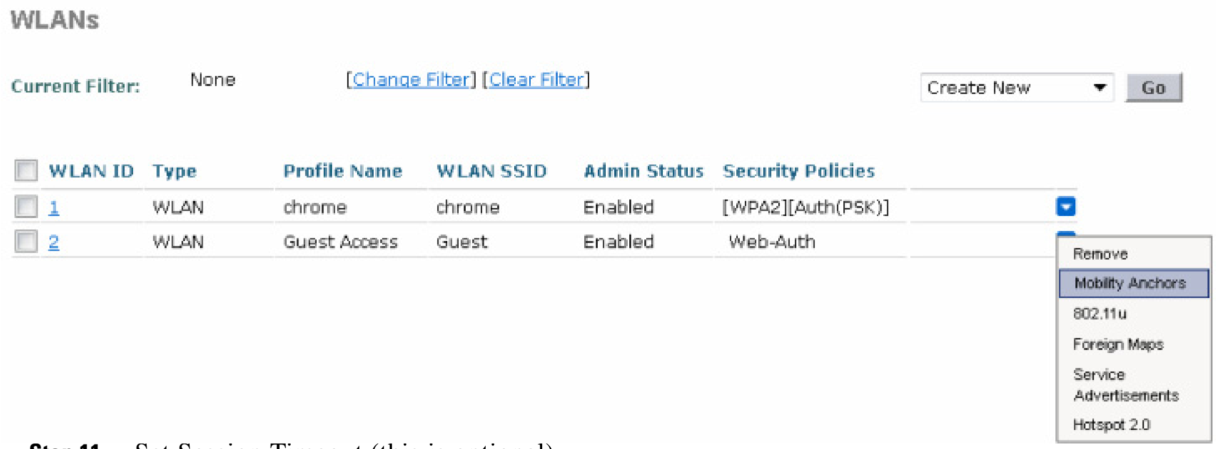
OEAP

Split Tunnel ☐ Enabled

Step 9 Optionally, set the upstream QoS profile for the guest WLAN. The default is 'Silver (Best Effort)'. In this example, the guest WLAN has been re-assigned to the lowest QoS class.

Step 10 Click the **Advanced** tab. (See Figure 10-24.)

Figure 10-24 Guest WLAN Advanced Configuration



WLANs

Current Filter: None

☐	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
☐	1	WLAN	chrome	chrome	Enabled	[WPA2][Auth(PSK)]
☐	2	WLAN	Guest Access	Guest	Enabled	Web-Auth

Step 11 Set Session Timeout (this is optional).

Note Any session timeout greater than 0 (default) forces de-authentication after expiration, and requires the user to re-authenticate through the web portal.

Step 12 Set DHCP Addr. Assignment to "Required".

Note Setting DHCP Addr. Assignment to "Required" is recommended to prevent guest users from attempting to use the guest network using a static IP configurations.

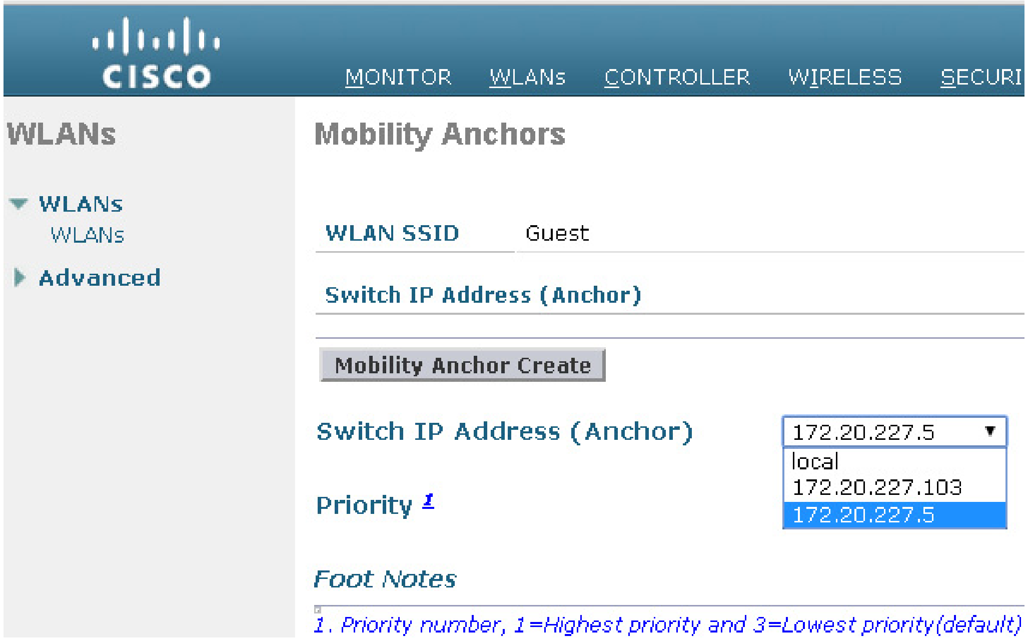
Step 13 Click **Apply** when finished.

Establishing the Guest WLAN Mobility Anchor(s)

Step 1 From the WLAN menu on the foreign WLC find the newly created guest WLAN.

Step 2 Highlight and click **Mobility Anchors** from the right-hand pull-down selection list. (See Figure 10-25.)

Figure 10-25 WLAN Mobility Anchor



WLAN SSID Guest

Switch IP Address (Anchor)

Switch IP Address (Anchor) 172.20.227.5

Priority [1]

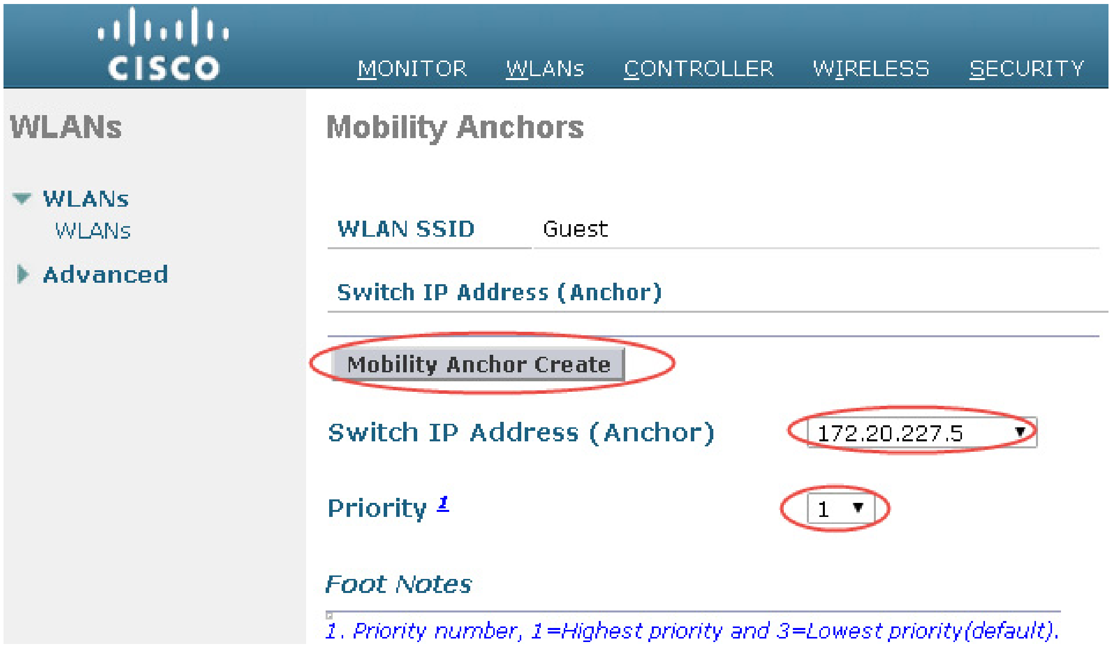
1. Priority number, 1=Highest priority and 3=Lowest priority(default)

Step 3 In the Switch IP Address (Anchor) pull-down selection list, select the IP address corresponding to the management interface of the anchor WLC deployed in the network DMZ. This is the same IP address configured in Adding the Anchor WLC as a Mobility Group Member of a Foreign WLC.

Step 4 In the Priority field, select a priority number for the anchor WLC (applicable if there are more than one anchor WLCs configured).

Step 5 Click **Mobility Anchor Create**. (See Figure 10-27.)

Figure 10-26 Selecting Management Interface from Switch IP Address (Anchor)



Mobility Anchors

WLAN SSID Guest

Switch IP Address (Anchor)

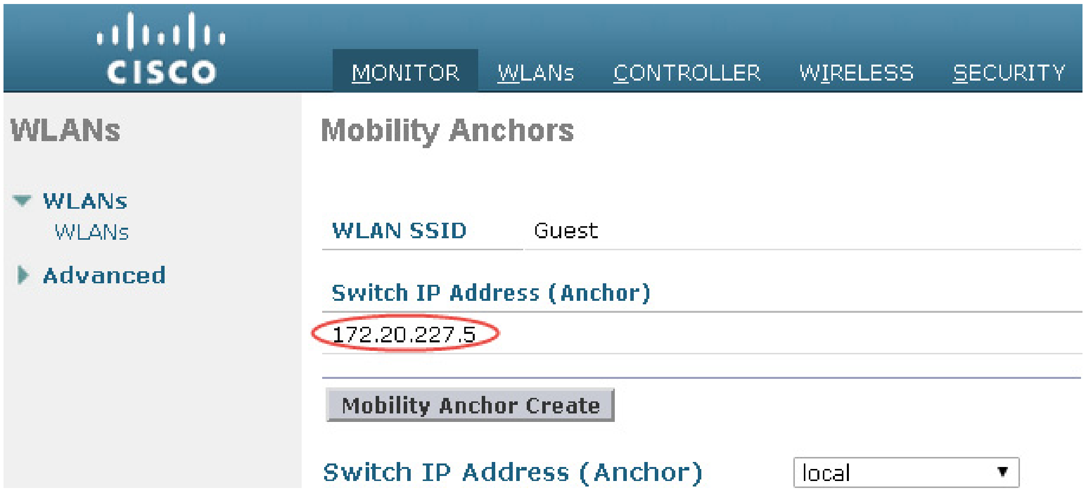
Switch IP Address (Anchor) 172.20.227.5

Priority [1] 1

Foot Notes

1. Priority number, 1=Highest priority and 3=Lowest priority(default).

Figure 10-27 Selecting WLAN Mobility Anchor



Mobility Anchors

WLAN SSID Guest

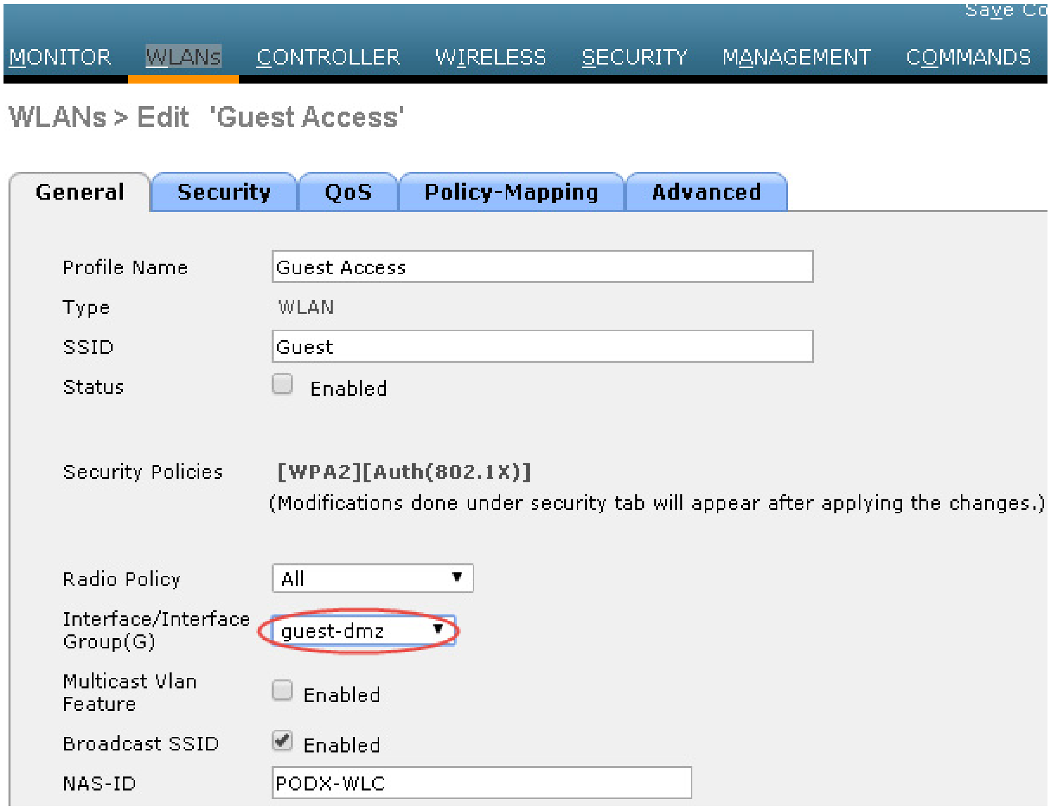
Switch IP Address (Anchor)

172.20.227.5

Switch IP Address (Anchor) local

Once configured, the screen shown in Figure 10-28 shows the mobility anchor (selected from above), assigned to the Guest WLAN.

Figure 10-28 Verifying the Guest WLAN Mobility Anchor



WLANs > Edit 'Guest Access'

Profile Name	Guest Access
Type	WLAN
SSID	Guest
Status	☐ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	guest-dmz
Multicast Vlan Feature	☐ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	PODX-WLC

For ease of verification, the page displays whether or not the mobility tunnel data path and CAPWAP control path have been established with the anchor. The pull-down selection list to the right offers the option to send a ping to the destination anchor WLC.

Step 6 When finished, click **Back**.

Step 7 Repeat the steps above for each additional anchor WLC being deployed (guest anchor redundancy).

This completes the guest WLAN configuration. Repeat all steps from Foreign WLC-Guest WLAN Configuration through Establishing the Guest WLAN Mobility Anchor(s) for each additional foreign WLC that will support the guest WLAN.

Guest WLAN Configuration on the Anchor WLC

Guest WLAN configuration on the anchor controller(s) is identical to that of the foreign controller except for minor differences in the WLAN interface and mobility anchor configuration, which are detailed below.

Note The SSID defined for the guest WLAN must be exactly the same as what is defined on the foreign WLCs.

Anchor WLC-Guest WLAN Interface

As indicated above, the parameters configured for the guest WLAN on the anchor WLC are the same except the interface to which the WLAN is mapped. In this case, the guest WLAN is assigned to an interface/VLAN on the anchor WLC, which connects to an interface on a firewall or Internet border router.

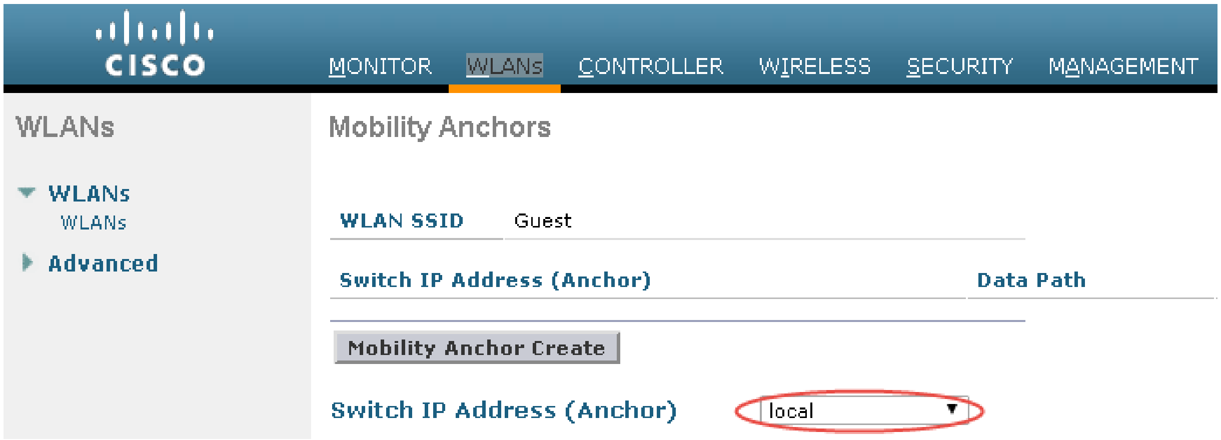
Step 1 Click the **WLANs** tab.

Step 2 Create, configure, and enable the guest WLAN the same way it was configured on the foreign WLC(s) except for the following:

In the WLANs general configuration, under Interface, choose the interface name created in Guest VLAN Interface Configuration. (See Figure 10-29.)

Step 3 Click **Apply**.

Figure 10-29 Anchor WLC Guest WLAN Interface Configuration



WLAN SSID Guest

Switch IP Address (Anchor) local

Anchor WLC-Defining the Guest WLAN Mobility Anchor

The second parameter that differs in configuration from the foreign WLC is the WLAN mobility anchor configuration. The guest WLAN mobility anchor is the anchor WLC itself.

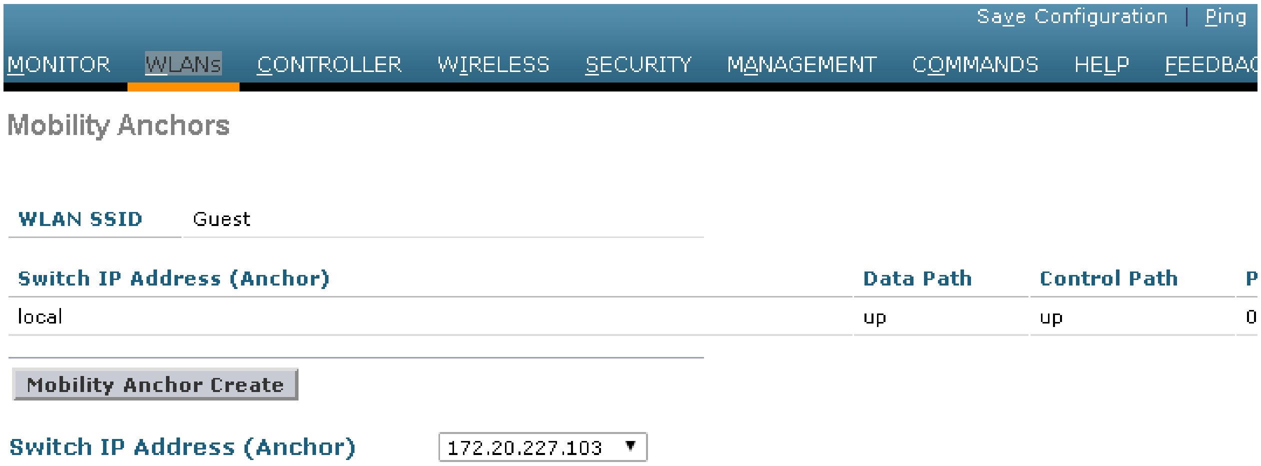
Step 1 Click the **WLANs** tab.

Step 2 Find the Guest WLAN and click **Mobility Anchors**.

Step 3 From the pull-down selection list, choose the IP address representing the anchor controller. The IP address has (Local) next to it.

Step 4 Click **Mobility Anchor Create**. (See Figure 10-30.)

Figure 10-30 Defining the Guest WLAN Mobility Anchor



Mobility Anchors

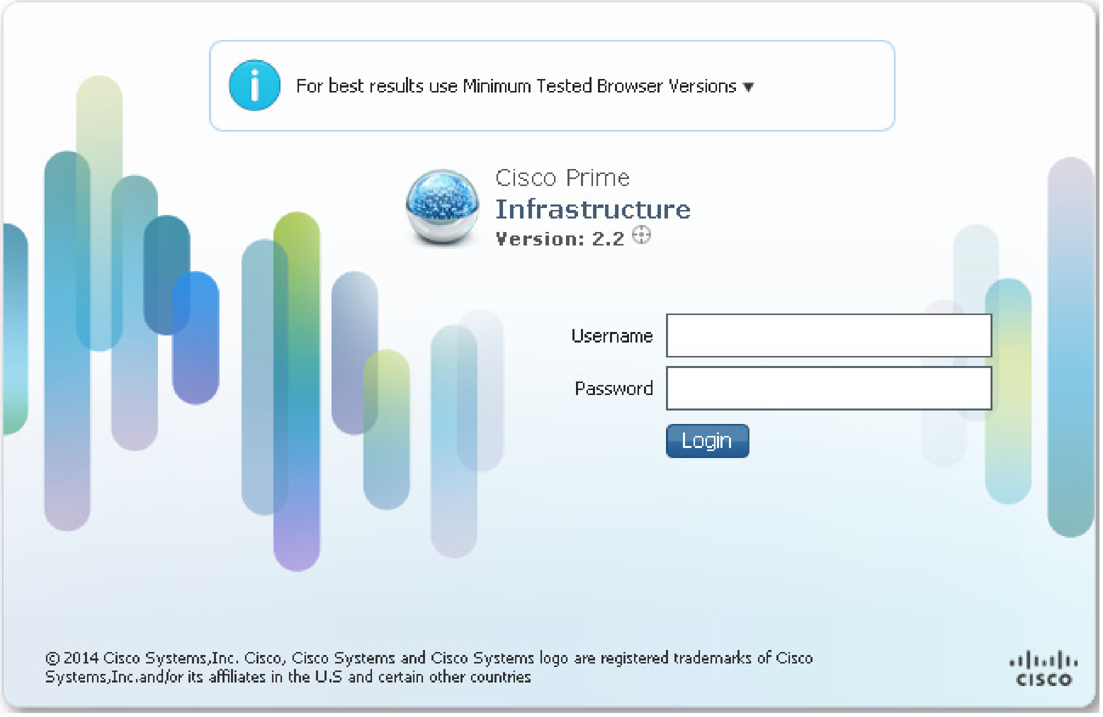
WLAN SSID: Guest

Switch IP Address (Anchor)	Data Path	Control Path	P
local	up	up	0

Switch IP Address (Anchor): 172.20.227.103

Note The guest WLAN mobility anchor is *local*. (See Figure 10-31.)

Figure 10-31 Verifying Guest Mobility Anchor


For best results use Minimum Tested Browser Versions ▾

Cisco Prime
Infrastructure
Version: 2.2

Username
Password

© 2014 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc.and/or its affiliates in the U.S and certain other countries

Because the mobility anchor for the guest WLAN is the anchor WLC itself, the Data and Control Path status will always show "up". If not, check to ensure that you have selected the local WLC as the anchor from the 'Switch IP Address (Anchor) drop down menu. Anchor controller will always have priority 0 for the ssid.

Step 5 If guest anchor redundancy is being implemented; repeat the WLAN configuration for each additional anchor WLC being deployed. Otherwise, this completes the configuration steps required to create the guest WLAN on the anchor WLC.

Guest Account Management

If guest credentials are going to be managed locally on the anchor controller, there are two methods by which they can be created and applied:

- Through a lobby ambassador admin or super user/root admin account.
- Directly on the controller via a local lobby admin account or other management account with read/write access.

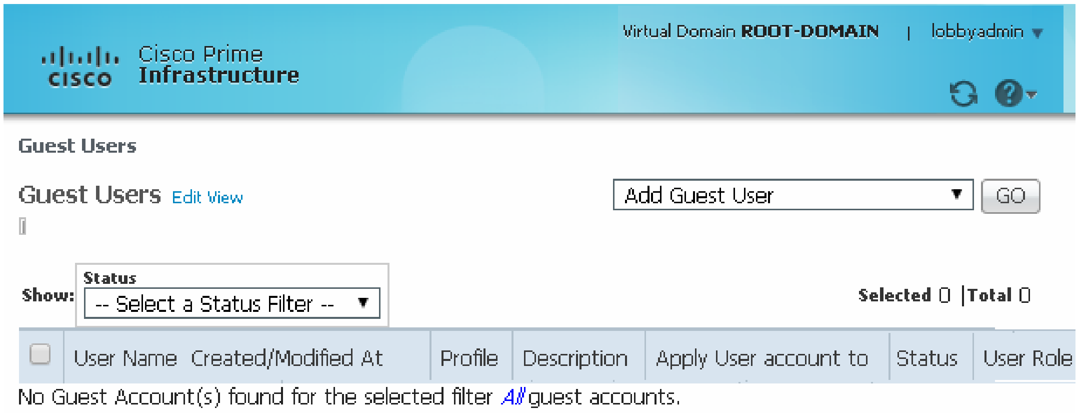
Guest Management Using the Management System

The following configuration examples assume the management system version 2.2 or later has been installed and configured, and a lobby ambassador account has been created.

Note Ensure that the individual WLC configurations are synchronized with the management system before creating guest templates.

Log in to the management system using the Lobby Ambassador credentials assigned by the system administrator. (See Figure 10-32.)

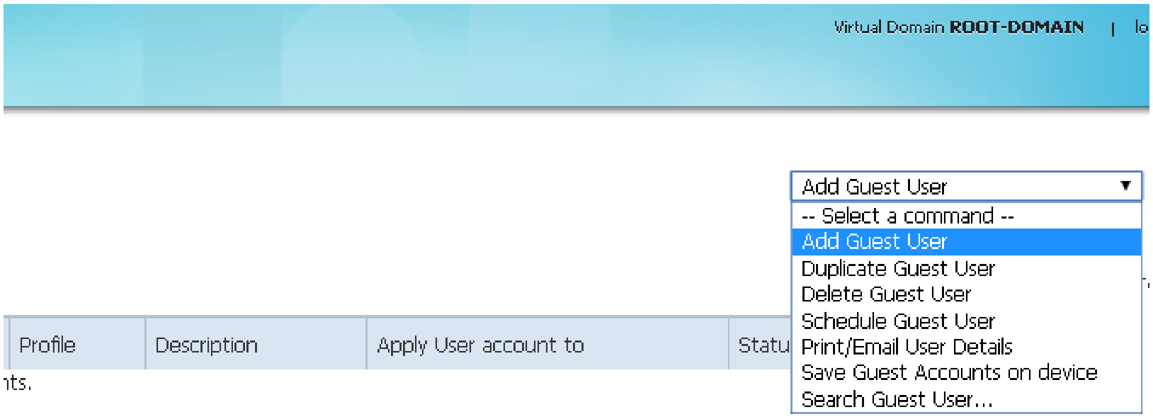
Figure 10-32 Lobby Ambassador



No Guest Account(s) found for the selected filter All guest accounts.

