Cisco Wireless LAN Controller
Configuration Guide
Software Release 7.2
February 2012

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.
CONTENTS

Preface xxxix
Audience xI
Purpose xI
Organization xI
Conventions xli
Related Documentation xliii
Obtaining Documentation and Submitting a Service Request xliv

CHAPTER 1

Overview 1-1
Cisco Unified Wireless Network Solution Overview 1-1
   Single-Controller Deployments 1-3
   Multiple-Controller Deployments 1-3
Operating System Software 1-4
Operating System Security 1-4
   Cisco WLAN Solution Wired Security 1-5
Layer 2 and Layer 3 Operation 1-5
   Operational Requirements 1-6
   Configuration Requirements 1-6
Cisco Wireless LAN Controllers 1-6
   Client Location 1-7
Controller Platforms 1-7
   Cisco 2500 Series Controller 1-7
      Features Not Supported 1-8
   Cisco 5500 Series Controllers 1-8
      Features Not Supported 1-8
   Cisco Flex 7500 Series Controller 1-9
      Features Not Supported 1-9
   Cisco Wireless Services Module 2 1-9
      Features Not Supported 1-10
   Cisco Wireless Controller on Cisco Services-Ready Engine (SRE) 1-10
      Features Not Supported 1-11
Cisco UWN Solution Wired Connections 1-11
Using the Web-Browser and CLI Interfaces 2-1

Configuring the Controller Using the GUI Configuration Wizard 2-1
  Connecting the Controller's Console Port 2-1
  Configuring the Controller (GUI) 2-2
  Additional References 2-13

Configuring the Controller Using the CLI Configuration Wizard 2-13
  Guidelines and Limitations 2-14
  Configuring the Controller (CLI) 2-14

Using the Controller Web GUI 2-16
  Guidelines and Limitations 2-17
  Logging On to the GUI 2-17
  Logging Out of the GUI 2-17
  Enabling Web and Secure Web Modes 2-18
    Enabling Web and Secure Web Modes (GUI) 2-18
    Enabling Web and Secure Web Modes (CLI) 2-19

Loading an Externally Generated SSL Certificate 2-20
  Guidelines and Limitations 2-20
  Loading an SSL Certificate 2-20
    Loading an SSL Certificate (GUI) 2-20
    Loading an SSL Certificate (CLI) 2-21

Using the Controller CLI 2-22
  Information About the Controller CLI 2-23
  Guidelines and Limitations 2-23
  Logging on to the Controller CLI 2-23
  Using a Local Serial Connection 2-23
  Using a Remote Ethernet Connection 2-24
  Logging Out of the CLI 2-25
  Navigating the CLI 2-25
  Additional References 2-26

Using the AutoInstall Feature for Controllers Without a Configuration 2-26
  Information About the AutoInstall Feature 2-26
  Guidelines and Limitations 2-27
<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Configuring Ports and Interfaces</th>
<th>3-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information About Ports</td>
<td>3-1</td>
<td></td>
</tr>
<tr>
<td>Information About Distribution System Ports</td>
<td>3-3</td>
<td></td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>3-3</td>
<td></td>
</tr>
<tr>
<td>Information About Service Ports</td>
<td>3-4</td>
<td></td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>3-4</td>
<td></td>
</tr>
<tr>
<td>Information About Interfaces</td>
<td>3-4</td>
<td></td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>3-5</td>
<td></td>
</tr>
<tr>
<td>Additional References</td>
<td>3-5</td>
<td></td>
</tr>
<tr>
<td>Configuring the Management Interface</td>
<td>3-5</td>
<td></td>
</tr>
</tbody>
</table>