After logging in, the screen shown in Figure 10-33 appears.

Figure 10-33 Cisco Prime Infrastructure Lobby Admin Interface

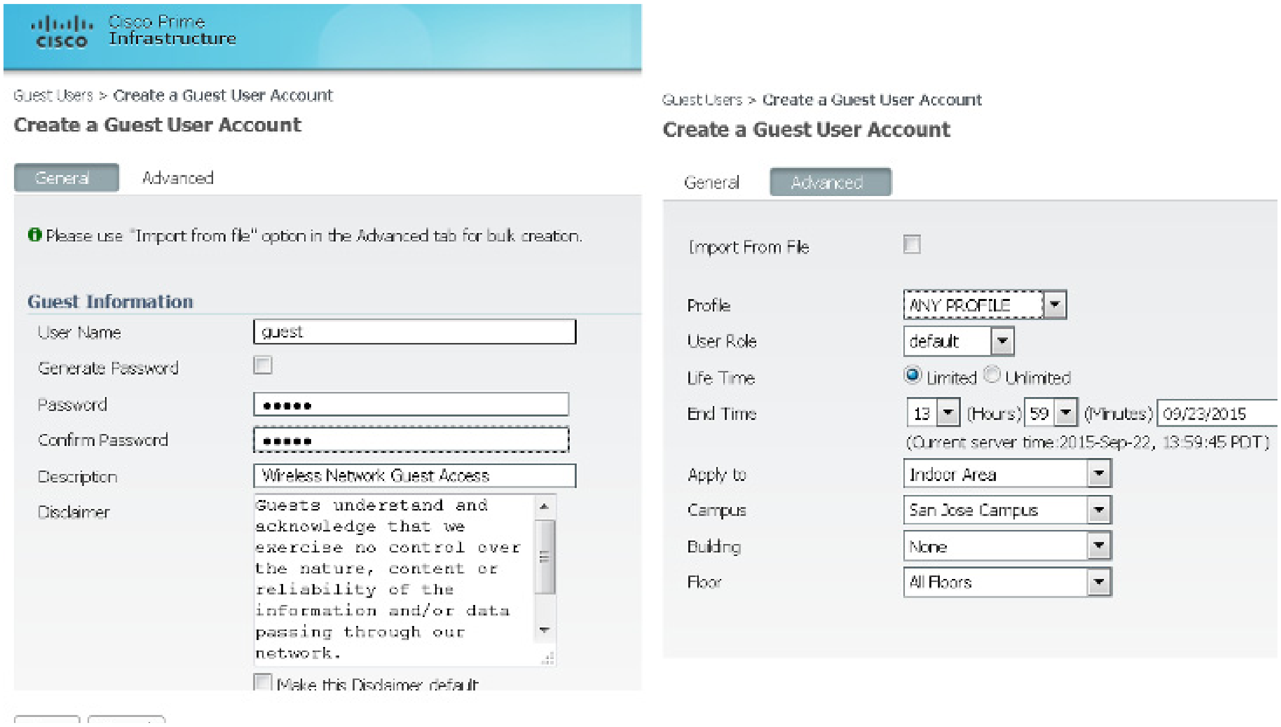


Note Cisco Prime Infrastructure was formally known as WCS and NCS.

There are two types of guest templates:

- The **Add Guest User** template allows administrators to create and immediately apply guest credentials to one or more anchor WLCs.
- The **Schedule Guest User** template allows administrators to create guest credentials that are applied to one or more anchor WLCs at some future month, day, and time. (See Figure 10-34.)

Figure 10-34 Guest User Template Option


Cisco Prime Infrastructure
Guest Users > Create a Guest User Account
General
Advanced

Create a Guest User Account

Please use "Import from file" option in the Advanced tab for bulk creation.

Guest Information

User Name	guest
Generate Password	☐
Password	•••••
Confirm Password	•••••
Description	Wireless Network Guest Access
Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.

☐ Make this Disclaimer default

Create a Guest User Account

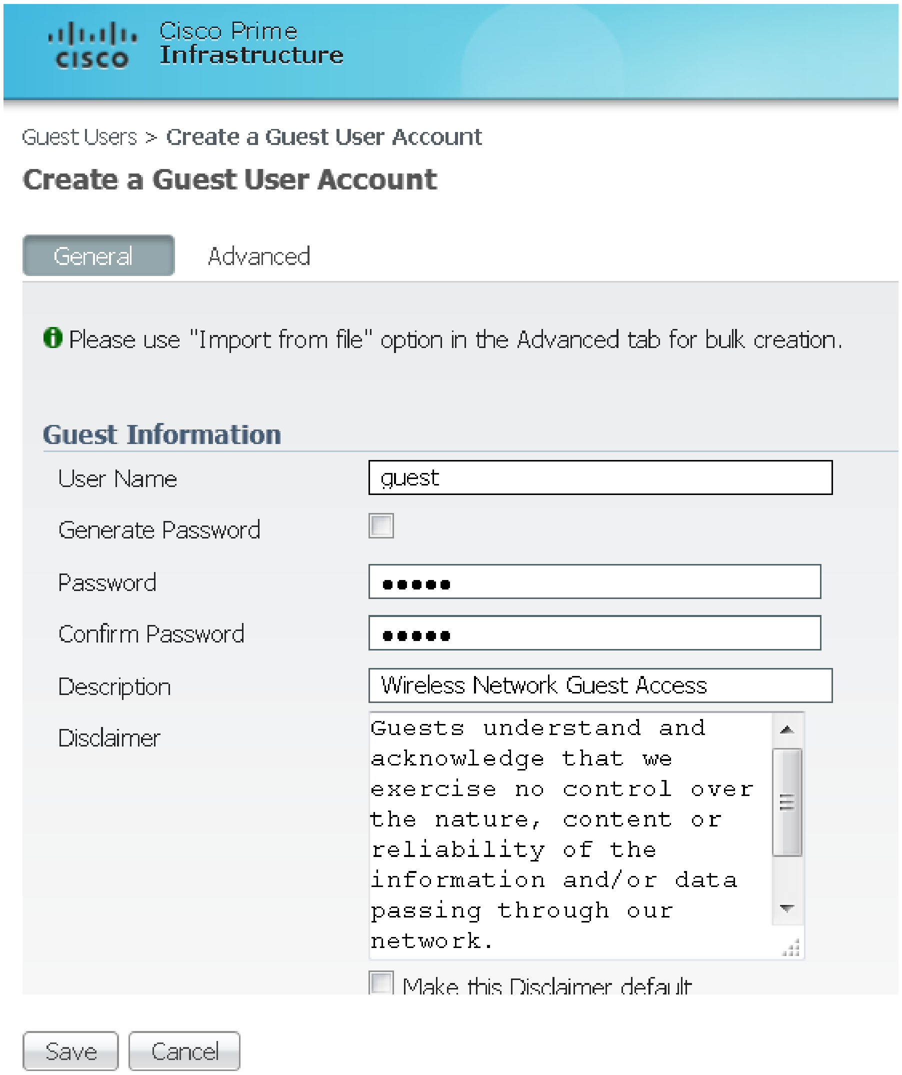
Import From File	☐
Profile	ANY PROFILE
User Role	default
Life Time	● Limited ○ Unlimited
End Time	13 (Hours) 59 (Minutes) 09/23/2015
	(Current server time:2015-Sep-22, 13:59:45 PDT)
Apply to	Indoor Area
Campus	San Jose Campus
Building	None
Floor	All Floors

Using the Add Guest User Template

Step 1 From the pull-down selection list, select **Add Guest User** and click **Go**.

Step 2 The template shown in Figure 10-35 appears.

Figure 10-35 Add Guest User Template


Cisco Prime Infrastructure
Guest Users > Create a Guest User Account

Create a Guest User Account

Please use "Import from file" option in the Advanced tab for bulk creation.

Guest Information

User Name: guest

Generate Password: ☐

Password: ●●●●●

Confirm Password: ●●●●●

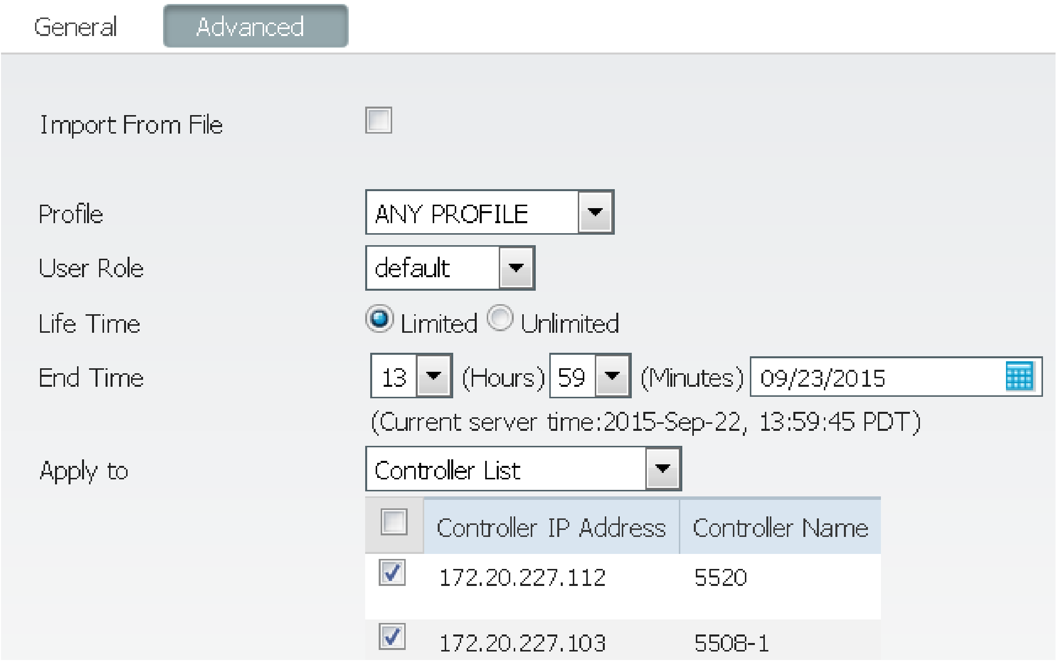
Description: Wireless Network Guest Access

Disclaimer: Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.

☐ Make this Disclaimer default

Figure 10-36 shows an example of guest user account creation.

Figure 10-36 Guest User Account Creation



Import From File ☐

Profile: ANY PROFILE

User Role: default

Life Time: ● Limited ○ Unlimited

End Time: 13 (Hours) 59 (Minutes) 09/23/2015

(Current server time:2015-Sep-22, 13:59:45 PDT)

Apply to: Controller List

☐	Controller IP Address	Controller Name
☑	172.20.227.112	5520
☑	172.20.227.103	5508-1

Step 3 Under **Guest Information**, enter a User Name and Password.

Passwords are case sensitive. User names are restricted to 24 characters or less. Administrators also have an option to allow the system to automatically generate a password by clicking on the **Generate Password** check box.

Step 4 Under **Account Configuration**, select the following:

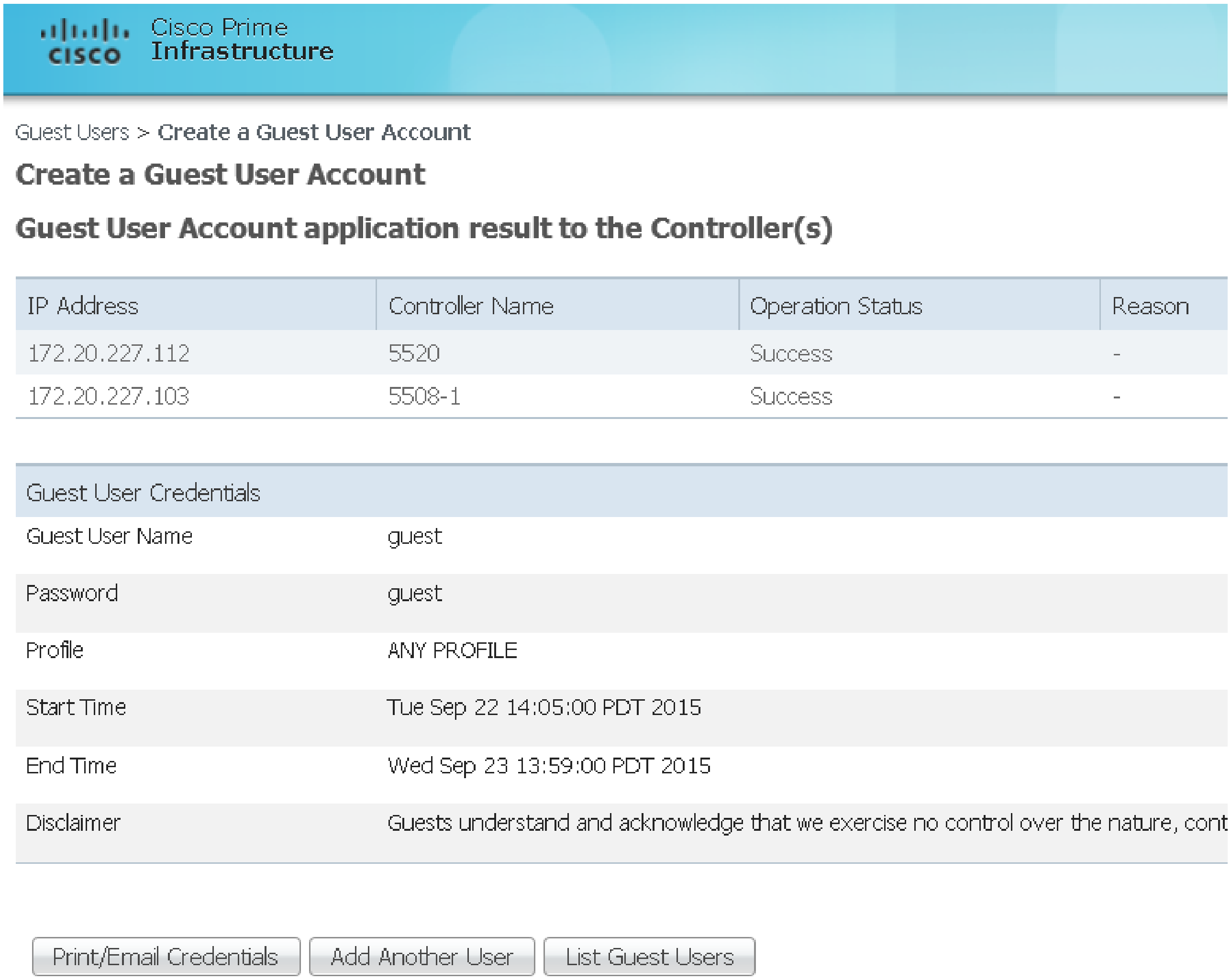
- **Profile**—The pull-down selection list displays a list of WLANs (SSIDs) configured with an L3 Web Policy.
- **User Role**—They are predefined by the administrator and are associated with the guests' access (such as contractor, customer, partner, vendor, visitor, and so on).
- **Life Time**—Select "limited" or "unlimited".
- **End Time**—If the guest account is "limited", select the month, day, and time the credentials are to expire.
- **Apply To**—From the pull-down selection list, select **Controller List** and click the check box next to the controller(s) representing anchor WLCs. Note that there will be other controllers listed; however, these represent the foreign WLCs. There is no need to apply user credentials on the foreign WLCs because the authentication enforcement point is the anchor WLC.

Note As seen in Figure 10-36, there are various options for where the credentials can be applied, including being able to control the physical/geographic location where a user can access the guest WLAN. These include outdoor areas, indoor areas, building, floor, and so on. This location-based access method can only be used if: 1) the WLAN deployment has been integrated into the management system mapping database, and 2) the guest WLAN (a WLAN with web policy) does not use mobility anchors.

- **Description**—Enter a description. The description is displayed on the WLC to which the credentials are applied under **Security > Local Net Users**. It is also included in the e-mail that can be sent to a guest informing them of what credentials to use to access the network.
- **Disclaimer**—Used in the e-mail that can be sent to a guest user informing them of what credentials to use to access the network.

Step 5 Click **Save** when finished. The summary screen shown in Figure 10-37 appears, acknowledging that credentials have been applied to the anchor controller(s). The admin is also presented with an option to print or e-mail the credentials to the guest user.

Figure 10-37 Successful Guest Account Creation



Guest Users > Create a Guest User Account

Create a Guest User Account

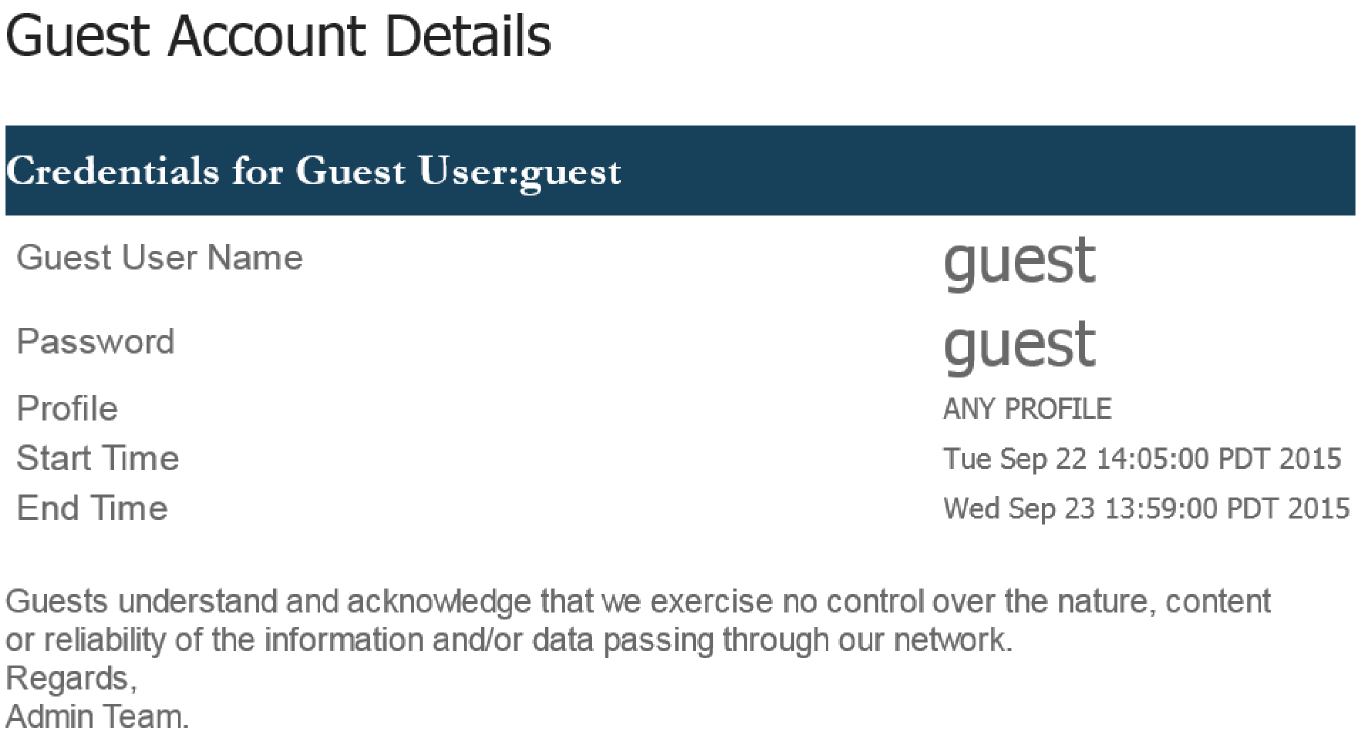
Guest User Account application result to the Controller(s)

IP Address	Controller Name	Operation Status	Reason
172.20.227.112	5520	Success	-
172.20.227.103	5508-1	Success	-

Guest User Credentials	
Guest User Name	guest
Password	guest
Profile	ANY PROFILE
Start Time	Tue Sep 22 14:05:00 PDT 2015
End Time	Wed Sep 23 13:59:00 PDT 2015
Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, cont

Step 6 Click **Print/Email Guest User Credentials**. The screen shown in Figure 10-38 appears.

Figure 10-38 Print/Email Guest User Details



Guest Account Details

Credentials for Guest User:guest

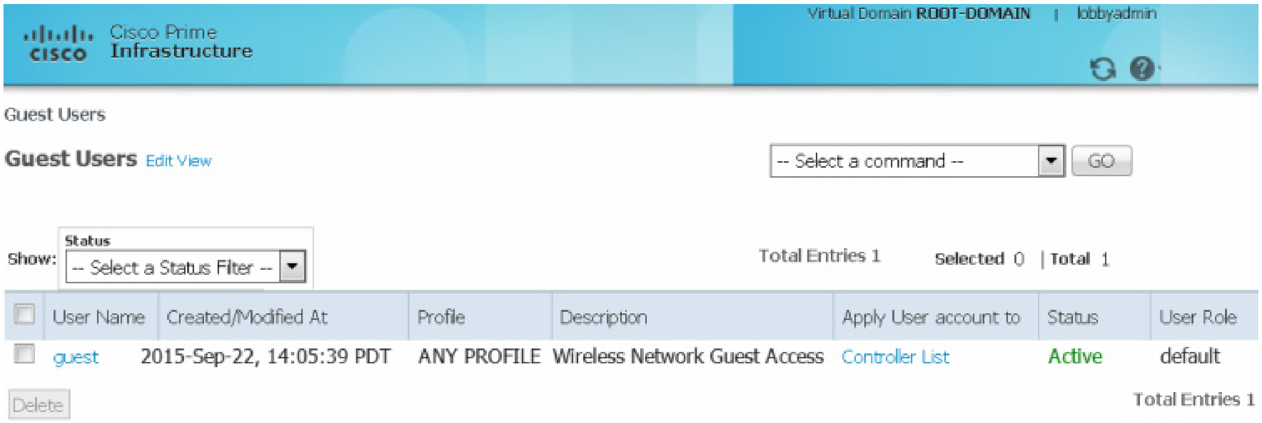
Guest User Name	guest
Password	guest
Profile	ANY PROFILE
Start Time	Tue Sep 22 14:05:00 PDT 2015
End Time	Wed Sep 23 13:59:00 PDT 2015

Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.
Regards,
Admin Team.

Note For details on setting up an SMTP mail server to support e-mailing guest account information to users, see the Prime Infrastructure Configuration Guide.

After printing and or e-mailing the account details, the screen shown in Figure 10-39 appears. By clicking the User Name, an admin can go back and edit the guest account or remove it by checking the box next to the User Name and selecting Delete Guest User from the pull-down selection list.

Figure 10-39 Cisco Prime Infrastructure Guest Users Summary



☐	User Name	Created/Modified At	Profile	Description	Apply User account to	Status	User Role
☐	guest	2015-Sep-22, 14:05:39 PDT	ANY PROFILE	Wireless Network Guest Access	Controller List	Active	default

Note If a user template is deleted from Cisco Prime Infrastructure while a user is active, they are de-authenticated.

Using the Schedule Guest User Template

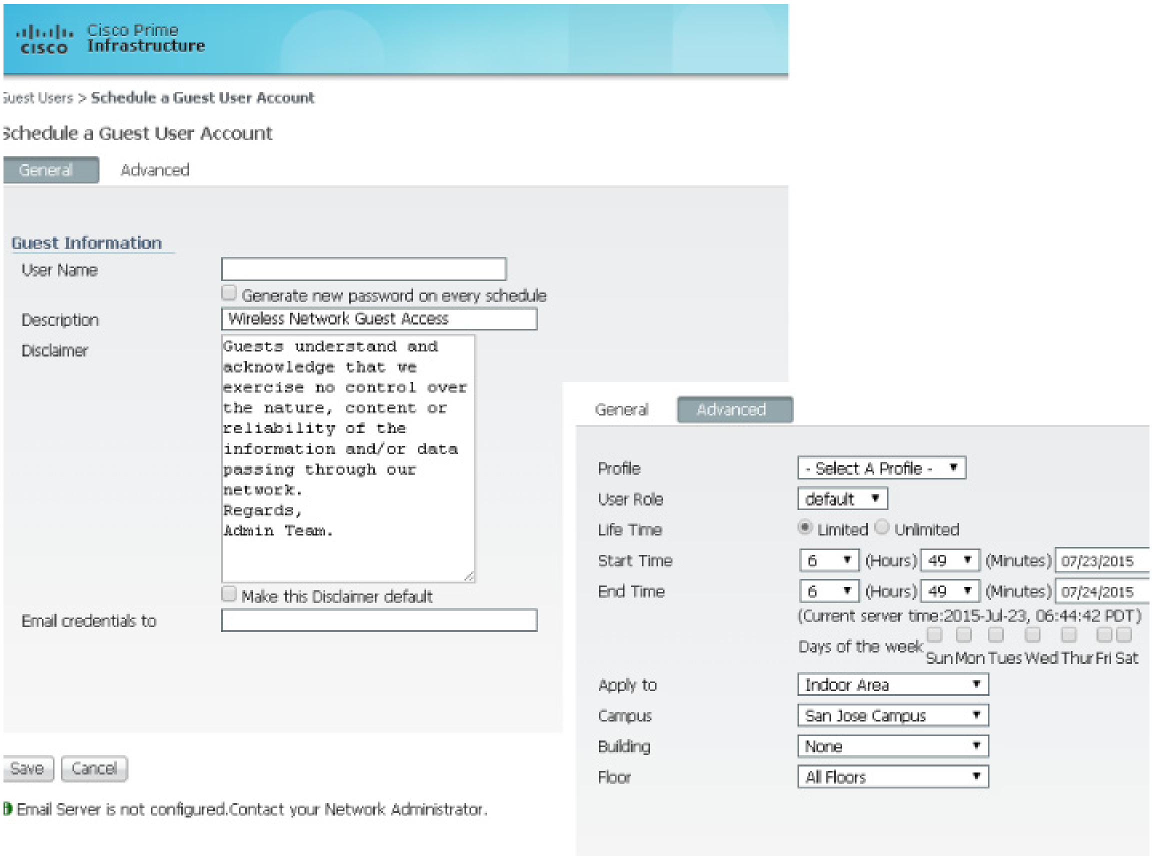
For details about configuring guest accounts, see Prime Infrastructure Configuration Guide.

Figure 10-40 shows the guest user template option.

Step 1 From the pull-down selection list, select **Schedule Guest User** and click **Go**.

The template shown in Figure 10-41 appears.

Figure 10-40 Guest User Template Option



Guest Users > Schedule a Guest User Account

Schedule a Guest User Account

Guest Information

User Name:

☐ Generate new password on every schedule

Description: Wireless Network Guest Access

Disclaimer: Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.
Regards,
Admin Team.

☐ Make this Disclaimer default

Email credentials to:

Email Server is not configured.Contact your Network Administrator.

Profile: - Select A Profile -

User Role: default

Life Time: ● Limited ○ Unlimited

Start Time: 6 (Hours) 49 (Minutes) 07/23/2015

End Time: 6 (Hours) 49 (Minutes) 07/24/2015

(Current server time:2015-Jul-23, 06:44:42 PDT)

Days of the week ☐ Sun ☐ Mon ☐ Tues ☐ Wed ☐ Thur ☐ Fri ☐ Sat

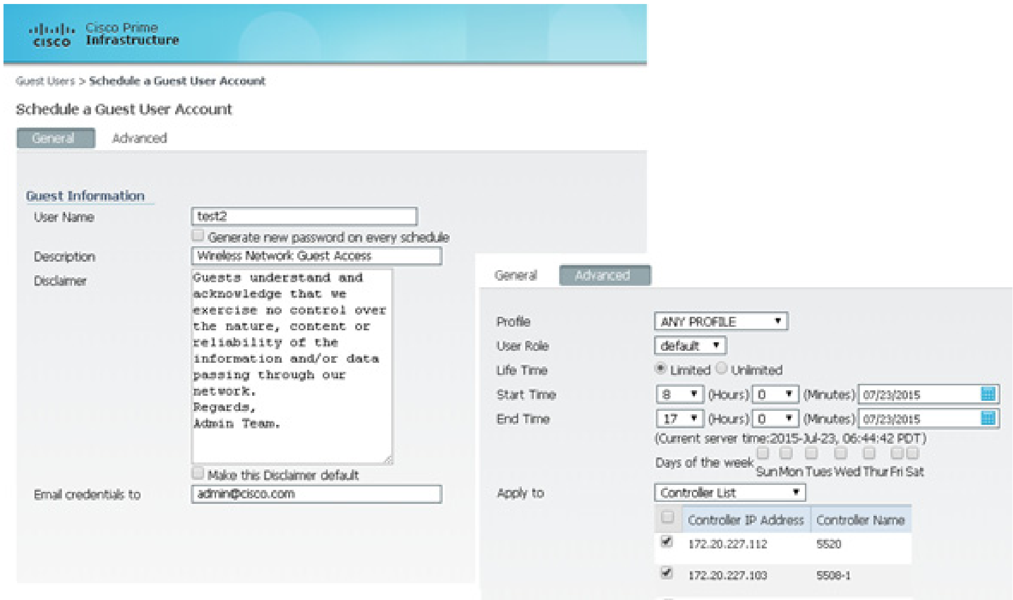
Apply to: Indoor Area

Campus: San Jose Campus

Building: None

Floor: All Floors

Figure 10-41 Schedule Guest User Template



Guest Users > Schedule a Guest User Account

Schedule a Guest User Account

Guest Information

User Name: test2

☐ Generate new password on every schedule

Description: Wireless Network Guest Access

Disclaimer: Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.
Regards,
Admin Team.

☐ Make this Disclaimer default

Email credentials to: admin@cisco.com

Profile: ANY PROFILE

User Role: default

Life Time: ● Limited ○ Unlimited

Start Time: 8 (Hours) 0 (Minutes) 07/23/2015

End Time: 17 (Hours) 0 (Minutes) 07/23/2015

(Current server time:2015-Jul-23, 06:44:42 PDT)

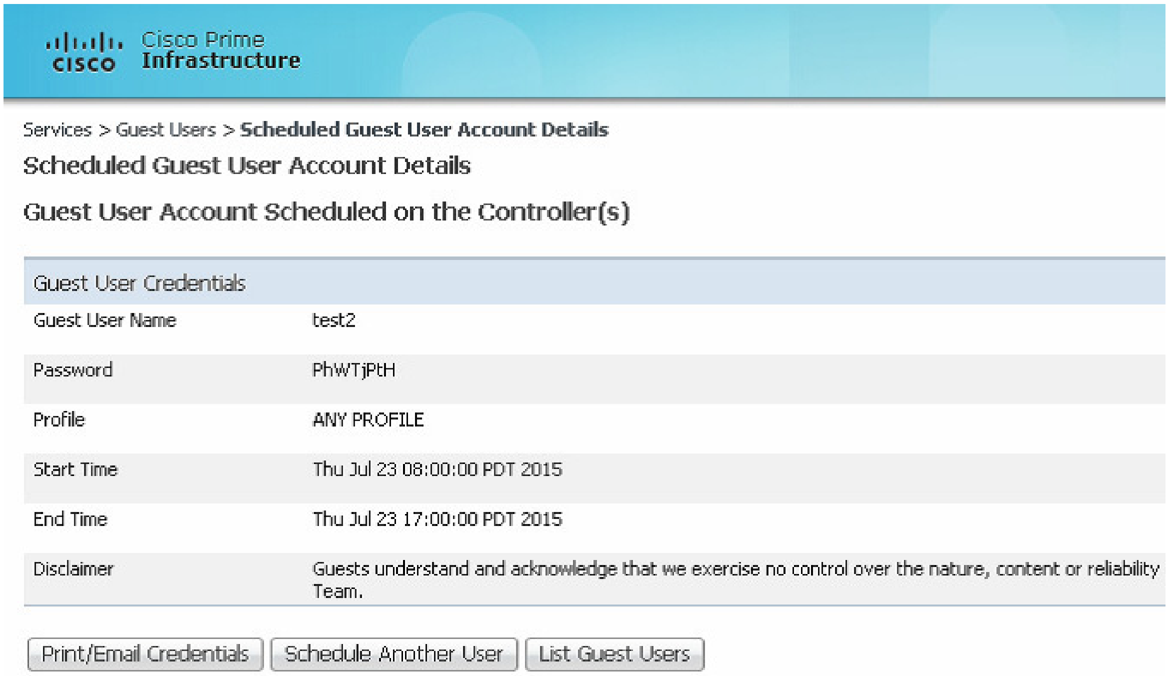
Days of the week ☐ Sun ☐ Mon ☐ Tues ☐ Wed ☐ Thur ☐ Fri ☐ Sat

Apply to: Controller List

☐	Controller IP Address	Controller Name
☑	172.20.227.112	5520
☑	172.20.227.103	5508-1

Figure 10-42 shows an example of a schedule guest user account creation.

Figure 10-42 Schedule Guest User Account Creation



Services > Guest Users > **Scheduled Guest User Account Details**

Scheduled Guest User Account Details

Guest User Account Scheduled on the Controller(s)

Guest User Credentials	
Guest User Name	test2
Password	PhWTjPtH
Profile	ANY PROFILE
Start Time	Thu Jul 23 08:00:00 PDT 2015
End Time	Thu Jul 23 17:00:00 PDT 2015
Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliability Team.

Step 2 Under **Guest Information**, enter a User Name. User names can be up to 24 characters long. When using the schedule-based template, administrators have the option to allow the system to automatically generate the user name for each new day that access is being offered. Also, when using this template, the system automatically generates the user password. There is no option to manually assign a password.

Step 3 Under **Account Configuration**, select the following:

- **Profile**—The pull-down selection list displays a list of WLANs (SSIDs) configured with an L3 Web Policy.
- **User Role**—They are predefined by the administrator and are associated with the guests' access (such as contractor, customer, partner, vendor, visitor, and so on).
- **Life Time**—Select "limited" or "unlimited".
- **Start Time**—Select the time, month, and day when the account is to become active.

Note The start time cannot begin within the current day that the account is being created. The start day must be one or more days beyond the day the account is being created.

- **End Time**—If the account is "limited", select the stop time, month, and day.

Note The stop day can be a period no longer than 30 days from the start day.

- **Days of Week**—Depending on the lifetime of the account, administrators have the ability to control for which days of the week access is available. Click the check boxes next to those days of the week access is permitted.

Note If "Days of the Week" is selected, the start and stop times represent the period within each day that access is available. Upon expiry within a given day, Cisco Prime Infrastructure removes the credentials from the applicable controllers. For each new day/interval that access is permitted, Cisco Prime Infrastructure automatically generates a new password (and optionally a username), e-mails it to the guest user, and re-applies the new credentials to the applicable WLCs. If "Days of the Week" is not defined, access begins based on the start day and time and is continuously active until the end day and time.

- **Apply To**—From the pull-down selection list, select **Controller List** and click the check box next to the controller(s) representing anchor WLCs. Note that there will be other controllers listed; however, these represent the foreign WLCs. There is no need to apply user credentials on the foreign WLCs because the authentication enforcement point is the anchor WLC.

Note As seen in Figure 10-42, there are various options for where the credentials can be applied, including being able to control the physical/geographic location where a user can access the guest WLAN. These include outdoor areas, indoor areas, building, floor, and so on. This location-based access method can only be used if: 1) the WLAN deployment has been integrated into the management system mapping database, and 2) the guest WLAN (a WLAN with web policy) does not use mobility anchors.

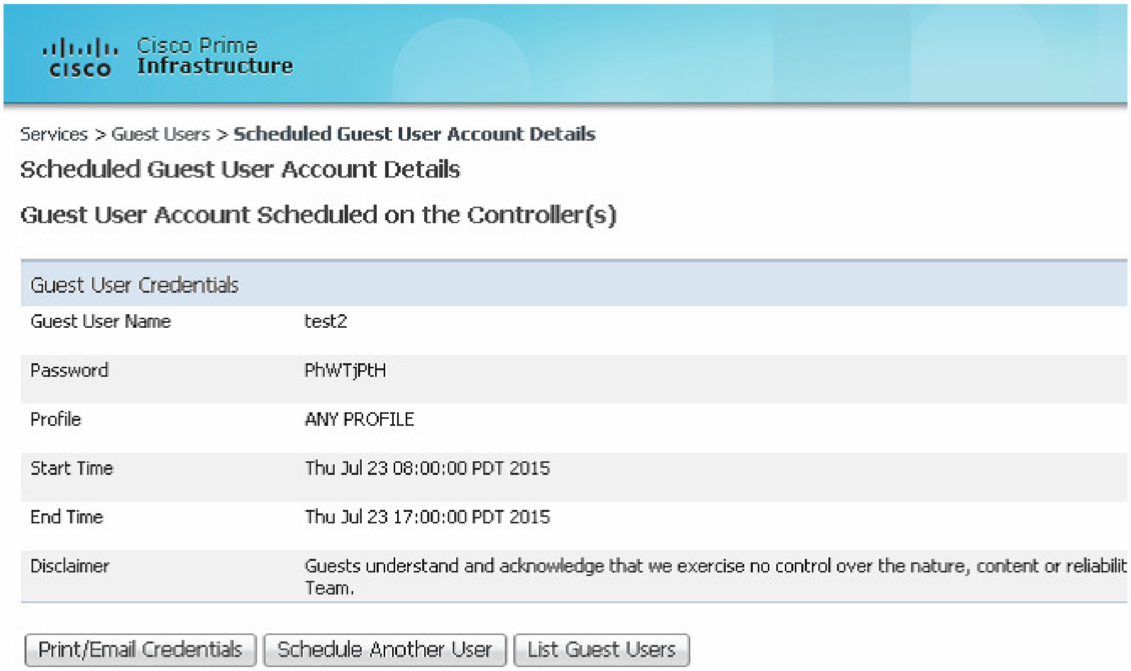
- **E-mail Credentials to**—Enter the e-mail address for whom an account is being established. This is a mandatory field.

Note An SMTP mail server must be configured in Cisco Prime Infrastructure so that it can use to send guest account information. For details, see Cisco Wireless System Configuration Guide.

- **Description**—Enter a description. The description is displayed on the WLC to which the credentials are applied under **Security > Local Net Users**. It is also included in the e-mail that can be sent to a guest informing them of what credentials to use to access the network.
- **Disclaimer**—Used in the e-mail that can be sent to a guest user informing them of what credentials to use to access the network.

Step 4 Click **Save** when finished. The screen shown in Figure 10-43 appears, acknowledging that the scheduled account has been created. The admin is also presented with an option to print or e-mail the credentials to the guest user.

Figure 10-43 Successful Scheduled Account Creation



Services > Guest Users > **Scheduled Guest User Account Details**

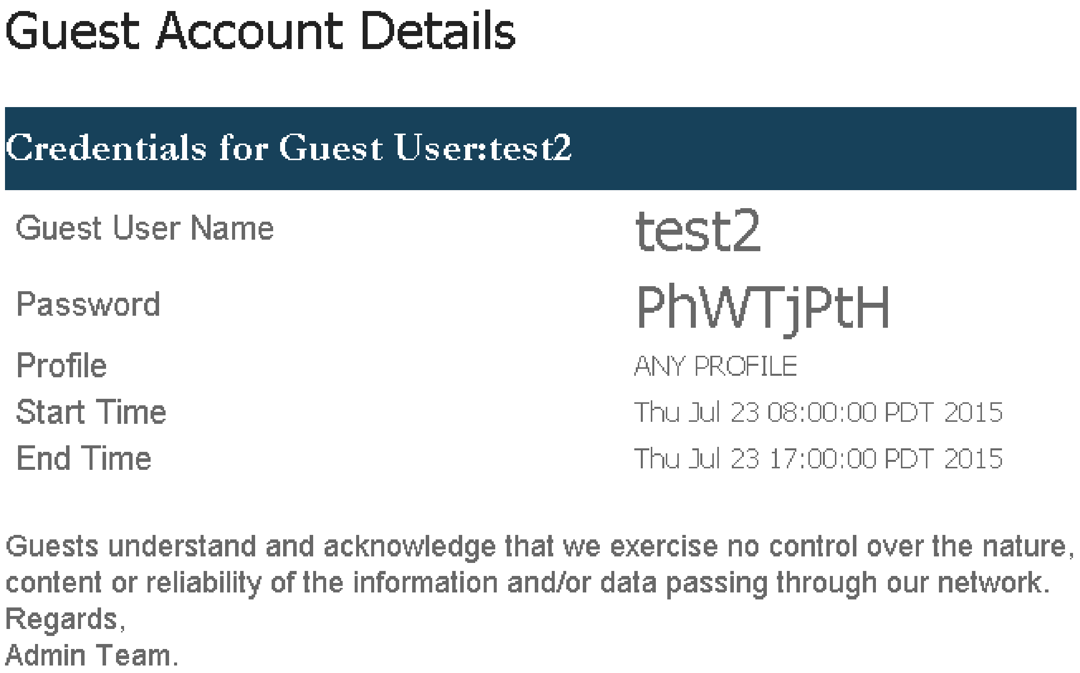
Scheduled Guest User Account Details

Guest User Account Scheduled on the Controller(s)

Guest User Credentials	
Guest User Name	test2
Password	PhWTjPtH
Profile	ANY PROFILE
Start Time	Thu Jul 23 08:00:00 PDT 2015
End Time	Thu Jul 23 17:00:00 PDT 2015
Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliabilit Team.

Step 5 Optionally, click **Print/Email Guest User Credentials**. The screen shown in Figure 10-44 appears.

Figure 10-44 Print/E-mail Guest User Details



Guest Account Details

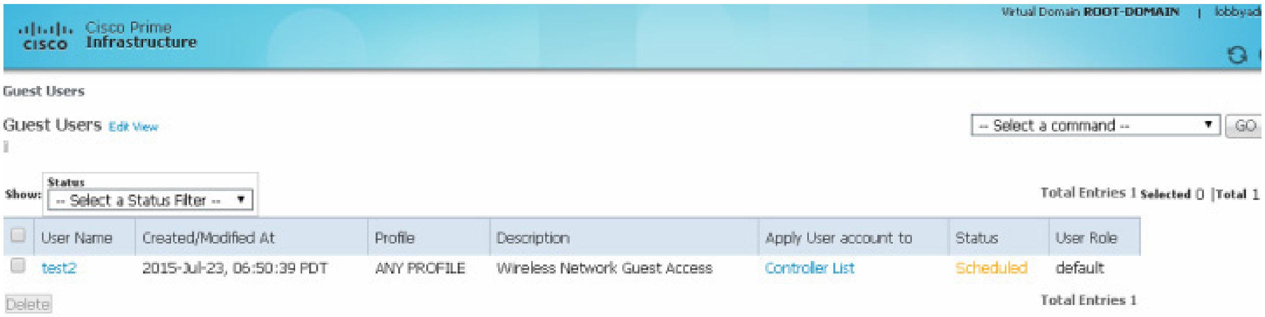
Credentials for Guest User:test2

Guest User Name	test2
Password	PhWTjPtH
Profile	ANY PROFILE
Start Time	Thu Jul 23 08:00:00 PDT 2015
End Time	Thu Jul 23 17:00:00 PDT 2015

Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.
Regards,
Admin Team.

After printing and/or e-mailing the account details, the summary screen shown in Figure 10-45 appears. By clicking the **User Name**, an admin can go back and edit the guest account or remove it by checking the box next to the User Name and selecting **Delete Guest User** from the pull-down selection list.

Figure 10-45 Cisco Prime Infrastructure Guest Users Summary


Virtual Domain ROOT-DOMAIN | lobbyad
Cisco Prime Infrastructure
Edit View
-- Select a command --
GO
-- Select a Status Filter --
Delete

Guest Users

Guest Users

Show: Status

Total Entries 1 Selected 0 | Total 1

☐	User Name	Created/Modified At	Profile	Description	Apply User account to	Status	User Role
☐	test2	2015-Jul-23, 06:50:39 PDT	ANY PROFILE	Wireless Network Guest Access	Controller List	Scheduled	default

Total Entries 1

Note If a user template is deleted from Cisco Prime Infrastructure while a user is active, they are de-authenticated.

This completes the steps required to create a guest account using the lobby ambassador interface in Cisco Prime Infrastructure.

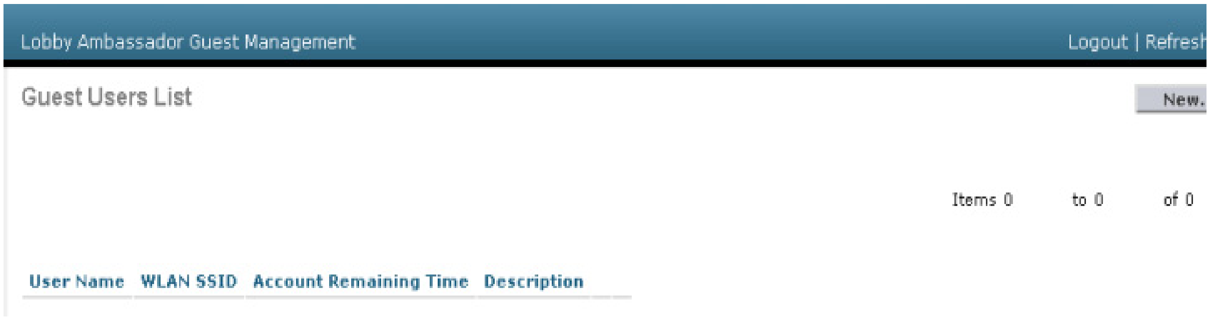
Managing Guest Credentials Directly on the Anchor Controller

The following procedure assumes that a network administrator has established a local management account with lobby admin privileges on one or more anchor controllers.

Step 1 Login to the anchor controller using the lobby admin credentials assigned by the system administrator. Remember that conduits might need to be opened through a firewall to permit HTTP/HTTPS for web administration of the controller. See Anchor Controller Positioning.

After login, the screen shown in Figure 10-46 appears.

Figure 10-46 Anchor Controller Login



Guest Users List

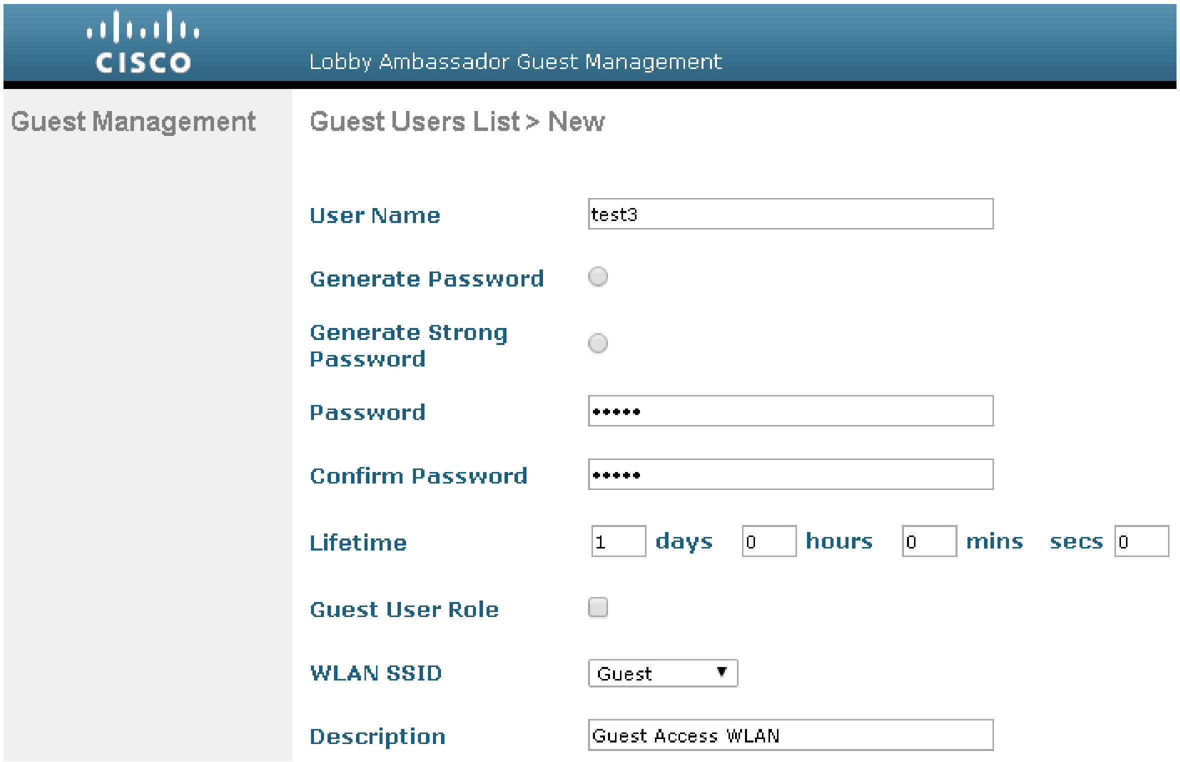
Items 0 to 0 of 0

User Name	WLAN SSID	Account Remaining Time	Description

Step 2 Click **New**.

The screen shown in Figure 10-47 appears.

Figure 10-47 Creating Local WLC Guest Credentials



User Name: test3
Generate Password ○
Generate Strong Password ○
Password: •••••
Confirm Password: •••••
Lifetime: 1 days 0 hours 0 mins secs 0
Guest User Role ☐
WLAN SSID: Guest
Description: Guest Access WLAN

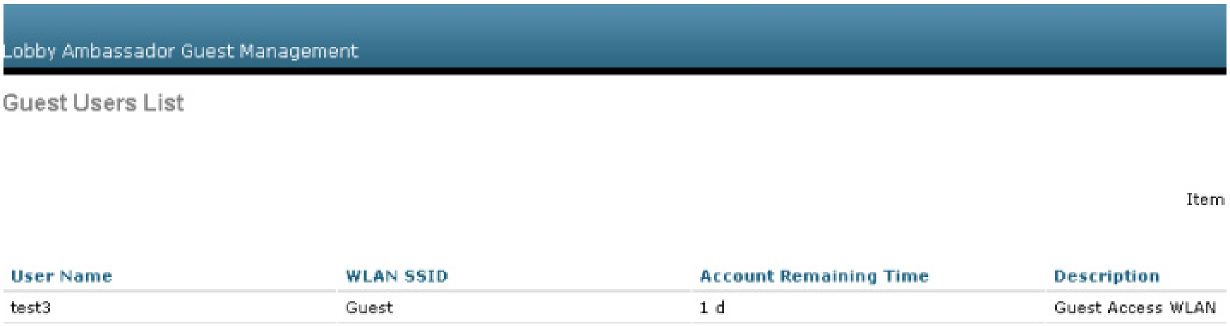
Step 3 To create user credentials, perform the following steps:

1. Enter a username and password (manual or auto).
2. Select the WLAN/SSID to which the guest account applies (only WLANs configured with an L3 web policy are displayed).
3. Enter a lifetime for the credentials.
4. Enter User Role if needed.
5. Enter a description for the user.

Step 4 Click **Apply**.

The screen shown in Figure 10-48 appears and shows the newly-added guest user.

Figure 10-48 Anchor WLC Guest Users List



Guest Users List

Item

User Name	WLAN SSID	Account Remaining Time	Description
test3	Guest	1 d	Guest Access WLAN

From this screen you have the option to do the following:

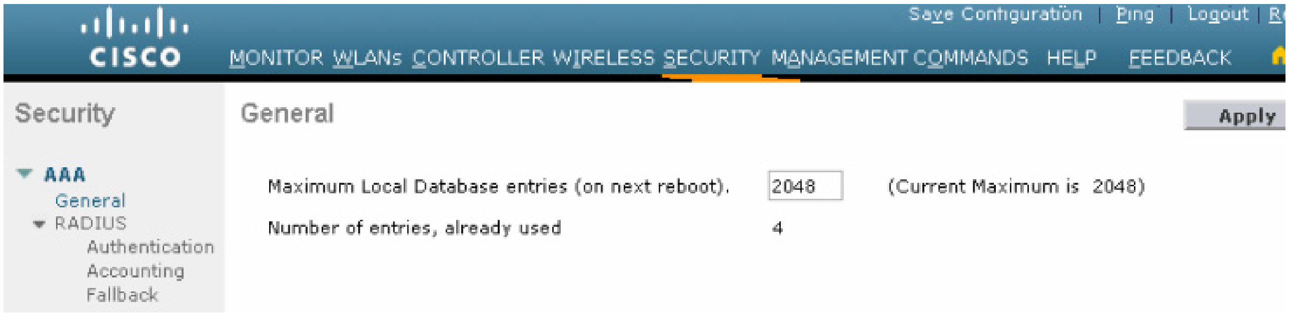
- Edit the existing user (link at far right; not visible).
- Delete the existing user (link at far right; not visible).
- Add a new user.