Managing the Controller System Date and Time | 2-30 |

Information About Controller System Date and Time | 2-30 |

Guidelines and Limitations | 2-30 |

Configuring an NTP Server to Obtain the Date and Time | 2-30 |

Configuring NTP Authentication | 2-31 |

Configuring NTP Authentication (GUI) | 2-31 |

Configuring NTP Authentication (CLI) | 2-31 |

Configuring the Date and Time | 2-32 |

Configuring the Date and Time (GUI) | 2-32 |

Configuring the Date and Time (CLI) | 2-33 |

Configuring Telnet and SSH Sessions | 2-35 |

Information About Telnet and SSH | 2-35 |

Guidelines and Limitations | 2-35 |

Configuring Telnet and SSH Sessions | 2-35 |

Configuring Telnet and SSH Sessions (GUI) | 2-35 |

Configuring Telnet and SSH Sessions (CLI) | 2-37 |

Additional References | 2-38 |

Managing the Controller Wirelessly | 2-38 |

Information About Managing the Controller Wirelessly | 2-38 |

Enabling Wireless Connections | 2-38 |

Enabling Wireless Connections (GUI) | 2-38 |

Enabling Wireless Connections (CLI) | 2-39 |

2-39

Obtaining an IP Address Through DHCP and Downloading a Configuration File from a TFTP Server | 2-27 |

Selecting a Configuration File | 2-28 |

Example: AutoInstall Operation | 2-29 |

Additional References | 2-30 |
Contents

Information About the Management Interface 3-6
Guidelines and Limitations 3-6
Configuring the Management Interface 3-6
Configuring the Management Interface (GUI) 3-6
Configuring the Management Interface (CLI) 3-8
Configuring the AP-Manager Interface 3-10
Information About the AP-Manager Interface 3-10
Guidelines and Limitations 3-10
Configuring the AP-Manager Interface 3-10
Configuring the AP-Manager Interface (GUI) 3-11
Configuring the AP-Manager Interface (CLI) 3-12
Additional References 3-12
Configuring Virtual Interfaces 3-12
Information About Virtual Interfaces 3-13
Guidelines and Limitations 3-13
Configuring Virtual Interfaces 3-13
Configuring Virtual Interfaces (GUI) 3-13
Configuring Virtual Interfaces (CLI) 3-14
Configuring Service-Port Interfaces 3-15
Information About Service-Port Interfaces 3-15
Guidelines and Limitations 3-15
Configuring Service-Port Interfaces 3-15
Configuring Service-Port Interfaces (GUI) 3-15
Configuring Service-Port Interfaces (CLI) 3-16
Configuring Dynamic Interfaces 3-16
Information About Dynamic Interfaces 3-17
Guidelines and Limitations 3-17
Configuring Dynamic Interfaces 3-17
Configuring Dynamic Interfaces (GUI) 3-17
Configuring Dynamic Interfaces (CLI) 3-19
Information About Dynamic AP Management 3-21
Information About WLANs 3-21
Configuring Ports 3-23
Information About Configuring Ports 3-23
Configuring Ports (GUI) 3-23
Configuring Port Mirroring 3-25
Information About Port Mirroring 3-26
Guidelines and Limitations 3-26
Enabling Port Mirroring (GUI) 3-26
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the Spanning Tree Protocol</td>
</tr>
<tr>
<td>Information About the Spanning Tree Protocol</td>
</tr>
<tr>
<td>Configuring the Spanning Tree Protocol</td>
</tr>
<tr>
<td>Configuring the Spanning Tree Protocol (GUI)</td>
</tr>
<tr>
<td>Configuring the Spanning Tree Protocol (CLI)</td>
</tr>
<tr>
<td>Using the Cisco 5500 Series Controller USB Console Port</td>
</tr>
<tr>
<td>Installing the Cisco Windows USB Console Driver</td>
</tr>
<tr>
<td>Changing the Cisco USB Systems Management Console COM Port to an Unused Port</td>
</tr>
<tr>
<td>Choosing Between Link Aggregation and Multiple AP-Manager Interfaces</td>
</tr>
<tr>
<td>Configuring Link Aggregation</td>
</tr>
<tr>
<td>Information About Link Aggregation</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
</tr>
<tr>
<td>Enabling Link Aggregation</td>
</tr>
<tr>
<td>Enabling Link Aggregation (GUI)</td>
</tr>
<tr>
<td>Enabling Link Aggregation (CLI)</td>
</tr>
<tr>
<td>Verifying Link Aggregation Settings (CLI)</td>
</tr>
<tr>
<td>Configuring Neighbor Devices to Support Link Aggregation</td>
</tr>
<tr>
<td>Configuring Multiple AP-Manager Interfaces</td>
</tr>
<tr>
<td>Information About Multiple AP-Manager Interfaces</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
</tr>
<tr>
<td>Creating Multiple AP-Manager Interfaces</td>
</tr>
<tr>
<td>Creating Multiple AP-Manager Interfaces (GUI)</td>
</tr>
<tr>
<td>Creating Multiple AP-Manager Interfaces (CLI)</td>
</tr>
<tr>
<td>Configuration Example: Configuring AP-Manager on a Cisco 5500 Series Controller</td>
</tr>
<tr>
<td>Configuring VLAN Select</td>
</tr>
<tr>
<td>Information About VLAN Select</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
</tr>
<tr>
<td>Configuring Interface Groups</td>
</tr>
<tr>
<td>Information About Interface Groups</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
</tr>
<tr>
<td>Configuring Interface Groups</td>
</tr>
<tr>
<td>Creating Interface Groups (GUI)</td>
</tr>
<tr>
<td>Creating Interface Groups (CLI)</td>
</tr>
<tr>
<td>Adding Interfaces to Interface Groups (GUI)</td>
</tr>
<tr>
<td>Adding Interfaces to Interface Groups (CLI)</td>
</tr>
<tr>
<td>Viewing VLANs in Interface Groups (CLI)</td>
</tr>
<tr>
<td>Adding an Interface Group to a WLAN (GUI)</td>
</tr>
<tr>
<td>Adding an Interface Group to a WLAN (CLI)</td>
</tr>
<tr>
<td>Multicast Optimization</td>
</tr>
</tbody>
</table>
**Information About Multicast Optimization** | 3-50
---|---
**Configuring Multicast VLAN** | 3-50
- Configuring Multicast VLAN (GUI) | 3-50
- Configuring Multicast VLAN (CLI) | 3-50