Configuring the Maximum Number of User Accounts

The default number of guest user accounts that can be defined on the controller is 2048. This value can be changed by completing the following steps.

Step 1 Click the **Security** tab. (See Figure 10-49.)

Figure 10-49 Configuring the Maximum Number of User Accounts


Save Configuration | Ping | Logout | R
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
Apply

General

Maximum Local Database entries (on next reboot). 2048 (Current Maximum is 2048)

Number of entries, already used 4

Step 2 In the left pane, click **General** under AAA properties.

Step 3 Configure the maximum number of user database entries (maximum 2048).

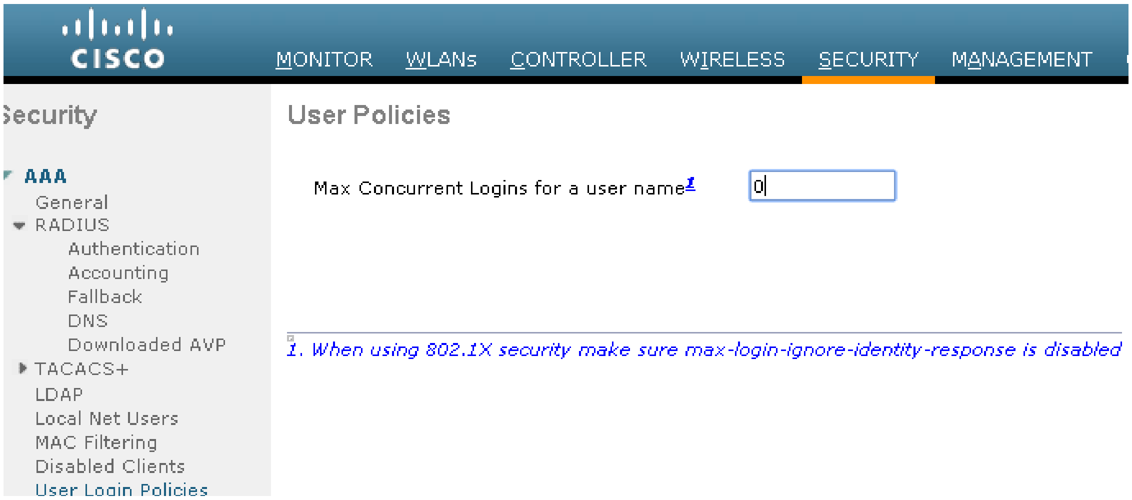
Step 4 Click **Apply**.

Maximum Concurrent User Logins

The maximum number of concurrent logins for a local user account on the WLC can be configured. Values include 0 for unlimited concurrent logins or can be limited from 1 to 8. The maximum user logins is configured by completing the following steps:

Step 1 Click the **Security** tab. (See Figure 10-50.)

Figure 10-50 User Login Policies



User Policies

Max Concurrent Logins for a user name[1] 0

1. When using 802.1X security make sure max-login-ignore-identity-response is disabled

Step 2 In the left pane, click **User Login Policies** under AAA.

Step 3 Configure the maximum number of concurrent user logins (between 0-8).

Step 4 Click **Apply**.

Guest User Management Caveats

Note the following caveats:

- Guest accounts can be added using either method above or both methods together.
- When using Cisco Prime Infrastructure, the lobby admin may not have visibility of user accounts that might have been created locally on the anchor controller if the controller configuration has not been recently synchronized with Cisco Prime Infrastructure. If this is the case and a Cisco Prime Infrastructure lobby admin attempts to add an account with a user name that is already configured on the WLC, the Cisco Prime Infrastructure configuration overrides the local configuration.
- When adding user accounts locally on the controller, the local admin will have visibility of all accounts that have been created, including those that were created via Cisco Prime Infrastructure.
- If a guest user is currently authenticated to a WLAN and their credentials are deleted from Cisco Prime Infrastructure or locally on the controller, the user traffic stops flowing, and the user is de-authenticated.

Other Features and Solution Options

Web Portal Page Configuration and Management

The internal web server and associated functionality is hosted locally on the anchor controller. When a WLAN is configured to use the web policy, either for authentication or pass-through, the internal web server is invoked by default. No further configuration is required. The internal portal includes a few optional configuration parameters.

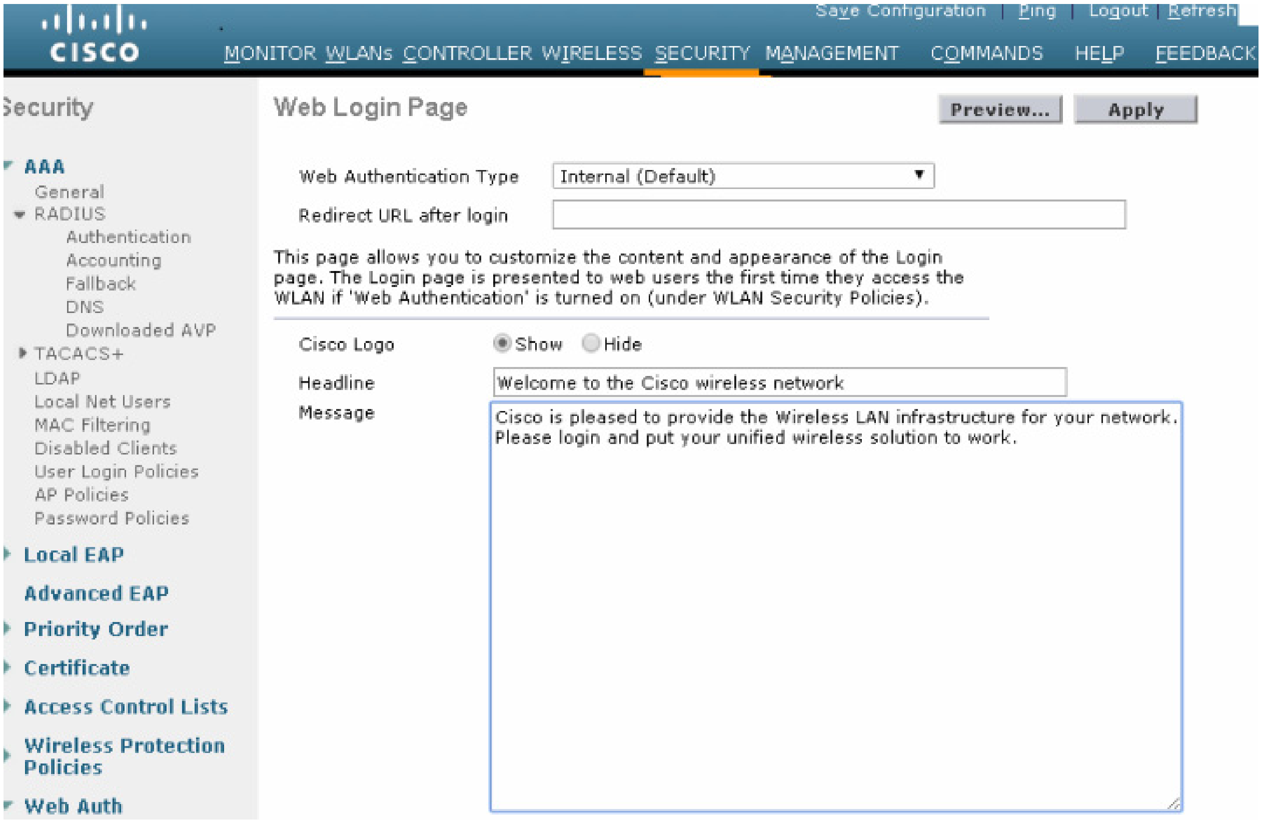
Internal Web Page Management

Step 1 Click the **Security** tab.

Step 2 In the left pane, click **Web Auth** and then **Web Login Page**.

The configuration screen shown Figure 10-51 is displayed. You can change the heading and message information that appears on the portal page. You can also choose a post-authentication redirect URL.

Figure 10-51 Web Login Page Configuration Screen



Web Login Page

Web Authentication Type: Internal (Default)

Redirect URL after login:

This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

Cisco Logo: ● Show ○ Hide

Headline: Welcome to the Cisco wireless network

Message: Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

Step 3 Click **Apply**.

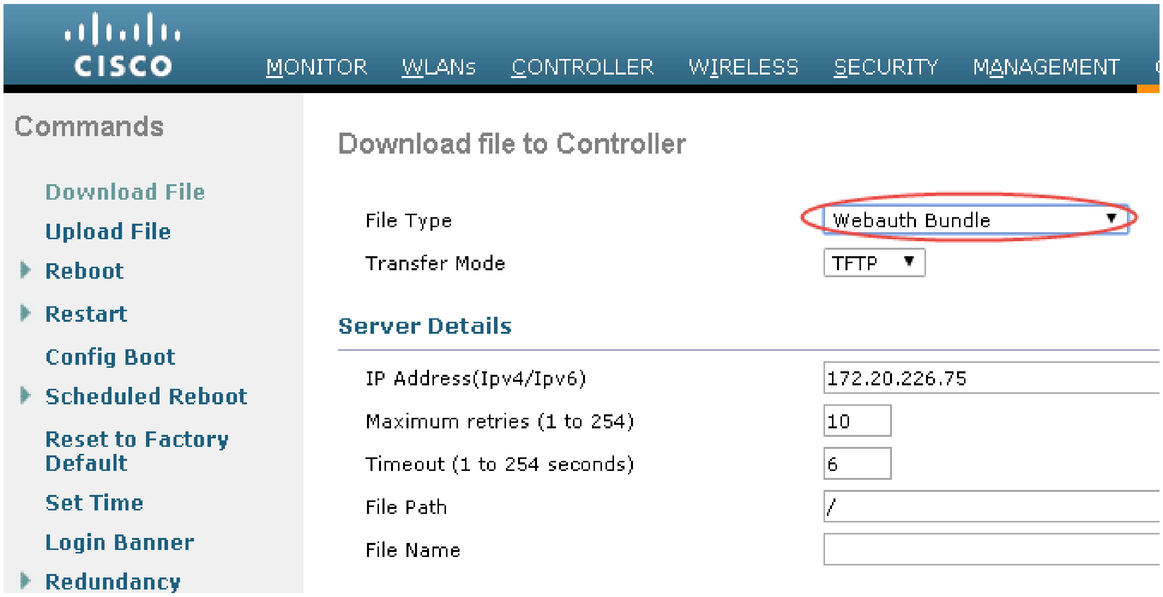
Step 4 Optionally, click **Preview** to view what the user sees when redirected.

Importing a Web Page

You can download a customized web page and store it locally on the anchor controller. To import a customized web page, perform the following steps.

Step 1 Click the **Commands** tab. (See Figure 10-52.)

Figure 10-52 Importing a Web Page



Download file to Controller

File Type: Webauth Bundle

Transfer Mode: TFTP

Server Details

IP Address(Ipv4/Ipv6): 172.20.226.75

Maximum retries (1 to 254): 10

Timeout (1 to 254 seconds): 6

File Path: /

File Name:

Step 2 Under File Type, select **Web Auth Bundle**.

Step 3 Define the IP address and file path on the TFTP server where the files reside.

Step 4 Click **Download** to begin.

Be aware of these caveats when downloading a web auth bundle:

- Select **Web Auth Bundle** from the pull-down selection list to ensure that the files are stored in the correct directory on the controller.
- The **Web Auth Bundle** must be a **.tar** file of the HTML and image files associated with the custom web login page. When downloaded, the WLC un-tars the files and places them in the appropriate directory.
- The **Web Auth Bundle** (**.tar** file) cannot be larger than 1 MB.
- The file name for the HTML login page must be **login.html**.

For more information about downloading and using customized web pages, see Cisco Wireless Controller Configuration Guide.

Selecting an Imported Web Auth Page

To use a customized web auth page that has been downloaded to the controller, perform the following steps:

Step 1 Click the **Security** tab.

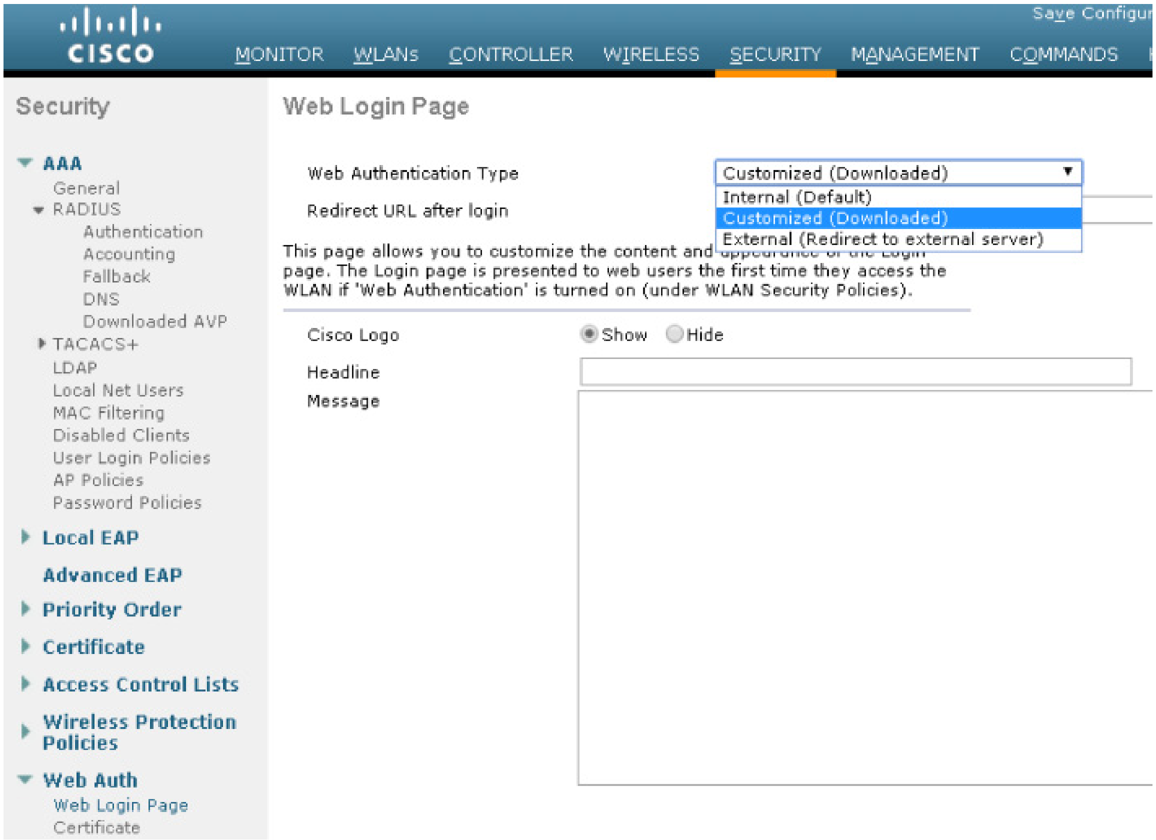
Step 2 In the left pane, click **Web Auth** and then **Web Login Page**.

Step 3 From the **Web Authentication Type** pull-down selection list, select **Customized** (Downloaded).

Step 4 Click **Preview** to view the downloaded page.

Step 5 Click **Apply** when finished. (See Figure 10-53.)

Figure 10-53 Selecting an Imported Web Auth Page



Web Login Page

Web Authentication Type: Customized (Downloaded)

Redirect URL after login

This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

Cisco Logo ● Show ○ Hide

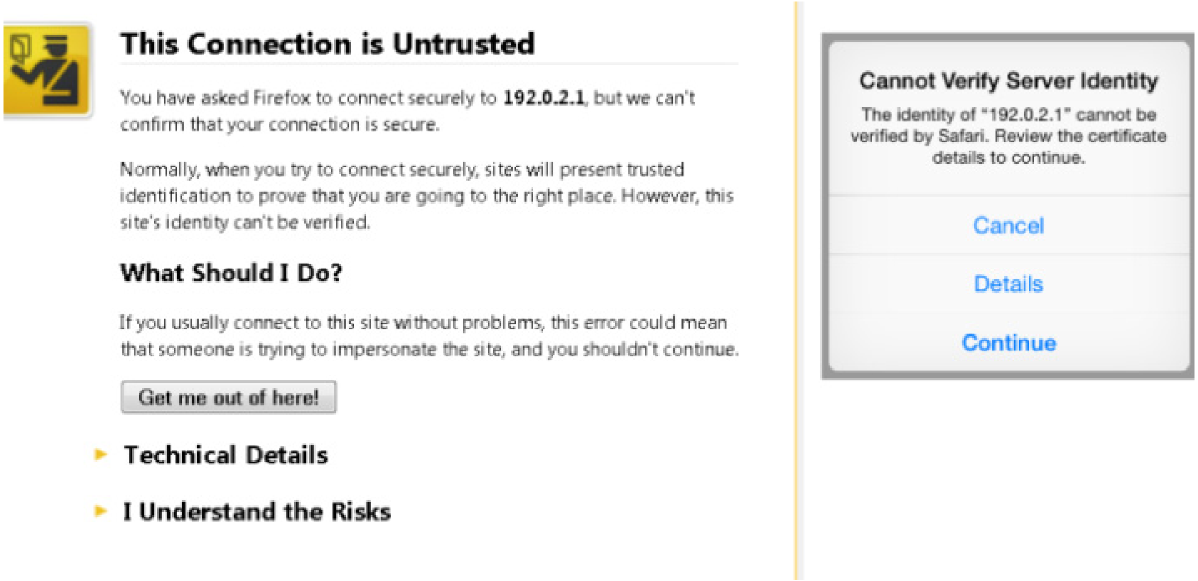
Headline

Message

Internal Web Certificate Management

The web auth login page uses SSL for safeguarding user credentials. For simplicity, the controller uses a self-signed certificate. Because the certificate is self-signed, guest users can expect to see a pop-up alert similar to the following when they are redirected to the authentication page shown in Figure 10-54.

Figure 10-54 Web Certificate Security Alert (Firefox 39.0 and Safari)



This Connection is Untrusted

You have asked Firefox to connect securely to **192.0.2.1**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Cannot Verify Server Identity

The identity of "192.0.2.1" cannot be verified by Safari. Review the certificate details to continue.

At this point, you can proceed by either clicking Yes or you can select View Certificate and manually install it as a trusted site. The web server uses the virtual interface IP address configured in Anchor WLC Installation and Interface Configuration, as its source address. If a hostname is defined along with the IP address, that host name must be resolvable by DNS so that:

- The client is redirected to the web auth page.
- The user does not encounter a web certificate error because of conflicts between hostname and host IP address.

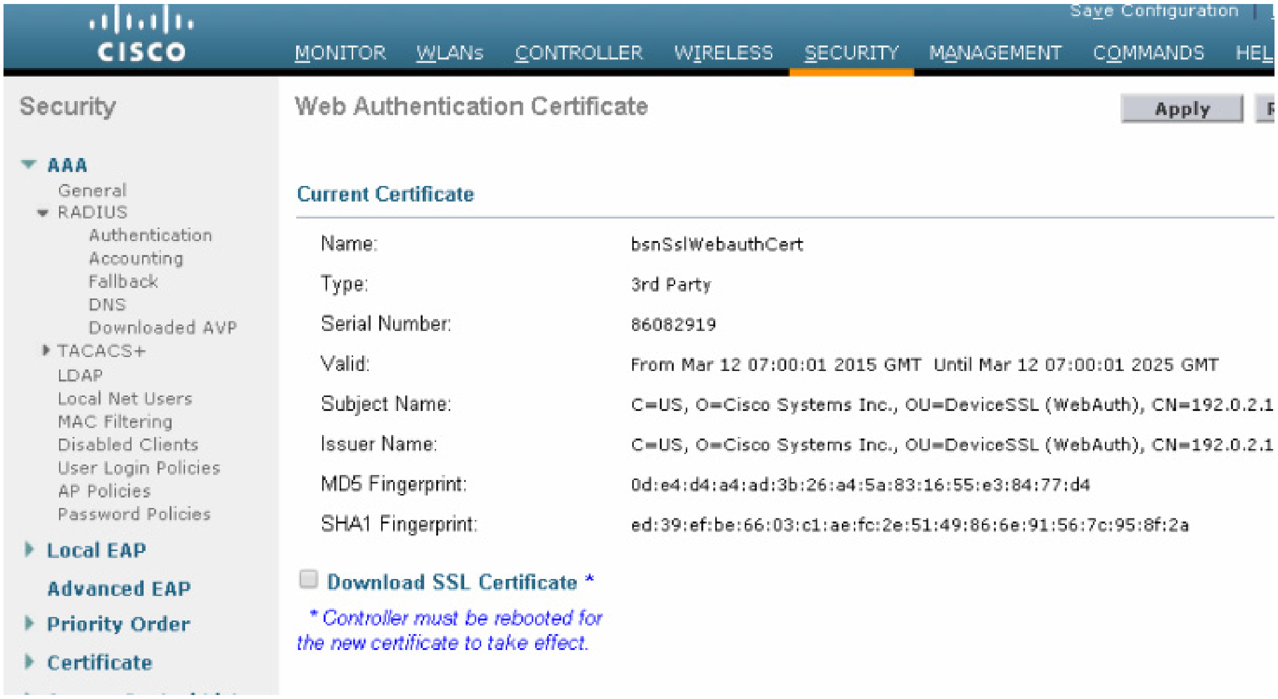
Importing an External Web Certificate

For cases where a legitimate web certificate issued by a trusted root CA is required, one can be downloaded to the controller by performing the following steps:

Step 1 Click the **Security** tab.

In the left pane, click **Web Auth** and then **Certificate**. (See Figure 10-55.)

Figure 10-55 Importing an External Web Certificate



Name: bsnSslWebauthCert
Type: 3rd Party
Serial Number: 86082919
Valid: From Mar 12 07:00:01 2015 GMT Until Mar 12 07:00:01 2025 GMT
Subject Name: C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAuth), CN=192.0.2.1
Issuer Name: C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAuth), CN=192.0.2.1
MD5 Fingerprint: 0d:e4:d4:a4:ad:3b:26:a4:5a:83:16:55:e3:84:77:d4
SHA1 Fingerprint: ed:39:ef:be:66:03:c1:ae:fc:2e:51:49:86:6e:91:56:7c:95:8f:2a

☐ Download SSL Certificate *

* Controller must be rebooted for the new certificate to take effect.

Step 2 Place a check mark in the **Download SSL Certificate** check box.

Step 3 Complete the required fields for downloading the certificate.

Step 4 Click **Apply**.

Step 5 After the certificate has been downloaded, reboot the server.

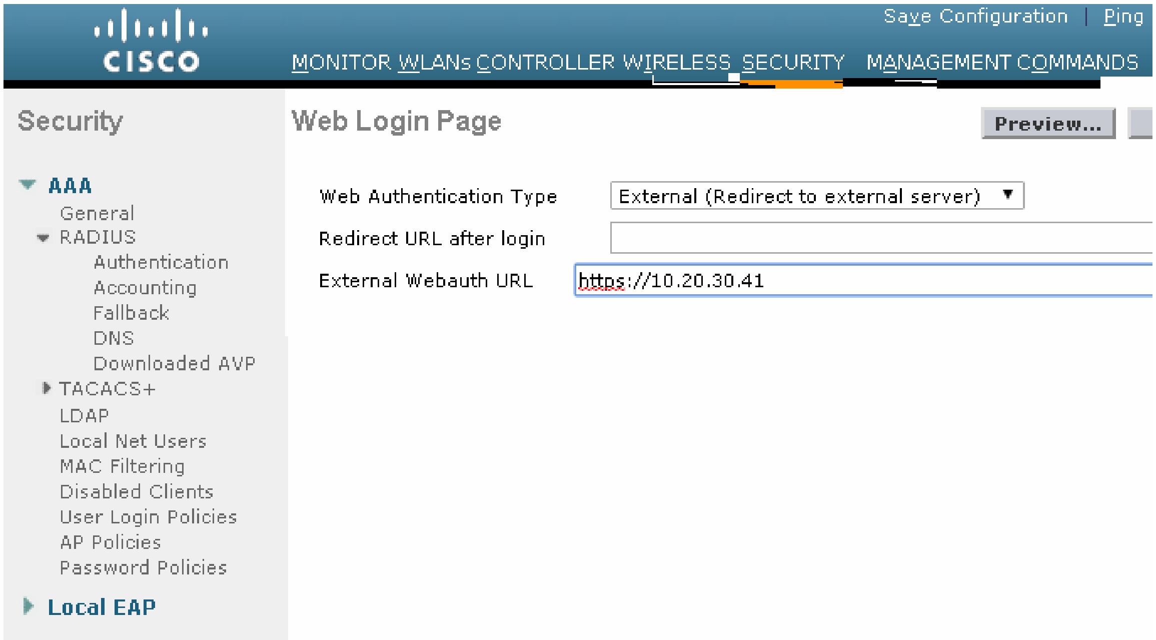
Support for External Web Redirection

In some cases, an enterprise might already have deployed a web-portal system to support wired guest access or NAC functionality. If this is the case, the anchor controller can be configured to redirect wireless guest users to an external web portal using the following steps:

Step 1 Click the **Security** tab.

Step 2 In the left pane, click **Web Auth** and then **Web Login Page**. (See Figure 10-56.)

Figure 10-56 Supporting External Web Redirection



Web Login Page

Web Authentication Type: External (Redirect to external server)
Redirect URL after login:
External Webauth URL: https://10.20.30.41

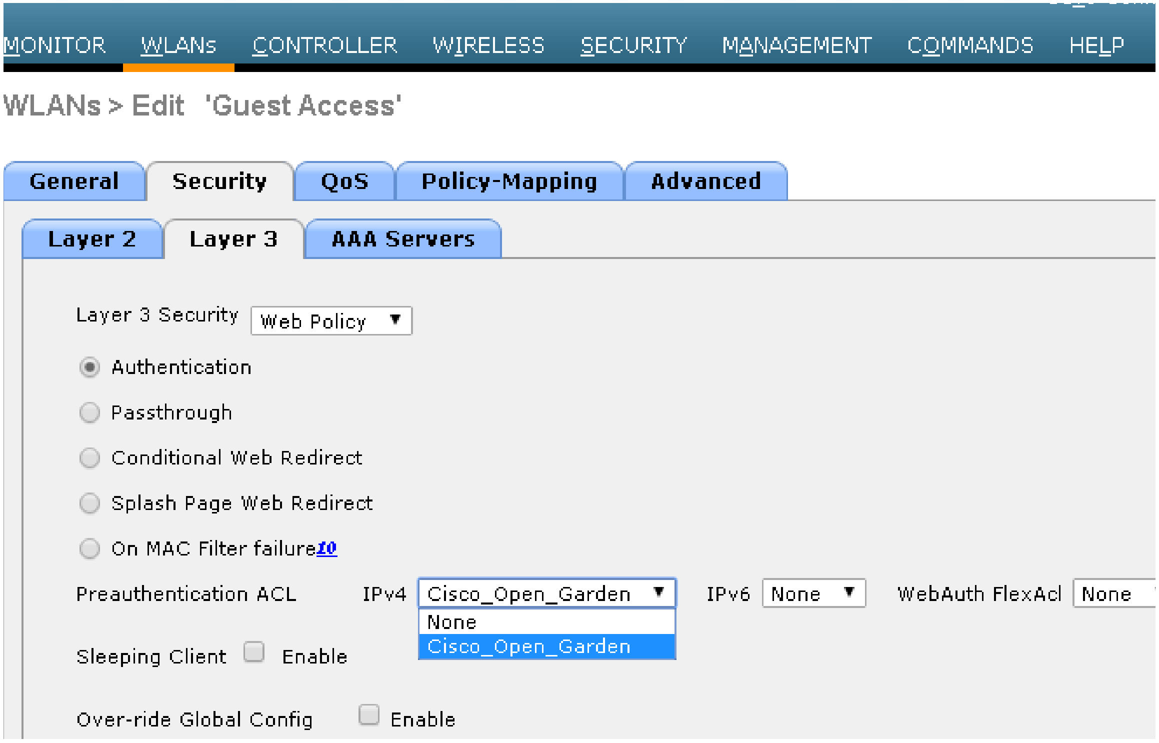
Step 3 Fill in the redirect URL after login and external webauth URL fields.

Step 4 Click **Apply**.

Anchor WLC-Pre-Authentication ACL

A pre-authentication ACL (pre-auth ACL) can be applied to the guest WLAN, which allows unauthenticated clients to connect to specific hosts or URL destinations prior to authenticating. The pre-auth ACL is applied under the guest WLAN Layer 3 Security settings and, if enabled, is performed only on the anchor WLC(s). (See Figure 10-57.)

Figure 10-57 WLAN Pre-authentication ACL



WLANs > Edit 'Guest Access'

Layer 3 Security: Web Policy

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure[10]

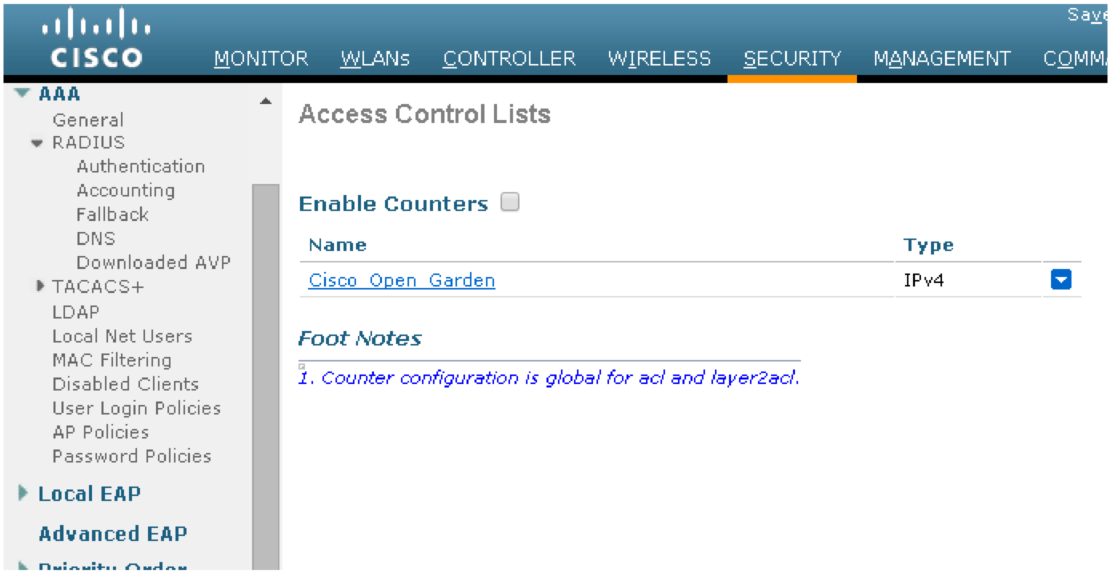
Preauthentication ACL IPv4: Cisco_Open_Garden (None / Cisco_Open_Garden) IPv6: None WebAuth FlexAcl: None

Sleeping Client ☐ Enable

Over-ride Global Config ☐ Enable

The specific ACL is configured under **Security > Access Control Lists** (See Figure 10-58 and Figure 10-59.)

Figure 10-58 WLC Access Control Lists



Access Control Lists

Enable Counters ☐

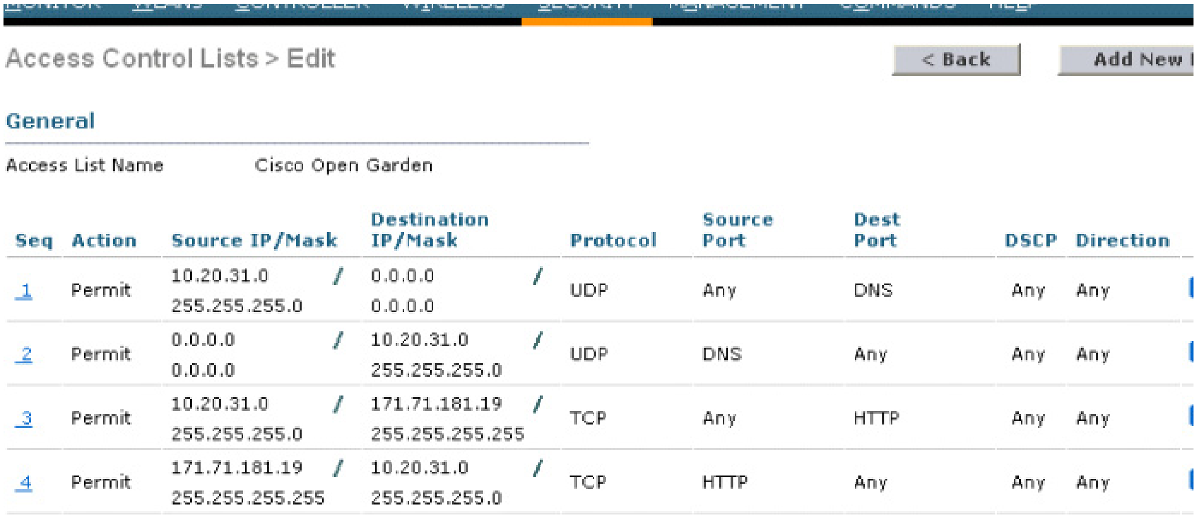
Name	Type
Cisco_Open_Garden	IPv4

Foot Notes

1. Counter configuration is global for acl and layer2acl.

Note If a pre-authentication ACL is used in conjunction with the web auth policy, it must include a rule to permit DNS requests; otherwise, the client is unable to resolve and connect to a destination host/URL that is otherwise allowed by the ACL.

Figure 10-59 Pre-Auth ACL Example



Access Control Lists > Edit

General

Access List Name Cisco Open Garden

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	10.20.31.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any
2	Permit	0.0.0.0 / 0.0.0.0	10.20.31.0 / 255.255.255.0	UDP	DNS	Any	Any	Any
3	Permit	10.20.31.0 / 255.255.255.0	171.71.181.19 / 255.255.255.255	TCP	Any	HTTP	Any	Any
4	Permit	171.71.181.19 / 255.255.255.255	10.20.31.0 / 255.255.255.0	TCP	HTTP	Any	Any	Any

External Radius Authentication

As described in Guest User Authentication, an external RADIUS server can be used to authenticate guest users in place of creating and storing guest credentials locally on the anchor controller. If this method is used, the lobby admin features described in Guest Account Management cannot be used. It is assumed that some other guest management system will be used in conjunction with the external RADIUS server.

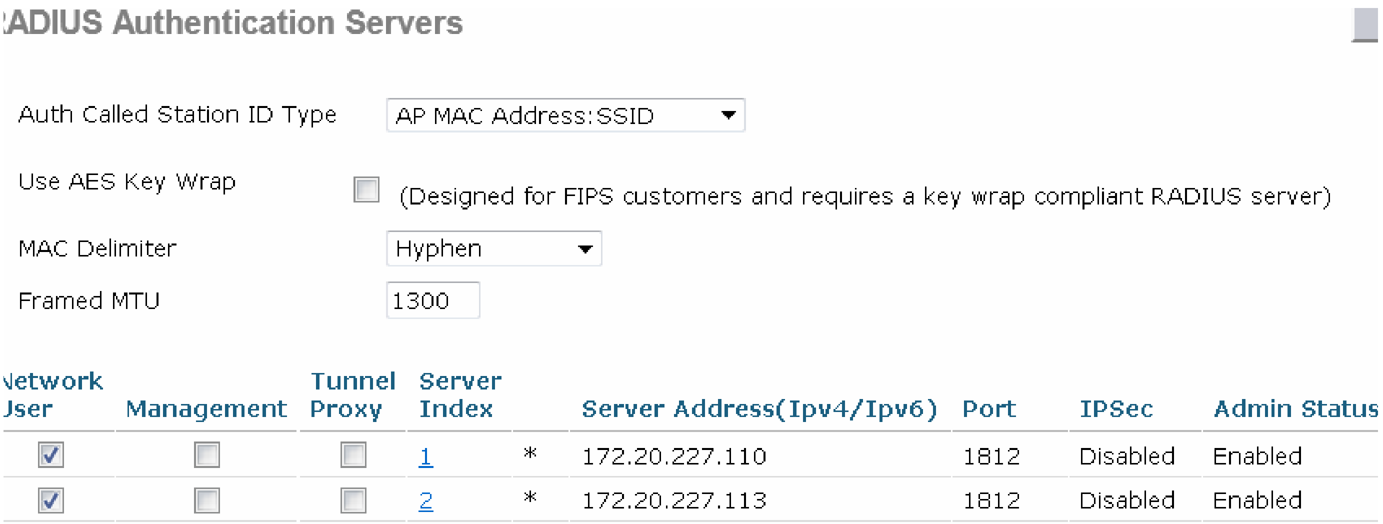
To configure a guest WLAN to use an external RADIUS server, perform the following configuration steps on the anchor controller.

Adding a RADIUS Server

Step 1 Click the **Security** tab.

A summary screen is displayed. (See Figure 10-60.)

Figure 10-60 Summary Screen



ADIUS Authentication Servers

Auth Called Station ID Type: AP MAC Address:SSID

Use AES Key Wrap ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Hyphen

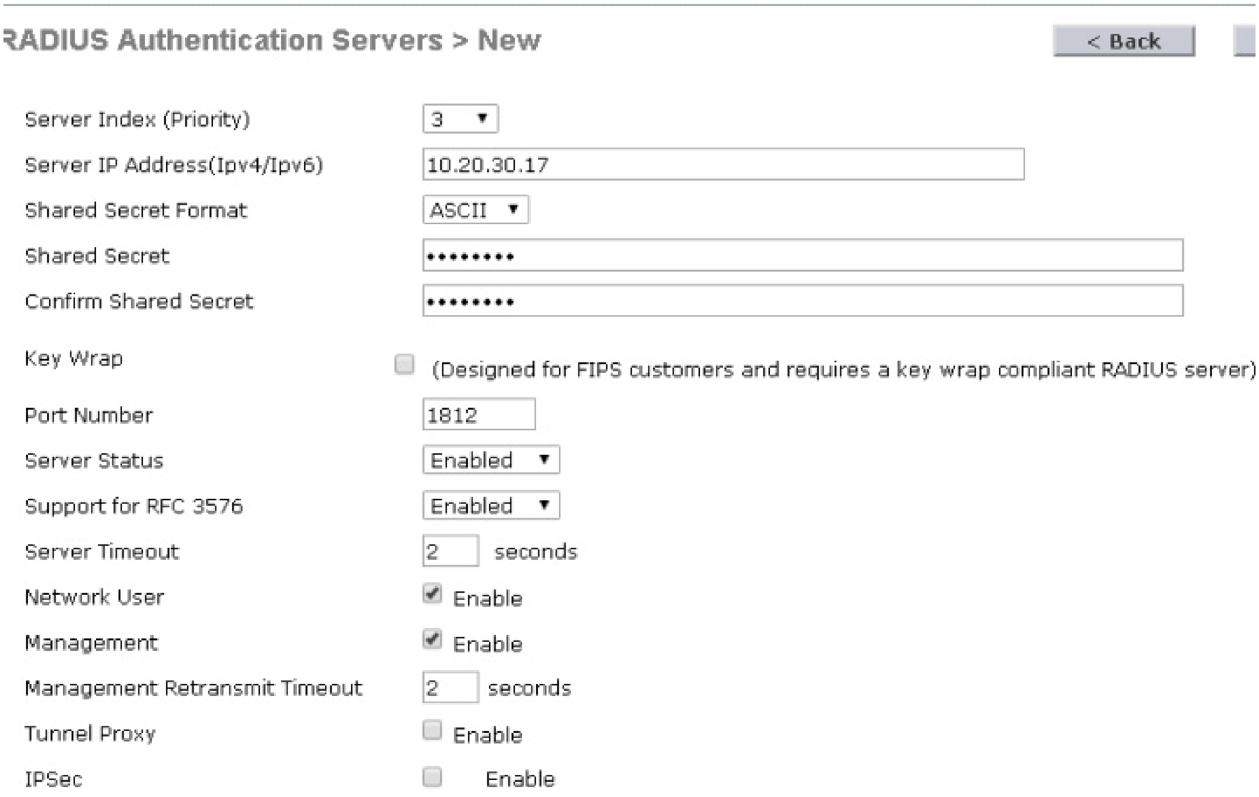
Framed MTU: 1300

etwork ser	Management	Tunnel Proxy	Server Index		Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	☐	☐	1	*	172.20.227.110	1812	Disabled	Enabled
☑	☐	☐	2	*	172.20.227.113	1812	Disabled	Enabled

Step 2 Click **New**.

The screen shown in Figure 10-61 appears.

Figure 10-61 Defining RADIUS Server Settings



ADIUS Authentication Servers > New

Server Index (Priority): 3

Server IP Address(Ipv4/Ipv6): 10.20.30.17

Shared Secret Format: ASCII

Shared Secret: ••••••••

Confirm Shared Secret: ••••••••

Key Wrap ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number: 1812

Server Status: Enabled

Support for RFC 3576: Enabled

Server Timeout: 2 seconds

Network User: ☑ Enable

Management: ☑ Enable

Management Retransmit Timeout: 2 seconds

Tunnel Proxy: ☐ Enable

IPSec: ☐ Enable

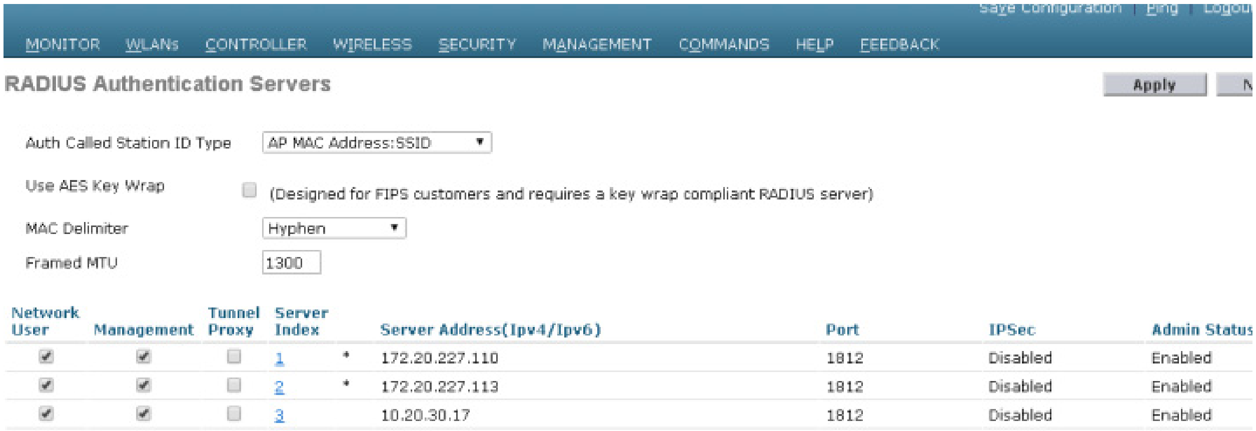
Step 3 To define RADIUS server settings, configure the IP address, shared secret, and authentication port number as defined on the RADIUS server.

If the Network User check box is cleared, the RADIUS server is used only for user authentication when it is specifically selected under the RADIUS setting of a given WLAN. Otherwise, if the Network User check box is checked, the server is used globally for all user authentications based on its server priority.

Step 4 Click **Apply**.

The summary screen shown in Figure 10-62 shows the newly-added server.

Figure 10-62 Summary Screen


Save Configuration | Ping | Logou
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Apply
N

RADIUS Authentication Servers

Auth Called Station ID Type: AP MAC Address:SSID

Use AES Key Wrap ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Hyphen

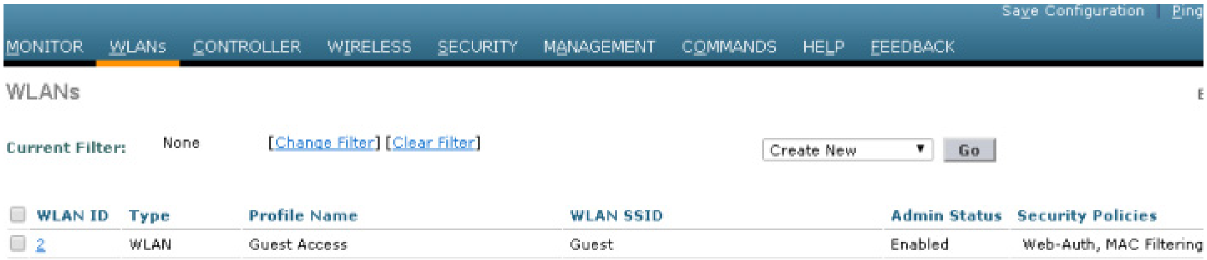
Framed MTU: 1300

Network User	Management	Tunnel Proxy	Server Index		Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	☑	☐	1	*	172.20.227.110	1812	Disabled	Enabled
☑	☑	☐	2	*	172.20.227.113	1812	Disabled	Enabled
☑	☑	☐	3		10.20.30.17	1812	Disabled	Enabled

Step 5 To select a RADIUS server, click the **WLANs** tab.

The screen shown in Figure 10-63 appears.

Figure 10-63 WLANs Tab


Save Configuration | Ping
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
E
[Change Filter] [Clear Filter]
Create New
Go

WLANs

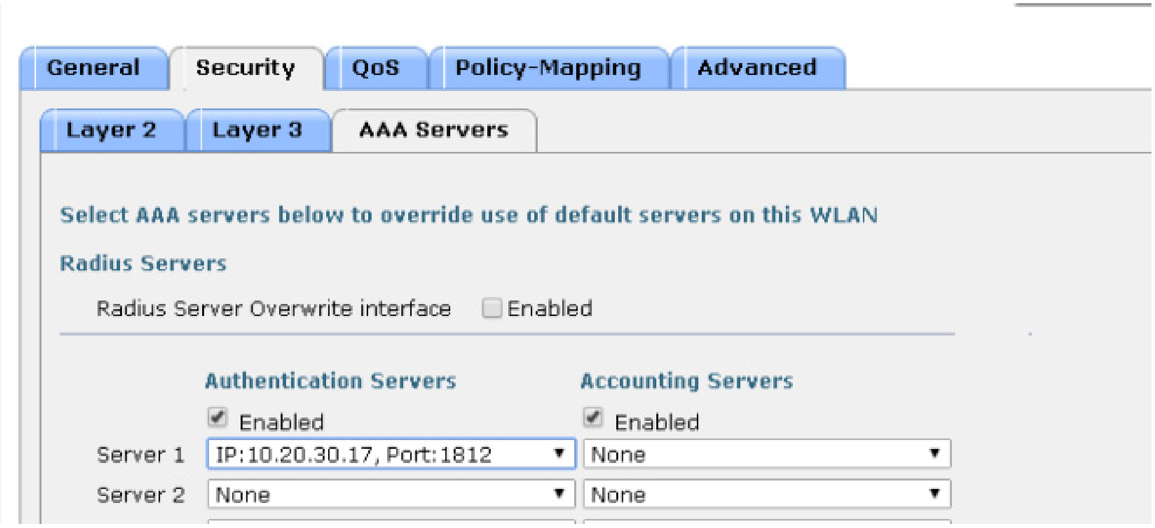
Current Filter: None

☐ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
☐ 2	WLAN	Guest Access	Guest	Enabled	Web-Auth, MAC Filtering

Step 6 Find the guest WLAN and click on its **Profile Name**.

The guest WLAN configuration screen is displayed, as shown in Figure 10-64.

Figure 10-64 Guest WLAN Configuration Screen



Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface ☐ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:10.20.30.17, Port:1812	None
Server 2	None	None

Step 7 Select **AAA Servers** under the WLAN Security tab.

Step 8 Select the RADIUS server to be used for web authentication from the pull-down selection list under Authentication Servers.

Verifying Guest Access Functionality

The guest access service is working correctly if a user:

- Can associate to the guest WLAN.
- Receives an IP address via DHCP.
- Opens their browser and is redirected to the web authentication page.
- Enters their credentials and connects to the Internet (or other authorized upstream services).

CHAPTER 11

802.11r, 802.11k, 802.11v, 802.11w Fast Transition Roaming

802.11r Fast Transition Roaming

The 802.11r Fast Transition (FT) Roaming is an amendment to the 802.11 IEEE standards. It is a new concept for roaming. The initial handshake with the new Access Point (AP) occurs before client roams to the target AP, called as Fast Transition (FT).

Initial handshake allows the client and APs to do Pairwise Master Key (PMK) calculation in advance. Once the client performs the re-association request or response exchange with the new AP, the PMK keys are applied to the client and AP. The FT key hierarchy allows clients to make fast Base Station Subsystem (BSS) transitions between APs without the need for re-authentication at every AP. 802.11r eliminates the handshake overhead while roaming and thereby reduces the hand off times between APs, which provides security and QoS. It is useful for client devices with delay-sensitive applications, such as, voice and video over Wi-Fi.

Methods of Client Roaming

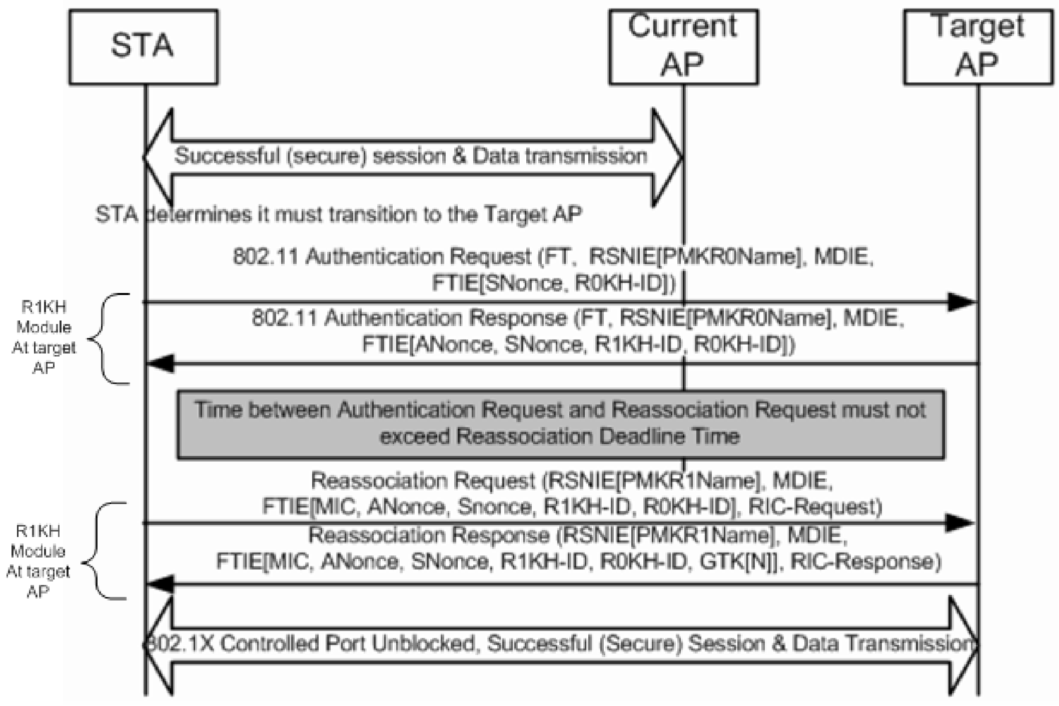
For a client to move from the current AP to target AP using FT protocols, the message exchanges are performed using one of the following methods:

- Over-the-Air FT Roaming
- Over-the-DS (Distribution System) FT Roaming

Over-the-Air Fast Transition Roaming

The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.