**CHAPTER 4**

**Configuring Controller Settings** | 4-1
---|---
**Installing and Configuring Licenses** | 4-2
- Information About Installing and Configuring Licenses | 4-2
- Guidelines and Limitations | 4-2
- Obtaining an Upgrade or Capacity Adder License | 4-4
  - Information About Obtaining an Upgrade or Capacity Adder License | 4-4
  - Obtaining and Registering a PAK Certificate | 4-5
- Installing a License | 4-6
  - Installing a License (GUI) | 4-6
  - Installing a License (CLI) | 4-7
- Additional References | 4-7
- Viewing Licenses | 4-8
  - Viewing Licenses (GUI) | 4-8
  - Viewing Licenses (CLI) | 4-9
- Activating an AP-Count Evaluation License | 4-12
  - Information About Activating an AP-Count Evaluation License | 4-12
- Rehosting Licenses | 4-15
  - Information About Rehosting Licenses | 4-15
- Transferring Licenses to a Replacement Controller after an RMA | 4-19
  - Information About Transferring Licenses to a Replacement Controller after an RMA | 4-19
- Configuring the License Agent | 4-20
  - Information About Configuring the License Agent | 4-20
- Configuring 802.11 Bands | 4-23
  - Information About Configuring 802.11 Bands | 4-23
- Configuring 802.11n Parameters | 4-27
  - Information About Configuring 802.11n Parameters | 4-27
Contents

Cisco Wireless LAN Controller Configuration Guide

OL-21524-03

Configuring Aggressive Load Balancing (CLI) 4-45

Configuring Band Selection 4-46
Information About Configuring Band Selection 4-46
Guidelines and Limitations 4-46
Configuring Band Selection 4-46
Configuring Band Selection (GUI) 4-47
Configuring Band Selection (CLI) 4-48

Configuring Fast SSID Changing 4-48
Information About Configuring Fast SSID Changing 4-49
Configuring Fast SSID 4-49
Configuring Fast SSID Changing (GUI) 4-49
Configuring Fast SSID Changing (CLI) 4-49

Enabling 802.3X Flow Control 4-49

Configuring 802.3 Bridging 4-49
Information About Configuring 802.3 Bridging 4-50
Guidelines and Limitations 4-50
Configuring 802.3 Bridging 4-50
Configuring 802.3 Bridging (GUI) 4-50
Configuring 802.3 Bridging (CLI) 4-51

Configuring Multicast Mode 4-52
Information About Configuring Multicast Mode 4-52
Guidelines and Limitations 4-53
Configuring Multicast Mode 4-54
Enabling Multicast Mode (GUI) 4-54
Enabling Multicast Mode (CLI) 4-55
Viewing Multicast Groups (GUI) 4-56
Viewing Multicast Groups (CLI) 4-56
Viewing an Access Point’s Multicast Client Table (CLI) 4-57

Configuring Client Roaming 4-57
Information About Client Roaming 4-58
Intra-Controller Roaming 4-58
Inter-Controller Roaming 4-58
Inter-Subnet Roaming 4-58
Voice-over-IP Telephone Roaming 4-58
CCX Layer 2 Client Roaming 4-59
Guidelines and Limitations 4-60
Configuring CCX Client Roaming Parameters 4-60
Configuring CCX Client Roaming Parameters (GUI) 4-60
Configuring CCX Client Roaming Parameters (CLI) 4-61
Obtaining CCX Client Roaming Information (CLI) 4-62
Debugging CCX Client Roaming Issues (CLI) 4-62

Configuring IP-MAC Address Binding 4-62
  Information About Configuring IP-MAC Address Binding 4-63
  Configuring IP-MAC Address Binding (CLI) 4-63

Configuring Quality of Service 4-64
  Information About Configuring Quality of Service Profiles 4-64
  Configuring Quality of Service Profiles 4-64
    Configuring QoS Profiles (GUI) 4-64
    Configuring QoS Profiles (CLI) 4-66

Configuring Quality of Service Roles 4-67
  Information About Configuring Quality of Service Roles 4-68
  Configuring QoS Roles 4-68
    Configuring QoS Roles (GUI) 4-68
    Configuring QoS Roles (CLI) 4-69

Configuring Voice and Video Parameters 4-71
  Information About Configuring Voice and Video Parameters 4-71
    Call Admission Control 4-72
    Expedited Bandwidth Requests 4-72
    U-APSD 4-73
    Traffic Stream Metrics 4-73
  Configuring Voice Parameters 4-74
    Configuring Voice Parameters (GUI) 4-74
    Configuring Voice Parameters (CLI) 4-76
  Configuring Video Parameters 4-77
    Configuring Video Parameters (GUI) 4-78
    Configuring Video Parameters (CLI) 4-79
  Viewing Voice and Video Settings 4-80
    Viewing Voice and Video Settings (GUI) 4-80
    Viewing Voice and Video Settings (CLI) 4-81
  Configuring Media Parameters (GUI) 4-84

Configuring SIP Based CAC 4-85
  Guidelines and Limitations 4-86
  Configuring SIP-Based CAC (CLI) 4-86

Configuring Voice Prioritization Using Preferred Call Numbers 4-86
  Information About Configuring Voice Prioritization Using Preferred Call Numbers 4-86
  Guidelines and Limitations 4-87
  Configuring a Preferred Call Number 4-87
    Configuring a Preferred Call Number (GUI) 4-87
Configuring a Preferred Call Number (CLI) 4-87

Configuring EDCA Parameters 4-88
  Information About EDCA Parameters 4-88
  Configuring EDCA Parameters 4-88
    Configuring EDCA Parameters (GUI) 4-88
    Configuring EDCA Parameters (CLI) 4-90

Configuring the Cisco Discovery Protocol 4-90
  Information About Configuring the Cisco Discovery Protocol 4-91
  Guidelines and Limitations 4-91
  Configuring the Cisco Discovery Protocol 4-93
    Configuring the Cisco Discovery Protocol (GUI) 4-93
    Configuring the Cisco Discovery Protocol (CLI) 4-95
  Viewing Cisco Discovery Protocol Information 4-96
    Viewing Cisco Discovery Protocol Information (GUI) 4-96
    Viewing Cisco Discovery Protocol Information (CLI) 4-98

Configuring Authentication for the Controller and NTP Server 4-99
  Information About Configuring Authentication for the Controller and NTP Server 4-100
  Configuring Authentication for the Controller and NTP Server 4-100
    Configuring the NTP Server for Authentication (GUI) 4-100
    Configuring the NTP Server for Authentication (CLI) 4-100