Figure 11-1 Fast BSS Transition over-the Air in RSN


STA
Current AP
Target AP
Successful (secure) session & Data transmission
STA determines it must transition to the Target AP
802.11 Authentication Request (FT, RSNIE[PMKR0Name], MDIE, FTIE[SNonce, R0KH-ID])
R1KH Module At target AP
802.11 Authentication Response (FT, RSNIE[PMKR0Name], MDIE, FTIE[ANonce, SNonce, R1KH-ID, R0KH-ID])
Time between Authentication Request and Reassociation Request must not exceed Reassociation Deadline Time
Reassociation Request (RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, Snonce, R1KH-ID, R0KH-ID], RIC-Request)
R1KH Module At target AP
Reassociation Response (RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID, GTK[N]], RIC-Response)
802.1X Controlled Port Unblocked, Successful (Secure) Session & Data Transmission

Roaming Over-the-Air Intra Controller

When a client is roaming between AP1 and AP2 that are connected to the same controller, the following steps takes place by default:

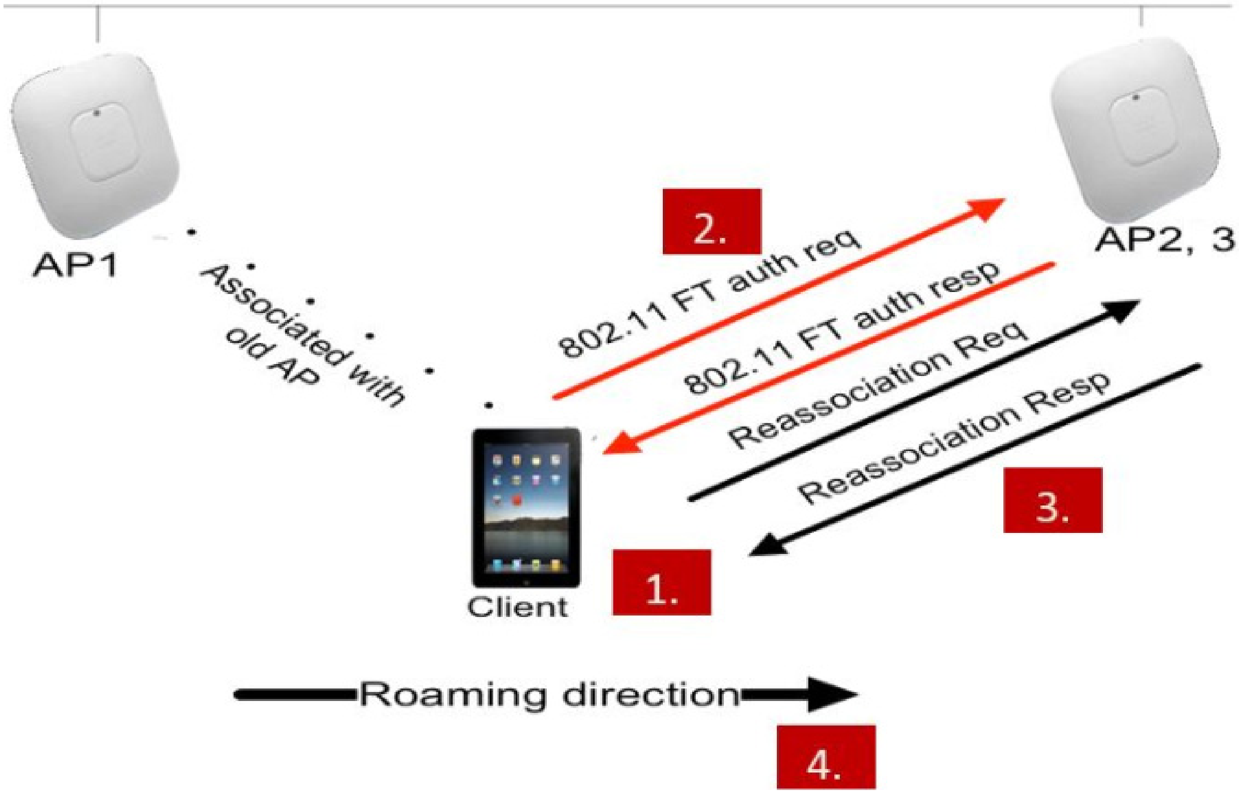
Step 1 Client associates with AP1 and requests to roam with AP2.

Step 2 Client sends a FT Authentication Request to AP2 and receives a FT Authentication Response from AP2.

Step 3 Client sends a FT Re-association Request to AP2 and receives a FT Re-association Response from AP2.

Step 4 Client completes its roam from AP1 to AP2.

Figure 11-2 Over-the- Air Intra Controller Roam



Roaming Over the Air Inter Controller

When a client is roaming between AP1 and AP2 which are connected to different controllers such as WLC1 and WLC2, respectively, within mobility group, the following steps takes place by default:

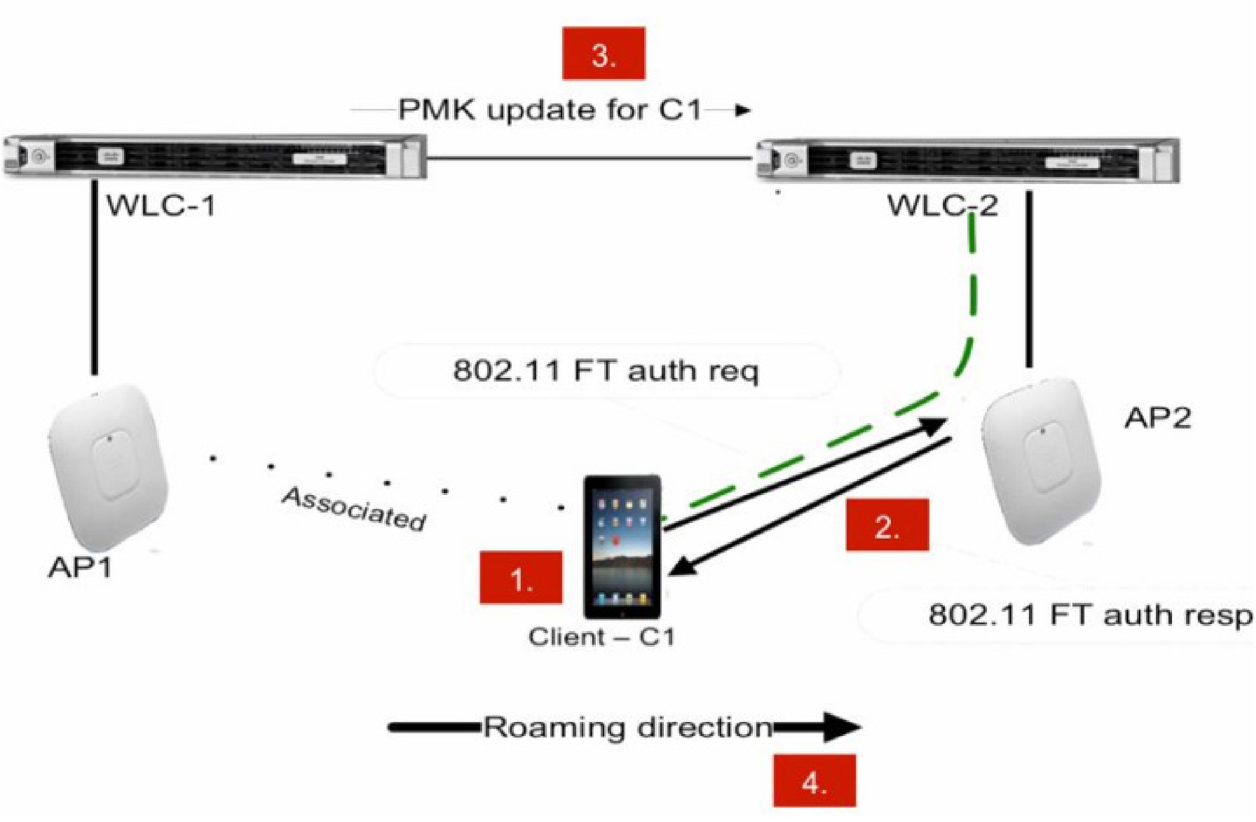
Step 1 Client associates with AP1 and requests to roam with AP2.

Step 2 Client sends a FT Authentication Request to AP2 and receives a FT Authentication Response from AP2.

Step 3 WLC-1 sends PMK and mobility message to WLC-2 about the roaming client that uses mobility infrastructure.

Step 4 Client completes its roam from AP1 to AP2.

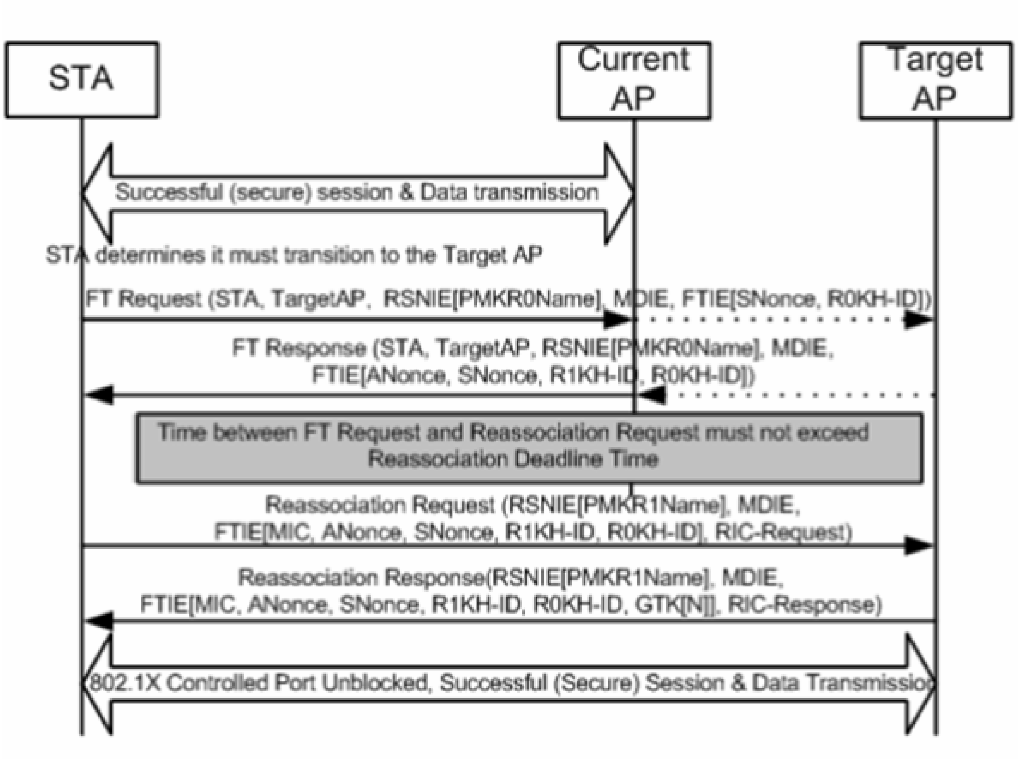
Figure 11-3 Over- the- Air Inter Controller Roam



Over-the-Distribution System Fast Transition Roaming

In roaming over the DS, the client communicates with the target AP through the current AP. The communication is in FT action frames between the client and the current AP through the controller.

Figure 11-4 Roaming Over the DS


STA
Current AP
Target AP
Successful (secure) session & Data transmission
STA determines it must transition to the Target AP
FT Request (STA, TargetAP, RSNIE[PMKR0Name], MDIE, FTIE[SNonce, R0KH-ID])
FT Response (STA, TargetAP, RSNIE[PMKR0Name], MDIE, FTIE[ANonce, SNonce, R1KH-ID, R0KH-ID])
Time between FT Request and Reassociation Request must not exceed Reassociation Deadline Time
Reassociation Request (RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], RIC-Request)
Reassociation Response(RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID, GTK[N]], RIC-Response)
802.1X Controlled Port Unblocked, Successful (Secure) Session & Data Transmission

Roaming Over the DS Intra Controller

When a client is roaming between AP1 and AP2 that are connected to the same controller, the following steps takes place by default:

Step 1 Client associates with AP1 and requests to roam with AP2.

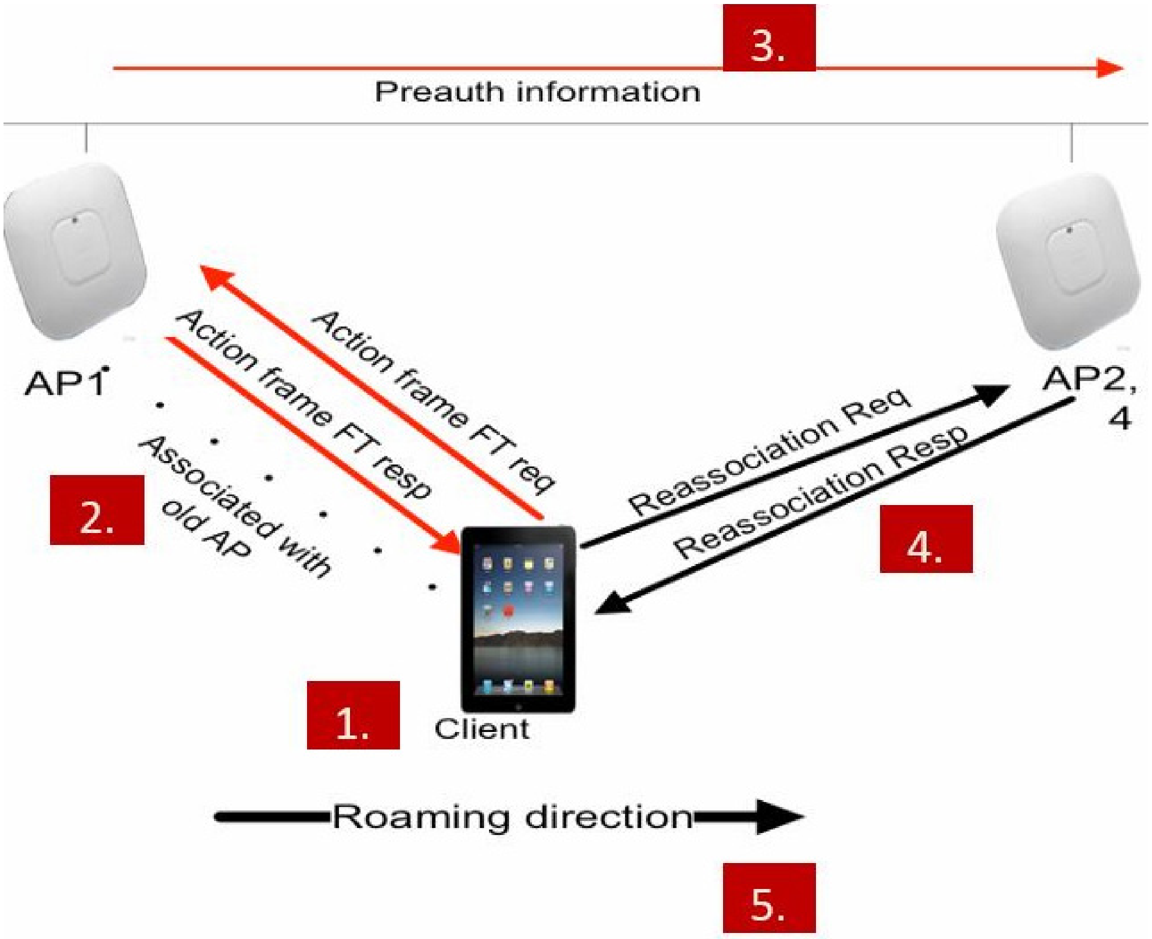
Step 2 Client sends a FT Authentication Request to AP1 and receives a FT Authentication Response from AP1.

Step 3 The controller sends the pre-authentication information to AP2 as the APs are connected to the same controller.

Step 4 Client sends a FT Re-association Request to AP2 and receives a FT Re-association Response from AP2.

Step 5 Client completes its roam from AP1 to AP2.

Figure 11-5 Over the DS intra controller roam



Roaming Over the DS Inter Controller

When a client is roaming between AP1 and AP2 that are connected to the different controllers such as WLC1 and WLC2 respectively within a mobility group, the following steps takes place by default:

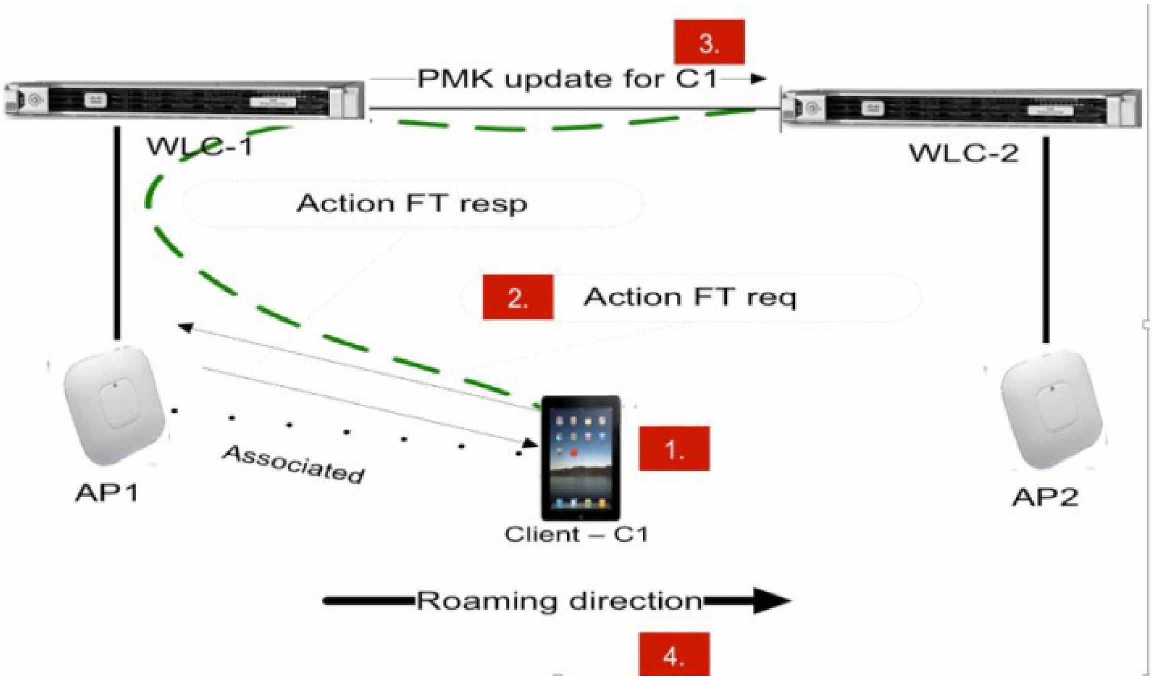
Step 1 Client associates with AP1 and requests to roam with AP2.

Step 2 Client sends a FT Authentication Request to AP1 and receives a FT Authentication Response from AP1.

Step 3 WLC-1 sends Pairwise Master Key (PMK) and mobility message to WLC-2 about the roaming client.

Step 4 Client completes its roam from AP1 to AP2.

Figure 11-6 Over the DS Inter Controller Roam



Configuring Fast Transition Roaming using GUI

To configure FT Roaming using GUI, perform the following steps:

Step 1 Click **WLANs**.

Step 2 Choose **WLAN ID > Edit page**.

Step 3 Choose **Security > Layer 2** tab.

Step 4 Choose **WPA+WPA2** from the drop-down list.

The Authentication Key Management parameter for FT appears.

Step 5 Check the **Fast Transition** check box to enable FT.

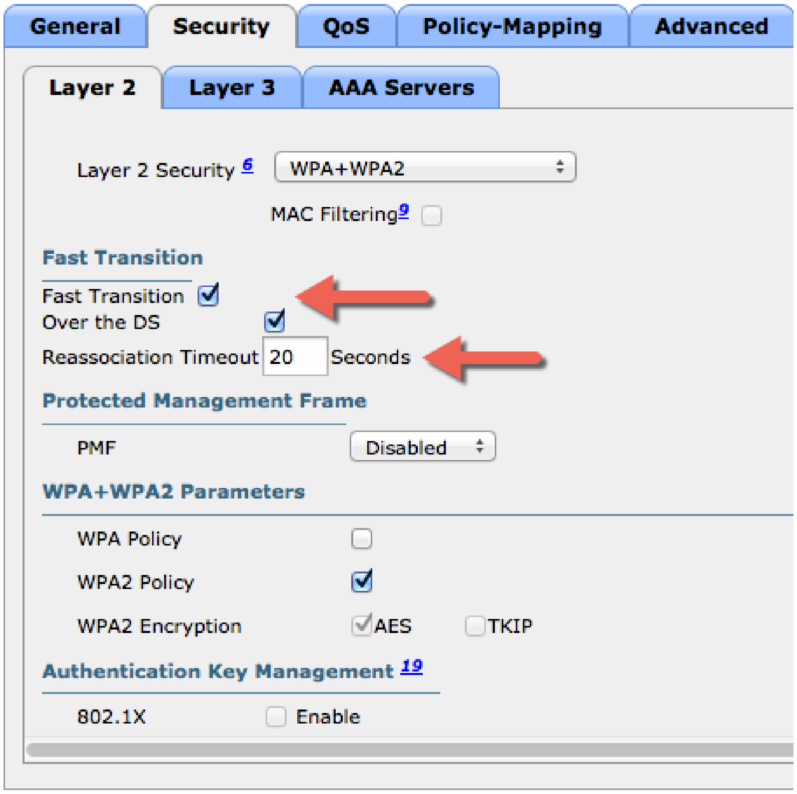
Step 6 Check the **Over the DS** check box to enable FT over a DS.

Note The **Over the DS** check box gets enabled only when you enable FT.

Step 7 In the **Reassociation Timeout** field, enter the number of seconds after which the reassociation attempt of a client to an AP must time out. The valid range is 1 to 100 seconds.

Note The **Reassociation Timeout** field gets enabled only when you enable FT.

Figure 11-7 Setting up Reassociation Timeout



Layer 2 Security [6] WPA+WPA2

MAC Filtering[9] ☐

Fast Transition

Fast Transition ☑

Over the DS ☑

Reassociation Timeout 20 Seconds

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☑

WPA2 Encryption ☑ AES ☐ TKIP

Authentication Key Management [19]

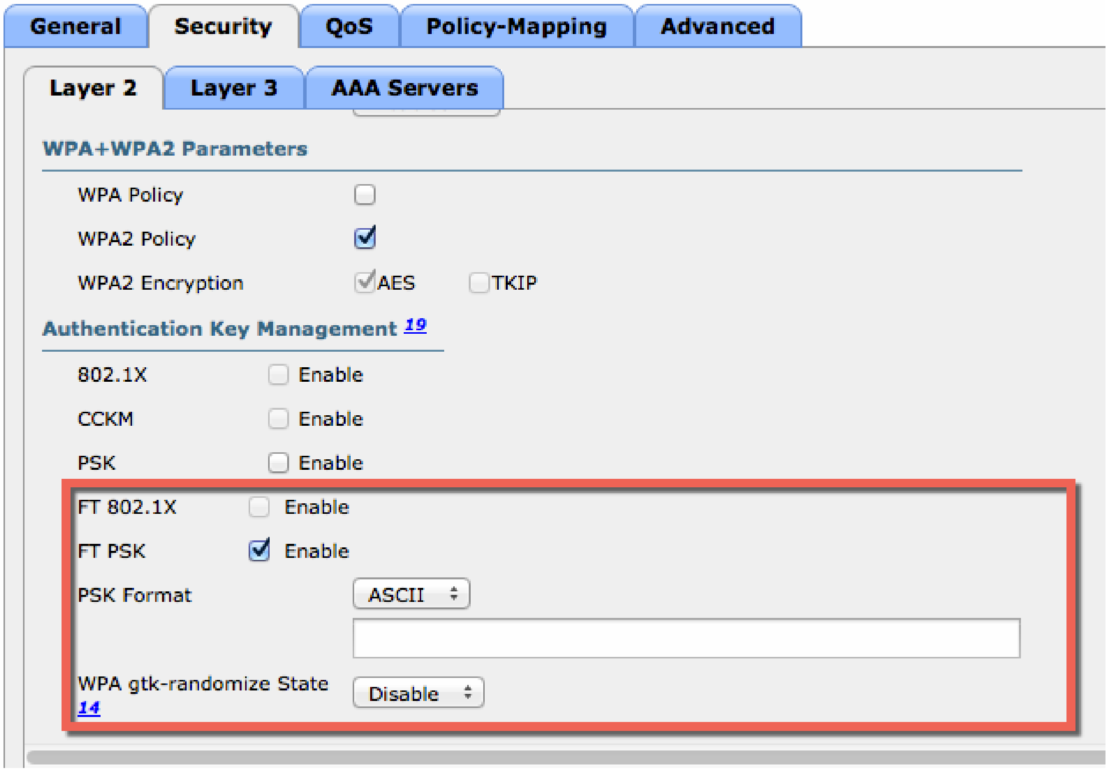
802.1X ☐ Enable

Step 8 Under **Authentication Key Management**, check the **Enable** check box of either **FT 802.1X** or **FT PSK** to enable the key. To disable the key, uncheck the **Enable** check box.

Note If you check the **FT PSK** check box, from the **PSK Format** drop-down list, choose **ASCII** or **Hex** and enter the key value.

Step 9 Choose **Enable** or **Disable** from the **WPA gtk-randomize State** drop-down list, to configure the WPA Group Temporal Key (GTK) to randomize state.

Figure 11-8 Security - Layer 2 - FT PSK



WPA+WPA2 Parameters

WPA Policy ☐
WPA2 Policy ☑
WPA2 Encryption ☑AES ☐TKIP

Authentication Key Management 19

802.1X ☐ Enable
CCKM ☐ Enable
PSK ☐ Enable
FT 802.1X ☐ Enable
FT PSK ☑ Enable
PSK Format ASCII
WPA gtk-randomize State 14 Disable

Step 10 Click **Apply**.

Configuring Fast Transition Roaming using CLI

To configure FT Roaming, enter the following commands:

config wlan security ft {**enable** | **disable**} *wlan-id*	Enable or disable 802.11r fast transition parameters.
config wlan security ft over-the-ds {**enable** | **disable**} *wlan-id*	Enable or disable 802.11r fast transition parameters over a distributed system. This is disabled, by default.
config wlan security ft reassociation-timeout timeout-in-seconds *wlan-id*	Enables 802.11r fast transition reassociation timeout. The range is between 1 to 100 seconds.

The WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

```
config wlan security wpa akm ft-psk {enable | disable} wlan-id
config wlan security wpa akm ft-802.1X {enable | disable} wlan-id
```

Enable or disable the AKM for FT over a DS, enter the following command:

```
config wlan security wpa akm ft over-the-ds {enable | disable} wlan-id
```

To view the WLAN and FT parameters on the WLAN, enter the following command:

```
show wlan wlan-id
```

Troubleshooting Support

- Enable or disable debugging of FT events, using the following command:

  ```
  debug ft events {enable | disable}
  ```

- Enable or disable debugging of key generation for FT, using the following command:

  ```
  debug ft keys {enable | disable}
  ```

Restrictions for 802.11r Fast Transition

- 802.11r FT feature does not support Mesh APs.
- 802.11r FT feature is not supported on Linux-based APs such as Cisco 600 Series OfficeExtend APs.
- 802.11r fast roaming is not supported on FlexConnect APs in standalone mode.
- 802.11r fast roaming between local authentication and central authentication WLAN is not supported with FlexConnect APs.
- 802.11r fast roaming is not supported if the client uses Over-the-DS pre-authentication in standalone mode on FlexConnect access points.
- The EAP LEAP method is not supported. The WAN link latency prevents association time to a maximum of 2 seconds.
- When a FlexConnect AP moves to standalone mode, existing clients connects until the session timer expires. A new 11r client does not accept while the AP is in standalone mode.
- 802.11r fast roaming does not support Traffic Specification (TSPEC). Therefore, it does not support RIC IE handling.
- If the WAN link latency exists for FlexConnect APs, fast roaming delays. Verify the voice or data maximum latency. The controller handles 802.11r FT authentication request during roaming for both Over-the-Air and Over-the-DS methods.
- The 802.11r FT feature supports only on open and WPA2 configured WLANs.
- Few legacy clients cannot associate with a WLAN that has 802.11r enabled, if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can associate with non-802.11r WLANs. Clients that are 802.11r capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled. The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r enabled WLANs. Another workaround is to have two SSIDs with the same name but with different security settings (FT and non-FT).
- 802.11r does not support FT resource request protocol because there are no clients to implement FT resource request protocol. Also, the resource request protocol is optional in the 802.11r amendment.
- To avoid any Denial of Service (DoS) attack, each controller allows a maximum of three FT handshakes with different APs.

802.11k Assisted Roaming

The 802.11k allows 11k capable clients to request a neighbor report containing information about known neighbor APs that are candidates for roaming.

To facilitate roaming, an 11k capable client associated with an AP sends request to a list of neighbor APs. The request is send in the form of an 802.11 management frame, known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with their Wi-Fi channel numbers. The response is also an action frame. The client identifies the APs candidates for the next roam from the response frame. The use of 802.11k radio resource management (RRM) process allows the client to roam efficiently and quickly.

To find an AP to roam from the neighbor list information, the 11k capable client does not probe all of the 2.4 GHz and 5 GHz channels. Client does not probe all the channels to reduce channel utilization, thereby, it increases bandwidth on all channels. It reduces roam time and improves the decisions taken by the client. Additionally, it increases battery life of the device as it neither changes the radio configuration for each channel nor sends probe requests on each channel. It avoids the device to process all the probe response frames.

Assisted Roaming with 802.11k

The 802.11k standard allows clients to request neighbor reports containing information about known neighbor APs that are candidates for a service set transition. The use of the 802.11k neighbor list can limit the need for active and passive scanning.

The assisted roaming feature is based on an intelligent and client optimized neighbor list. The 802.11k neighbor list is generated dynamically on-demand and is not maintained on the controller. Two clients on the same controller but different APs can have different neighbor lists delivered depending on their individual relationship with the surrounding APs.

By default, the neighbor list contains only neighbors in the same band with which the client is associated. However, the dual-list configuration allows 802.11k to return neighbors in both bands.

Clients send requests for neighbor lists only after they associate with the APs that advertise the Radio Management (RM) capability Information Element (IE) in the beacon. The neighbor list includes information about BSSID, channel, and operation details of the neighboring radios.

Assembling and Optimizing the Neighbor List

When the controller receives a request for an 802.11k neighbor list, the following occurs:

1. The controller searches the RM neighbor table for a list of neighbors on the same band as AP, with which the client is currently associated.
2. The controller checks the neighbors according to the Received Signal Strength Indication (RSSI) between the APs, the current location of the present AP, the floor information of the neighboring AP from Cisco Prime Infrastructure, and roaming history information on the controller to reduce the list of neighbors to six per band. The list is optimized for APs on the same floor.

802.11k Information Elements (IEs)

Clients send requests for neighbor lists only after they associate with the APs that advertise the RM capability Information Element (IE) in the beacon.

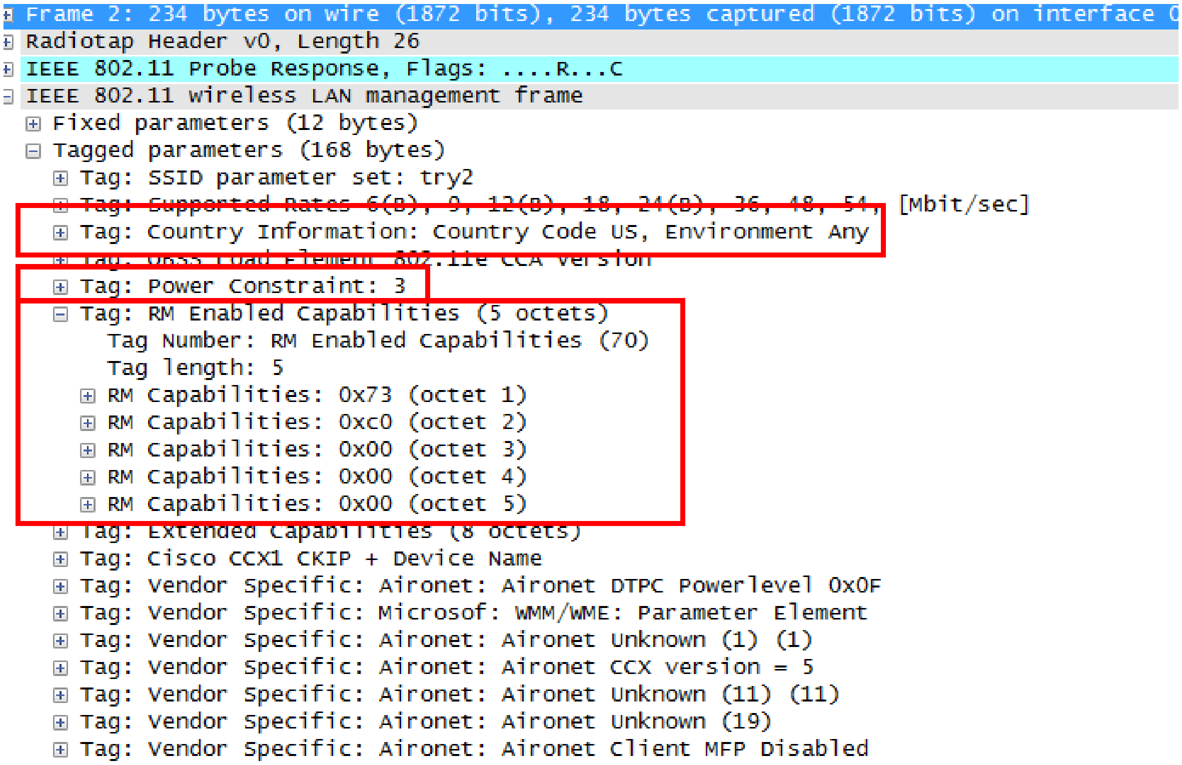
The following elements are implemented in the beacon and probe response on the AP to ensure smooth integration with Apple handheld devices:

- *Country Element*—The Country Information Element contains the information required to allow a station to identify the regulatory domain in which the station is located and to configure its PHY for operation in that regulatory domain.
- *Power Constraint Element*—The power constraint element contains the information necessary to allow a client to determine the local maximum transmit power in the current channel.
- *RM Enable Capabilities Element*—The RM Capabilities element is five octets long. When this element is included in a beacon or probe response, it uses bit 1 to signal so that the AP can provide neighbor list. When used in an association request, bit 1 signifies the client's request for a neighbor list.

The presence of all three of these IEs signifies that this SSID is configured to provide a neighbor list on request. For this release we send neighbor list based on the request from the client and not on the neighbor list capability of the client in the IE.

The following Wireshark capture displays these information elements:

Figure 11-9 802.11k information elements



```
⊞ Frame 2: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface
⊞ Radiotap Header v0, Length 26
⊞ IEEE 802.11 Probe Response, Flags: ....R...C
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊟ Tagged parameters (168 bytes)
    ⊞ Tag: SSID parameter set: try2
    ⊞ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    ⊞ Tag: Country Information: Country Code US, Environment Any
    ⊞ Tag: QBSS Load Element 802.11e CCA Version
    ⊞ Tag: Power Constraint: 3
    ⊟ Tag: RM Enabled Capabilities (5 octets)
        Tag Number: RM Enabled Capabilities (70)
        Tag length: 5
      ⊞ RM Capabilities: 0x73 (octet 1)
      ⊞ RM Capabilities: 0xc0 (octet 2)
      ⊞ RM Capabilities: 0x00 (octet 3)
      ⊞ RM Capabilities: 0x00 (octet 4)
      ⊞ RM Capabilities: 0x00 (octet 5)
    ⊞ Tag: Extended Capabilities (8 octets)
    ⊞ Tag: Cisco CCX1 CKIP + Device Name
    ⊞ Tag: Vendor Specific: Aironet: Aironet DTPC Powerlevel 0x0F
    ⊞ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    ⊞ Tag: Vendor Specific: Aironet: Aironet Unknown (1) (1)
    ⊞ Tag: Vendor Specific: Aironet: Aironet CCX version = 5
    ⊞ Tag: Vendor Specific: Aironet: Aironet Unknown (11) (11)
    ⊞ Tag: Vendor Specific: Aironet: Aironet Unknown (19)
    ⊞ Tag: Vendor Specific: Aironet: Aironet Client MFP Disabled
```

Configuring Assisted Roaming using GUI

To configure Fast Transition Roaming using GUI, perform the following steps:

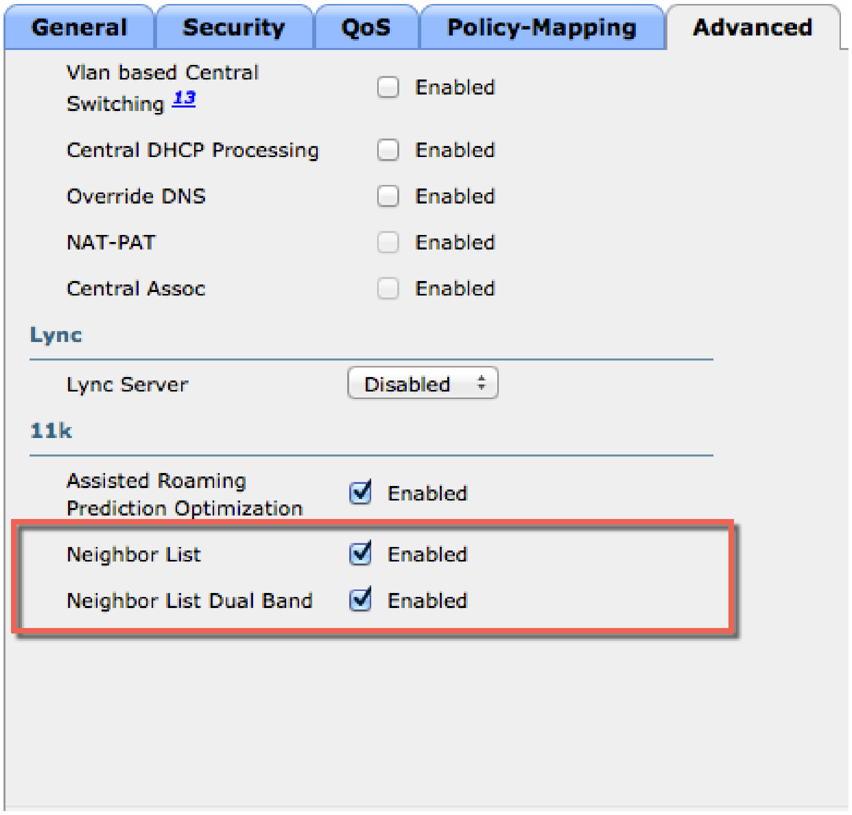
Step 1 Click **WLANs**.

Step 2 Choose **WLAN ID > Edit page**.

Step 3 Click **Advanced** tab.

Step 4 In the **11k** area, check the **Neighbor List** and **Neighbor List Dual Band** check box.

Figure 11-10 Advanced Tab - Neighbor List



Vlan based Central Switching 13 ☐ Enabled
Central DHCP Processing ☐ Enabled
Override DNS ☐ Enabled
NAT-PAT ☐ Enabled
Central Assoc ☐ Enabled

Lync

Lync Server: Disabled

11k

Assisted Roaming Prediction Optimization ☑ Enabled
Neighbor List ☑ Enabled
Neighbor List Dual Band ☑ Enabled

Configuring Assisted Roaming using CLI

To configure Assisted Roaming enter the following commands:

config wlan assisted-roaming neighbor-list enable *wlan-id*	Configures an 802.11k neighbor list for a WLAN. By default, assisted roaming is enabled on the neighbor list when you create a WLAN. The no form of the command disables assisted roaming neighbor list.
config wlan assisted-roaming dual-list enable *wlan-id*	Configures a dual-band 802.11k dual list for a WLAN. By default, assisted roaming is enabled on the dual list when you create a WLAN. The no form of the command disables assisted roaming dual list.
config wireless assisted-roaming floor-bias *dBm*	Configures neighbor floor label bias. The valid range is from 5 to 25 dBm, and the default value is 15 dBm.

Prediction Based Roaming-Assisted Roaming for Non-802.11k Clients

You can optimize roaming for non-802.11k clients by generating a prediction neighbor list for each client without sending an 802.11k neighbor list request. When prediction based roaming enables a WLAN, after each successful client association/re-association, the same neighbor list optimization applies on the non-802.11k client to generate and store the neighbor list in the mobile station software data structure. Clients at different locations have different lists because the client probes are seen with different RSSI values by the different neighbors as the clients usually probe before any association or re-association. This list is created with the most updated probe data and predicts the next AP that the client is likely to roam to.

The wireless infrastructure discourages clients from roaming to those less desirable neighbors by denying association if the association request to an AP does not match the entries on the stored prediction neighbor list.

- **Denial count**—Maximum number of times a client is refused association.
- **Prediction threshold**—Minimum number of entries required in the prediction list for the assisted roaming feature to activate.

Configuring Prediction Based Roaming using GUI

To configure Prediction Based Roaming using GUI, perform the following steps:

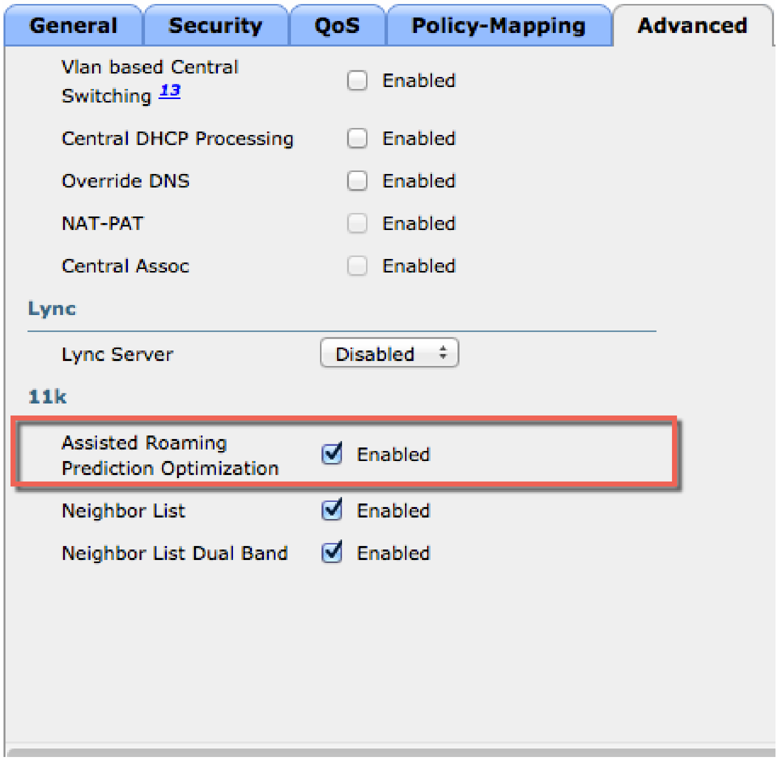
Step 1 Click **WLANs**.

Step 2 Choose **WLAN ID > Edit page**.

Step 3 Click **Advanced** tab.

Step 4 In the **11k** area, check the **Assisted Roaming Prediction Optimization** check box.

Figure 11-11 Advanced Tab - Assisted Roaming Prediction Optimization



Vlan based Central Switching 13 ☐ Enabled

Central DHCP Processing ☐ Enabled

Override DNS ☐ Enabled

NAT-PAT ☐ Enabled

Central Assoc ☐ Enabled

Lync

Lync Server Disabled

11k

Assisted Roaming Prediction Optimization ☑ Enabled

Neighbor List ☑ Enabled

Neighbor List Dual Band ☑ Enabled

Configuring Prediction Based Roaming using CLI

To configure Prediction Based Roaming enter the following commands:

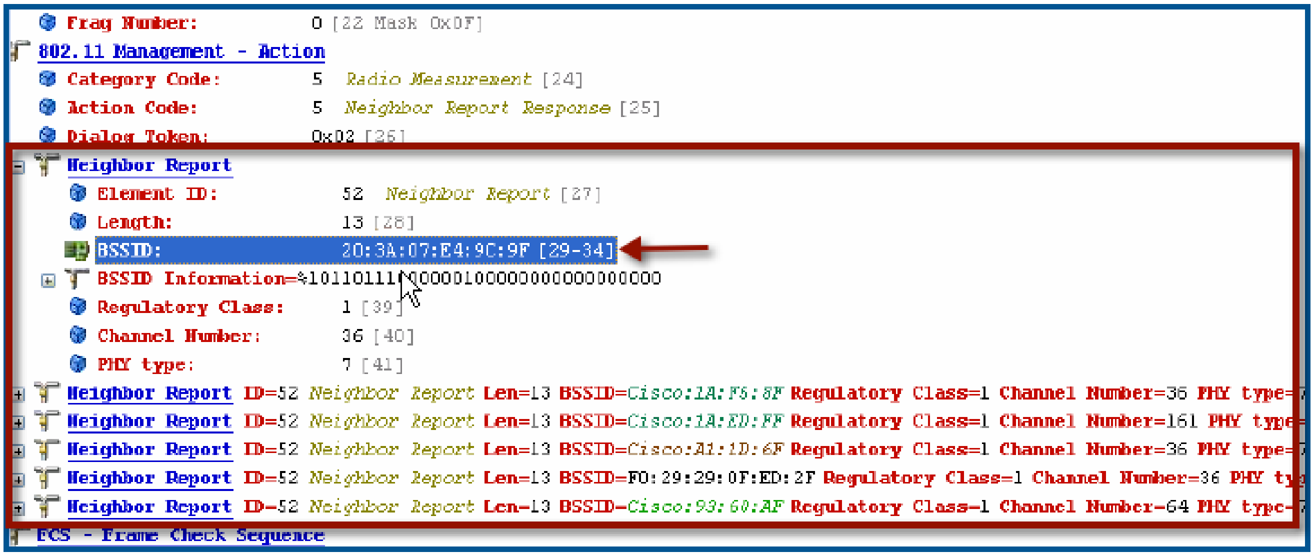
config wlan assisted-roaming prediction {**`enable`** | **`disable`**} *wlan-id*	Configures assisted roaming prediction list for a WLAN. By default, the assisted roaming prediction list is disabled. **Note** A warning message is displayed and load balancing is disabled for the WLAN, if load balancing is already enabled for the WLAN.

config assisted-roaming denial-maximum *count*	Configures the maximum number of times a client can deny association if the association request is sent to an AP which does not match any AP on the prediction. The valid range is from 1 to 10, and the default value is 5.
config assisted-roaming prediction-minimum *count*	Configures the minimum number of predicted APs required for the prediction list to activate. The default value is 3. **Note** If the number of AP in the prediction assigned to the client is less than the number that you specify, the assisted roaming does not apply on this roam.

Neighbor List Response

The neighbor list includes information about BSSID, channel and operation details of the neighboring radios as shown in the Wireshark capture below:

Figure 11-12 802.11k Neighbor Report



```
Frag Number:             0 [22 Mask 0x0F]
802.11 Management - Action
  Category Code:         5  Radio Measurement [24]
  Action Code:           5  Neighbor Report Response [25]
  Dialog Token:          0x02 [26]
  Neighbor Report
    Element ID:             52  Neighbor Report [27]
    Length:                 13 [28]
    BSSID:                  20:3A:07:E4:9C:9F [29-34]
    BSSID Information=%10110111 000010000000000000000000
    Regulatory Class:       1 [39]
    Channel Number:         36 [40]
    PHY type:               7 [41]
  Neighbor Report ID=52 Neighbor Report Len=13 BSSID=Cisco:1A:F5:8F Regulatory Class=1 Channel Number=36 PHY type=
  Neighbor Report ID=52 Neighbor Report Len=13 BSSID=Cisco:1A:ED:FF Regulatory Class=1 Channel Number=161 PHY type
  Neighbor Report ID=52 Neighbor Report Len=13 BSSID=Cisco:A1:1D:6F Regulatory Class=1 Channel Number=36 PHY type=
  Neighbor Report ID=52 Neighbor Report Len=13 BSSID=F0:29:29:0F:ED:2F Regulatory Class=1 Channel Number=36 PHY ty
  Neighbor Report ID=52 Neighbor Report Len=13 BSSID=Cisco:93:60:AF Regulatory Class=1 Channel Number=64 PHY type=
FCS - Frame Check Sequence
```

Troubleshooting Support

- Debug a client for assisted roaming, using the following command:

  debug mac addr *client-mac-addr*

- Configure the debugging of all of the 802.11k events, using the following command:

  debug 11k all {**enable** | **disable**}

- Configure the debugging of neighbor details, using the following command:

  debug 11k detail {**enable** | **disable**}

- Configure the debugging of 802.11k errors, using the following command:

```
debug 11k errors {enable | disable}
```

- Verify the neighbor requests that are received, using the following command:

```
debug 11k events {enable | disable}
```

- Configure the debugging of the client roaming history, using the following command:

```
debug 11k history {enable | disable}
```

- Configure the debugging of 802.11k optimizations, using the following command:

```
debug 11k optimization {enable | disable}
```

- Get details of client roaming parameters that are to be imported for offline simulation, using the following command:

```
debug 11k simulation {enable | disable}
```

802.11v Max Idle Period, Directed Multicast Service

From Release 8.0, controller supports 802.11v amendment for wireless networks, which describes enhancements to wireless network management, such as:

- Network assisted Power Savings—Helps clients to improve battery life by enabling them to sleep longer. For example, mobile devices use a certain amount of idle period to ensure that they remain connected to access points and therefore consume more power when performing the following tasks in a wireless network.
- Network assisted Roaming—Enables the WLAN to send messages to associated clients, for better APs to associate with clients. This is useful for both load balancing and in directing poorly connected clients.

Enabling 802.11v Network Assisted Power Savings

Wireless devices consume battery to maintain their connection to the clients, in several ways:

- By waking up at regular intervals to listen to the access point beacons containing a DTIM, which indicates buffered broadcast or multicast traffic that the AP will deliver to the clients.
- By sending null frames to the access points, in the form of keep alive messages to maintain connection with APs.
- Devices also periodically listen to beacons (even in the absence of DTIM fields) to synchronize their clock to that of the corresponding AP.
- All these processes consume battery and this consumption impacts some devices (such as Apple), because these devices use conservative session timeout estimation, and therefore, wake up often to send keep alive messages. The 802.11 standard, without 802.11v, does not include any mechanism for the controller or the access points to communicate to the wireless clients about the session timeout for the local client.

To save the power of clients, the following features in the 802.11v standard are used:

- Directed Multicast Service (DMS)
- Base Station Subsystem (BSS) Maximum Idle Period

Directed Multicast Service

The client requests the access point to transmit the required multicast packet as unicast frames. This allows the client to receive the multicast packets that are ignored in sleep mode and also ensures Layer 2 reliability. The unicast frame is transmitted to the client at a potentially higher wireless link rate, which enables the client to receive the packet quickly by enabling the radio for a shorter duration, thus saves battery power. Since the wireless client does not wake up at each DTIM interval to receive multicast traffic, thus allows longer sleeping intervals.

Base Station Subsystem Maximum Idle Period

The BSS Max Idle period is the time frame during which an AP does not disassociate a client due to non-receipt of frames from the connected client. This ensures that the client device does not send keep alive messages frequently. The idle period timer value is transmitted using the association and re-association response frame from the AP to the client. The idle time value indicates the maximum time a client can remain idle without transmitting any frame to an AP. As a result, the clients remain in sleep mode for a longer duration without transmitting the keep alive messages. This in turn saves battery power.

Configuring 802.11v Network Assisted Power Savings using CLI

- Configure the value of BSS Max Idle period, using the following commands:

```
config wlan usertimeout wlan-id
config wlan bssmaxidle {enable | disable} wlan-id
```

- Configure the DMS, using the following command:

```
config wlan dms {enable | disable} wlan-id
```

Monitoring 802.11v Network Assisted Power Savings

- Display the DMS information on each radio slot on an AP, using the following command:

```
show controller d1/d0 | begin DMS
```

- Track the DMS requests processed by the controller, using the following commands:

```
debug 11v all {enable | disable}
debug 11v errors {enable | disable}
debug 11v detail {enable | disable}
```

Troubleshooting Support

- Enable or disable 802.11v debug, using the following command on the WLC:

```
debug 11v detail
```

- Track the DMS requests processed by an access point, using the following command on the AP:

```
debug dot11 dot11v
```

Managing 802.11v BSS Transition

802.11v BSS Transition is applied to the following three scenarios:

- **Solicited request**—Client can send an 802.11v BSS Transition Management Query before roaming for a better option of AP to re-associate with a client.
- **Unsolicited Load Balancing request**—If an AP is heavily loaded, it sends out an 802.11v BSS Transition Management Request to an associated client.
- **Unsolicited Optimized Roaming request**—If a client's RSSI and rate do not meet the requirement, AP sends out an 802.11v BSS Transition Management Request to this client.