Configuring RFID Tag Tracking 4-100
  Information About Configuring RFID Tag Tracking 4-101
  Configuring RFID Tag Tracking 4-102
    Configuring RFID Tag Tracking (CLI) 4-102
    Viewing RFID Tag Tracking Information (CLI) 4-103
    Debugging RFID Tag Tracking Issues (CLI) 4-104
    Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues (CLI) 4-105
    Viewing NMSP Settings (CLI) 4-105
    Debugging NMSP Issues 4-108

Configuring and Viewing Location Settings 4-108
  Information About Configuring and Viewing Location Settings 4-109
  Installing the Location Appliance Certificate 4-109
  Synchronizing the Controller and Location Appliance 4-110
  Configuring Location Settings 4-110
    Configuring Location Settings (CLI) 4-110
    Viewing Location Settings (CLI) 4-112

Using the Wireless LAN Controller Network Module 4-114

Resetting the Controller to Default Settings 4-114
  Information About Resetting the Controller to Default Settings 4-115
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Configuring VideoStream</td>
<td>5-1</td>
</tr>
<tr>
<td></td>
<td>Information About VideoStream</td>
<td>5-1</td>
</tr>
<tr>
<td></td>
<td>Guidelines and Limitations</td>
<td>5-1</td>
</tr>
<tr>
<td></td>
<td>Configuring VideoStream</td>
<td>5-2</td>
</tr>
<tr>
<td></td>
<td>Configuring the VideoStream on the Controller (GUI)</td>
<td>5-2</td>
</tr>
<tr>
<td></td>
<td>Configuring the VideoStream on the Controller (CLI)</td>
<td>5-6</td>
</tr>
<tr>
<td></td>
<td>Viewing and Debugging Media Streams</td>
<td>5-7</td>
</tr>
<tr>
<td>6</td>
<td>Configuring Security Solutions</td>
<td>6-1</td>
</tr>
<tr>
<td></td>
<td>Information about Cisco Unified Wireless Network Solution Security</td>
<td>6-2</td>
</tr>
<tr>
<td></td>
<td>Security Overview</td>
<td>6-2</td>
</tr>
<tr>
<td></td>
<td>Layer 1 Solutions</td>
<td>6-2</td>
</tr>
<tr>
<td></td>
<td>Layer 2 Solutions</td>
<td>6-2</td>
</tr>
<tr>
<td></td>
<td>Layer 3 Solutions</td>
<td>6-3</td>
</tr>
<tr>
<td></td>
<td>Integrated Security Solutions</td>
<td>6-3</td>
</tr>
<tr>
<td></td>
<td>Configuring RADIUS</td>
<td>6-3</td>
</tr>
<tr>
<td></td>
<td>Information About RADIUS</td>
<td>6-3</td>
</tr>
<tr>
<td></td>
<td>Guidelines and Limitations</td>
<td>6-4</td>
</tr>
<tr>
<td></td>
<td>RADIUS Server Support</td>
<td>6-4</td>
</tr>
<tr>
<td></td>
<td>Radius ACS Support</td>
<td>6-4</td>
</tr>
<tr>
<td></td>
<td>Primary and Fallback RADIUS Servers</td>
<td>6-4</td>
</tr>
<tr>
<td></td>
<td>Configuring RADIUS on the ACS</td>
<td>6-5</td>
</tr>
<tr>
<td></td>
<td>Configuring RADIUS</td>
<td>6-6</td>
</tr>
<tr>
<td></td>
<td>Configuring RADIUS (GUI)</td>
<td>6-6</td>
</tr>
<tr>
<td></td>
<td>Configuring RADIUS (CLI)</td>
<td>6-10</td>
</tr>
<tr>
<td></td>
<td>RADIUS Authentication Attributes Sent by the Access Point</td>
<td>6-13</td>
</tr>
<tr>
<td></td>
<td>RADIUS Accounting Attributes</td>
<td>6-16</td>
</tr>
<tr>
<td></td>
<td>Configuring TACACS+</td>
<td>6-17</td>
</tr>
<tr>
<td></td>
<td>Information About TACACS+</td>
<td>6-17</td>
</tr>
<tr>
<td></td>
<td>TACACS+ VSA</td>
<td>6-19</td>
</tr>
<tr>
<td></td>
<td>Guidelines and Limitations</td>
<td>6-19</td>
</tr>
<tr>
<td></td>
<td>Configuring TACACS+ on the ACS</td>
<td>6-19</td>
</tr>
<tr>
<td></td>
<td>Configuring TACACS+</td>
<td>6-21</td>
</tr>
<tr>
<td></td>
<td>Configuring TACACS+ (GUI)</td>
<td>6-21</td>
</tr>
<tr>
<td></td>
<td>Configuring TACACS+ (CLI)</td>
<td>6-23</td>
</tr>
</tbody>
</table>
Contents