802.11v BSS Transition Management Request is a suggestion given to client. Client can make its own decision whether to follow the suggestion or not. To force disassociating a client, you can turn on the disassociation-imminent function. This function is to disassociate the client after a period of time if the client does not re-associate to another AP.

Optimized Roaming + 802.11v

Disassociation function

Optimized Roaming behavior: Check client stats every 90 seconds(or less), if RSSI fails & data rate fails, disassociate the client.

Optimized Roaming + 802.11v behavior: If client is BSS Transition capable, instead of disassociating the client, send the client BSS Transition Request

Association RSSI check

Optimized Roaming behavior: During client association, check client RSSI. If RSSI check fails, don't allow the client to associate.

Optimized Roaming + 802.11v behavior: If client is BSS Transition capable, allow the client to associate, but also send the client BSS Transition Request

Load Balancing + 802.11v

Similar to Optimized roaming, If we just reject the client when Load Balancing fails then client might not have a clear sense of which AP to associate to and would most likely retry the same loaded AP over and over again.

With 11v BSS Transition, the client will not try the loaded AP but has the opportunity to pick an AP from the provided list to join.

Configuring 802.11v BSS Transition Management using GUI

To configure 802.11v BSS Transition Management using GUI, perform the following steps:

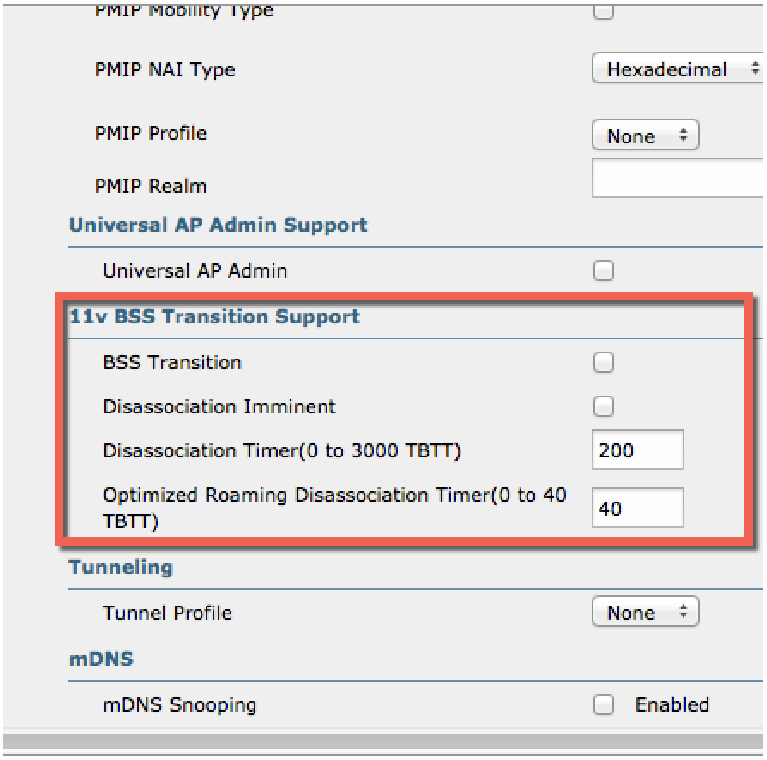
Step 1 Click **WLANs**.

Step 2 Choose **WLAN ID > Edit page**.

Step 3 Click **Advanced** tab.

Step 4 In the **11v BSS Transition Support** area, enter the values in the **Disassociation Time** and **Optimized Roaming Disassociation Timer** fields.

Figure 11-13 Advanced Tab - 11v BSS Transition Support



PMIP Mobility Type ☐

PMIP NAI Type: Hexadecimal

PMIP Profile: None

PMIP Realm

Universal AP Admin Support

Universal AP Admin ☐

11v BSS Transition Support

BSS Transition ☐

Disassociation Imminent ☐

Disassociation Timer(0 to 3000 TBTT): 200

Optimized Roaming Disassociation Timer(0 to 40 TBTT): 40

Tunneling

Tunnel Profile: None

mDNS

mDNS Snooping ☐ Enabled

Configuring 802.11v BSS Transition Management using CLI

To enable 802.11v BSS transition management on a controller, enter the following commands:

config wlan bss-transition enable *wlan-id*	Enables 802.11v BSS transition.
config wlan disassociation-imminent enable *wlan-id*	Disassociates the STA.
config wlan bss-transition disassociation-imminent oproam-timer *<timer> <WLAN id>*	For Unsolicited Optimized Roaming Requests (TBTT = beacon intervals).
config wlan bss-transition disassociation-imminent timer *<timer> <WLAN id>*	For solicited and unsolicited requests.

Troubleshooting 11v BSS transition

To troubleshoot 802.11v BSS transition, enter the following command:

```
debug 11v all
```

Restrictions

Client needs to support 802.11v BSS transition.

802.11w Protected Management Frames

Wi-Fi is a broadcast medium that enables any device to eavesdrop and participate either as a legitimate or rogue device. Management frames such as authentication, de-authentication, association, dissociation, beacons, and probes are used by wireless clients to initiate and teardown sessions for network services. Unlike data traffic, which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to attack a client associated with the AP.

The 802.11w protocol applies only to a set of robust management frames that are protected by the Protected Management Frames (PMF) service. These include Disassociation, De-authentication, and Robust Action frames.

The following management frames are considered as robust action and therefore protected:

- Spectrum Management
- QoS
- DLS
- Block Ack
- Radio Measurement
- Fast BSS Transition
- SA Query
- Protected Dual of Public Action
- Vendor-specific Protected

When 802.11w is implemented in the wireless medium, the following actions occur:

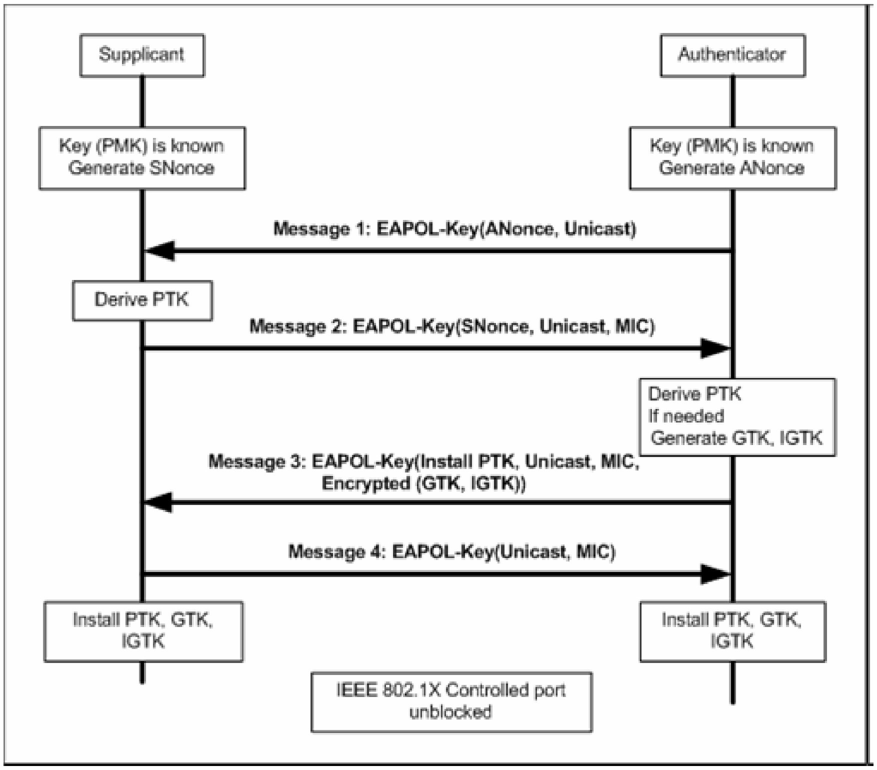
- **Client protection** is achieved by the AP, by adding cryptographic protection for de-authentication and dissociation frames thus prevents them from spoofing in a DOS attack.
- **Infrastructure protection** is achieved by adding a Security Association (SA) teardown protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.

802.11w has introduced a new IGTK Key, which is used to protect broadcast/multicast robust management frames.

- **IGTK** is a random value, assigned by the authenticator STA (WLC) and transmitted to the AP. It is used to protect MAC management protocol data units (MMPDUs) from that AP.

When Management Frame Protection is negotiated, the AP encrypts the GTK and IGTK values in the EAPOL-Key frame, which is delivered in message 3 of 4-way handshake.

Figure 11-14 IGTK exchange in 4-way handshake

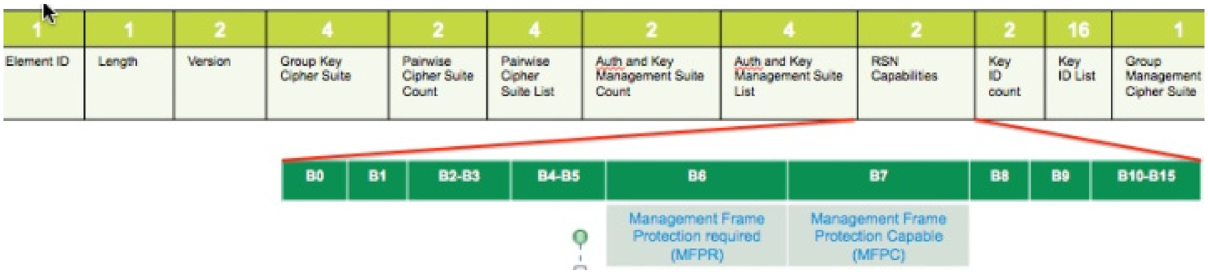

Supplicant
Authenticator
Key (PMK) is known
Generate SNonce
Key (PMK) is known
Generate ANonce
Message 1: EAPOL-Key(ANonce, Unicast)
Derive PTK
Message 2: EAPOL-Key(SNonce, Unicast, MIC)
Derive PTK
If needed
Generate GTK, IGTK
Message 3: EAPOL-Key(Install PTK, Unicast, MIC, Encrypted (GTK, IGTK))
Message 4: EAPOL-Key(Unicast, MIC)
Install PTK, GTK, IGTK
Install PTK, GTK, IGTK
IEEE 802.1X Controlled port unblocked

If the AP later changes the GTK, it sends the new GTK and IGTK to the client using the Group Key Handshake.

802.11w defines a new Broadcast/Multicast Integrity Protocol (BIP) that provides data integrity and replay protection for broadcast/multicast robust management frames after successful establishment of an IGTKSA. It adds a MIC that is calculated using the shared IGTK key.

802.11w Information Elements (IEs)

Figure 11-15 802.11w IEs


1
1
2
4
2
4
2
4
2
2
16
1
Element ID
Length
Version
Group Key Cipher Suite
Pairwise Cipher Suite Count
Pairwise Cipher Suite List
Auth and Key Management Suite Count
Auth and Key Management Suite List
RSN Capabilities
Key ID count
Key ID List
Group Management Cipher Suite
B0
B1
B2-B3
B4-B5
B6
B7
B8
B9
B10-B15
Management Frame Protection required (MFPR)
Management Frame Protection Capable (MFPC)

1. Modifications are performed in the RSN capabilities field of RSNIE.

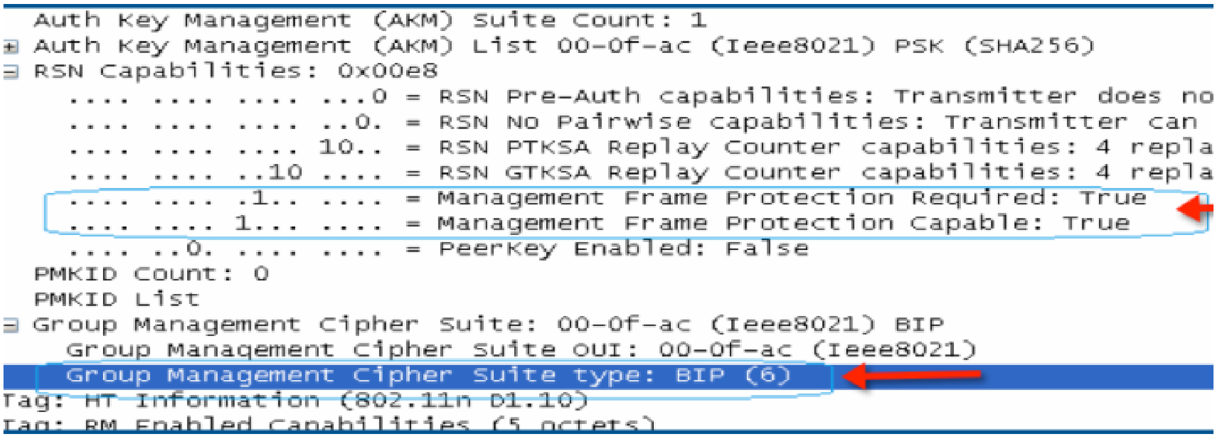
   - Bit 6: Management Frame Protection Required (MFPR)
   - Bit 7: Management Frame Protection Capable (MFPC)

2. Two new AKM Suites 5 and 6 are added for AKM Suite Selectors.
3. New Cipher Suite with type 6 is added to accommodate BIP.

The WLC adds the modified RSNIE in association and re-association responses. The APs add the modified RSNIE in beacons and probe responses.

The following Wireshark captures shows the RSNIE capabilities and the Group Management Cipher Suite elements:

Figure 11-16 802.11w information elements



```
  Auth Key Management (AKM) Suite Count: 1
⊞ Auth Key Management (AKM) List 00-0f-ac (Ieee8021) PSK (SHA256)
⊟ RSN Capabilities: 0x00e8
    .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does no
    .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can
    .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 repla
    .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 repla
    .... .... .1.. .... = Management Frame Protection Required: True
    .... .... 1... .... = Management Frame Protection Capable: True
    .... ..0. .... .... = PeerKey Enabled: False
  PMKID Count: 0
  PMKID List
⊟ Group Management Cipher Suite: 00-0f-ac (Ieee8021) BIP
    Group Management Cipher Suite OUI: 00-0f-ac (Ieee8021)
    Group Management Cipher Suite type: BIP (6)
Tag: HT Information (802.11n D1.10)
Tag: RM Enabled Capabilities (5 octets)
```

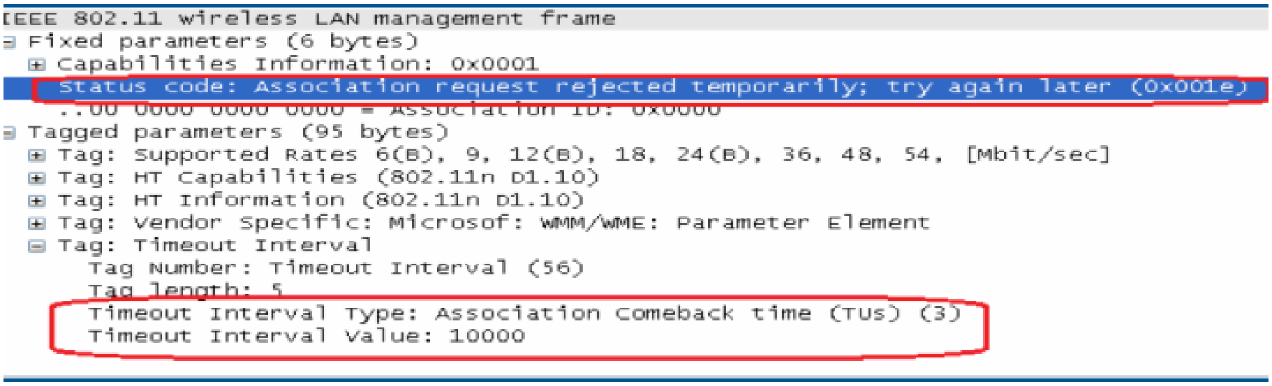
Security Association Teardown Protection

The Security Association (SA) teardown protection is a mechanism to prevent replay attacks from tearing down the session of an existing client. It consists of an Association Comeback Time and an SA-Query procedure preventing spoofed association requests from disconnecting an already connected client.

If a client has a valid security association, and has negotiated 802.11w, the AP shall reject another Association Request with status code 30. This status code means "Association request rejected temporarily; Try again later". The AP must not tear down or modify the state of the existing association until the SA-Query procedure determines the original SA is invalid and shall include in the Association Response an Association Comeback Time information element, specifying a comeback time when the AP is ready to accept an association with this client.

The following figure shows the Association Reject message with status code 0x1e (30) and the Association comeback time set to 10 seconds.

Figure 11-17 Association reject with Comeback time



```
IEEE 802.11 wireless LAN management frame
⊟ Fixed parameters (6 bytes)
  ⊞ Capabilities Information: 0x0001
    Status code: Association request rejected temporarily; try again later (0x001e)
    ..00 0000 0000 0000 = Association ID: 0x0000
⊟ Tagged parameters (95 bytes)
  ⊞ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
  ⊞ Tag: HT Capabilities (802.11n D1.10)
  ⊞ Tag: HT Information (802.11n D1.10)
  ⊞ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
  ⊟ Tag: Timeout Interval
      Tag Number: Timeout Interval (56)
      Tag length: 5
      Timeout Interval Type: Association Comeback time (TUs) (3)
      Timeout Interval Value: 10000
```

If the AP is not already engaged in an SA query with the client, the AP shall issue an SA query until a matching SA query response is received or the Association Comeback time expires. An AP may interpret reception of a valid protected frame as an indication of a successfully completed SA query. If an SA query response with a matching transaction identifier is not received within the time period, the AP shall allow the association process to start without additional SA Query procedures.

Configuring Protected Management Frames using GUI

To configure Protected Management Frames using GUI, perform the following steps:

Step 1 Click **WLANs**.

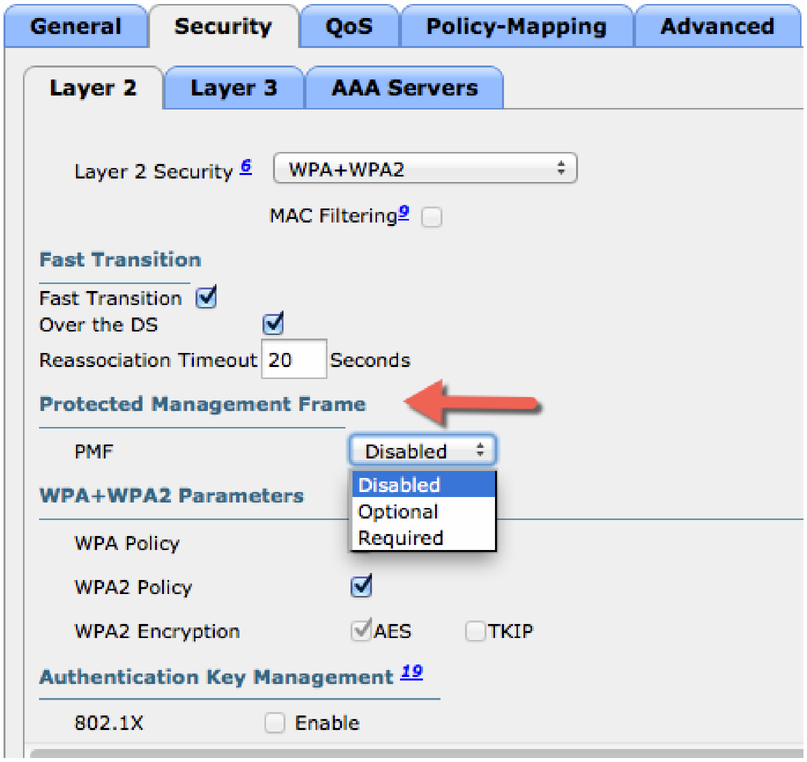
Step 2 Choose **WLAN ID > Edit page**.

Step 3 Choose **Security > Layer 2** tab.

Step 4 Choose **WPA+WPA2** from the drop-down list.

Note The 802.11w IGTK key is derived using the 4-way handshake. The key can only be used on WLANs that are configured for WPA2 security at layer 2.

Figure 11-18 Security - Layer 2 - Protected Management Frame 1



Layer 2 Security [6] WPA+WPA2

MAC Filtering[9] ☐

Fast Transition

Fast Transition ☑

Over the DS ☑

Reassociation Timeout 20 Seconds

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy ☑

WPA2 Encryption ☑AES ☐TKIP

Authentication Key Management [19]

802.1X ☐ Enable

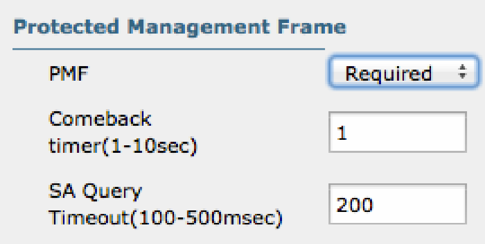
Step 5 In the **Protected Management Frame** area, choose the **PMF** state from the drop-down list. The following options are available:

- **Disabled**— Disables 802.11w MFP protection on a WLAN.
- **Optional**— To be used if the client supports 802.11w.
- **Required**— Ensures that the clients that do not support 802.11w cannot associate with the WLAN.

Step 6 If you choose the PMF state as either **Optional** or **Required**, perform the following:

- In the **Comeback timer** field, enter the association comeback interval in milliseconds. The comeback interval is the time within which the access point re-associates with the client after a valid security association.
- In the **SA Query Timeout** field, enter the maximum time before a Security Association (SA) query times out.

Figure 11-19 Security - Layer 2 - Protected Management Frame 2



Protected Management Frame

PMF	Required
Comeback timer(1-10sec)	1
SA Query Timeout(100-500msec)	200

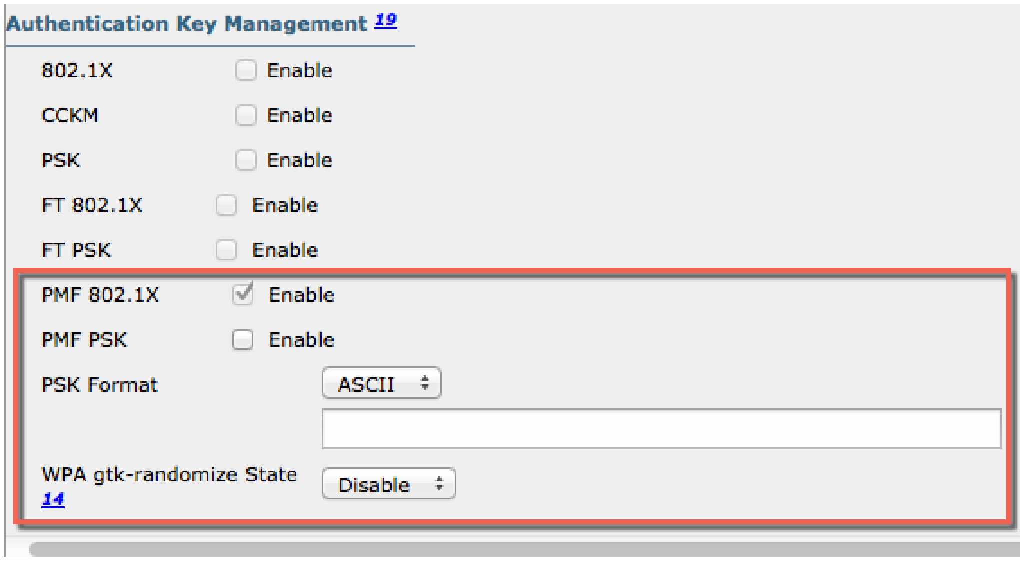
Step 7 In the **Authentication Key Management** area, perform the following:

- Check or uncheck the **PMF 802.1X** check box to configure the 802.1X authentication for the protection of management frames.
- Check or uncheck the **PMF PSK** check box to configure the pre-shared keys for PMF.
- From the PSK Format drop-down list, choose ASCII or Hexadecimal and enter the PSK value.

Step 8 Click **Apply**.

Step 9 Click **Save Configuration**.

Figure 11-20 Authentication Key Management



Authentication Key Management 19

802.1X	☐ Enable
CCKM	☐ Enable
PSK	☐ Enable
FT 802.1X	☐ Enable
FT PSK	☐ Enable
PMF 802.1X	☑ Enable
PMF PSK	☐ Enable
PSK Format	ASCII
WPA gtk-randomize State 14	Disable

Configuring Protected Management Frames using CLI

To configure Protected Management Frames, enter the following commands:

Config wlan security pmf {**disable** | **optional** | **required**} *wlan-id*	Configure the PMF parameters with the following options: • Association-comeback—Configures the 802.11w association. The range is from 1to20 seconds. • Required— Requires clients to negotiate 802.11w MFP protection on a WLAN. • Optional— Enables 802.11w MFP protection on a WLAN. • Saquery-retry-time— Time interval identified in milliseconds in the association response to an already associated client before the association can be tried again. This time interval checks if the client is a real client and not a rogue client during the association comeback time. If the client does not respond within this time, the client association is deleted from the controller. The saquery retry time in milliseconds. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.
Config wlan security pmf association-comeback *timeout-in-seconds wlan-id*	
Config wlan security pmf saquery-retrytimeout *timeout-in-milliseconds wlan-id*	

WLAN configuration contains a new Authenticated Key Management (AKM) type called Protected Management Frames (PMF).

- Configure the 802.1X authentication for PMF, using the following command:

  ```
  config wlan security wpa akm pmf 802.1x {enable | disable} wlan-id
  ```

- Configure the pre-shared key support for PMF, using the command:

  ```
  config wlan security wpa akm pmf psk {enable | disable} wlan-id
  ```

- Configure a pre-shared key for a WLAN, using the following command:

  ```
  config wlan security wpa akm psk set-key {ascii | hex} psk wlan-id
  ```

Note 802.11w cannot be enabled on WLANs of None, WEP-40, WEP-104, and WPA (AES or TKIP) encryption.

Monitoring 802.11w

To display the WLAN and PMF parameters on the WLAN, enter the following command:

```
show wlan wlan-id
```

Troubleshooting Support

To configure the debugging of PMF, enter the following command:

```
debug pmf events {enable | disable}
```