Viewing the TACACS+ Administration Server Logs 6-24
Prerequisites 6-24
Configuring Maximum Local Database Entries 6-26
Information About Configuring Maximum Local Database Entries 6-26
Configuring Maximum Local Database Entries (GUI) 6-26
Configuring Maximum Local Database Entries (CLI) 6-27
Configuring Local Network Users on the Controller 6-27
Information About Local Network Users on Controller 6-28
Configuring Local Network Users for the Controller 6-28
   Configuring Local Network Users for the Controller (GUI) 6-28
   Configuring Local Network Users for the Controller (CLI) 6-29
Additional References 6-30
Configuring Password Policies 6-30
   Information About Password Policies 6-30
   Configuring Password Policies (GUI) 6-30
   Configuring Password Policies (CLI) 6-31
Configuring LDAP 6-31
   Information About LDAP 6-32
   Configuring LDAP (GUI) 6-32
   Configuring LDAP (CLI) 6-34
Additional References 6-36
Configuring Local EAP 6-36
   Information About Local EAP 6-36
   Guidelines and Limitations 6-38
   Configuring Local EAP (GUI) 6-38
   Configuring Local EAP (CLI) 6-42
Additional References 6-47
Configuring the System for SpectraLink NetLink Telephones 6-47
   Information About SpectraLink NetLink Telephones 6-47
   Configuring SpectraLink NetLink Phones 6-47
      Enabling Long Preambles (GUI) 6-47
      Enabling Long Preambles (CLI) 6-48
      Configuring Enhanced Distributed Channel Access (CLI) 6-49
Configuring RADIUS NAC Support 6-49
   Information About RADIUS NAC Support 6-49
      Device Registration 6-49
      Central Web Authentication 6-50
      Local Web Authentication 6-50
Guidelines and Limitations 6-50
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring RADIUS NAC Support (GUI)</td>
<td>6-51</td>
</tr>
<tr>
<td>Configuring RADIUS NAC Support (CLI)</td>
<td>6-51</td>
</tr>
<tr>
<td>Using Management Over Wireless</td>
<td>6-52</td>
</tr>
<tr>
<td>Information About Management Over Wireless</td>
<td>6-52</td>
</tr>
<tr>
<td>Enabling Management over Wireless (GUI)</td>
<td>6-52</td>
</tr>
<tr>
<td>Enabling Management over Wireless (CLI)</td>
<td>6-52</td>
</tr>
<tr>
<td>Using Dynamic Interfaces for Management</td>
<td>6-53</td>
</tr>
<tr>
<td>Information About Using Dynamic Interfaces for Management</td>
<td>6-53</td>
</tr>
<tr>
<td>Enabling Management using Dynamic Interfaces (CLI)</td>
<td>6-53</td>
</tr>
<tr>
<td>Configuring DHCP Option 82</td>
<td>6-53</td>
</tr>
<tr>
<td>Information About DHCP Option 82</td>
<td>6-53</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>6-54</td>
</tr>
<tr>
<td>Configuring DHCP Option 82 (GUI)</td>
<td>6-54</td>
</tr>
<tr>
<td>Configuring DHCP Option 82 (CLI)</td>
<td>6-55</td>
</tr>
<tr>
<td>Additional References</td>
<td>6-56</td>
</tr>
<tr>
<td>Configuring and Applying Access Control Lists</td>
<td>6-56</td>
</tr>
<tr>
<td>Information About Access Control Lists</td>
<td>6-56</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>6-56</td>
</tr>
<tr>
<td>Configuring and Applying Access Control Lists (GUI)</td>
<td>6-57</td>
</tr>
<tr>
<td>Configuring Access Control Lists</td>
<td>6-57</td>
</tr>
<tr>
<td>Applying an Access Control List to an Interface</td>
<td>6-60</td>
</tr>
<tr>
<td>Applying an Access Control List to the Controller CPU</td>
<td>6-61</td>
</tr>
<tr>
<td>Applying an Access Control List to a WLAN</td>
<td>6-61</td>
</tr>
<tr>
<td>Applying a Preauthentication Access Control List to a WLAN</td>
<td>6-62</td>
</tr>
<tr>
<td>Configuring and Applying Access Control Lists (CLI)</td>
<td>6-63</td>
</tr>
<tr>
<td>Configuring Access Control Lists</td>
<td>6-63</td>
</tr>
<tr>
<td>Applying Access Control Lists</td>
<td>6-65</td>
</tr>
<tr>
<td>Configuring Management Frame Protection</td>
<td>6-66</td>
</tr>
<tr>
<td>Information About Management Frame Protection</td>
<td>6-66</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>6-67</td>
</tr>
<tr>
<td>Configuring Management Frame Protection (GUI)</td>
<td>6-68</td>
</tr>
<tr>
<td>Viewing the Management Frame Protection Settings (GUI)</td>
<td>6-69</td>
</tr>
<tr>
<td>Configuring Management Frame Protection (CLI)</td>
<td>6-70</td>
</tr>
<tr>
<td>Viewing the Management Frame Protection Settings (CLI)</td>
<td>6-70</td>
</tr>
<tr>
<td>Debugging Management Frame Protection Issues (CLI)</td>
<td>6-72</td>
</tr>
<tr>
<td>Configuring Client Exclusion Policies</td>
<td>6-72</td>
</tr>
<tr>
<td>Configuring Client Exclusion Policies (GUI)</td>
<td>6-73</td>
</tr>
<tr>
<td>Configuring Client Exclusion Policies (CLI)</td>
<td>6-73</td>
</tr>
<tr>
<td>Configuring Identity Networking</td>
<td>6-75</td>
</tr>
<tr>
<td>Information About Identity Networking</td>
<td>6-75</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>RADIUS Attributes Used in Identity Networking</td>
<td>6-75</td>
</tr>
<tr>
<td>Configuring AAA Override</td>
<td>6-78</td>
</tr>
<tr>
<td>Information About AAA Override</td>
<td>6-78</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>6-79</td>
</tr>
<tr>
<td>Updating the RADIUS Server Dictionary File for Proper QoS Values</td>
<td>6-79</td>
</tr>
<tr>
<td>Configuring AAA Override (GUI)</td>
<td>6-80</td>
</tr>
<tr>
<td>Configure AAA Override (CLI)</td>
<td>6-81</td>
</tr>
<tr>
<td>Managing Rogue Devices</td>
<td>6-81</td>
</tr>
<tr>
<td>Information About Rogue Devices</td>
<td>6-81</td>
</tr>
<tr>
<td>Detecting Rogue Devices</td>
<td>6-82</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>6-82</td>
</tr>
<tr>
<td>WCS Interaction and Rogue Detection</td>
<td>6-83</td>
</tr>
<tr>
<td>Configuring Rogue Detection (GUI)</td>
<td>6-83</td>
</tr>
<tr>
<td>Configuring Rogue Detection (CLI)</td>
<td>6-85</td>
</tr>
<tr>
<td>Classifying Rogue Access Points</td>
<td>6-88</td>
</tr>
<tr>
<td>Information About Classifying Rogue Access Points</td>
<td>6-88</td>
</tr>
<tr>
<td>Configuring Rogue Classification Rules (GUI)</td>
<td>6-90</td>
</tr>
<tr>
<td>Viewing and Classifying Rogue Devices (GUI)</td>
<td>6-93</td>
</tr>
<tr>
<td>Configuring Rogue Classification Rules (CLI)</td>
<td>6-96</td>
</tr>
<tr>
<td>Viewing and Classify Rogue Devices (CLI)</td>
<td>6-98</td>
</tr>
<tr>
<td>Configuring Cisco TrustSec SXP</td>
<td>6-102</td>
</tr>
<tr>
<td>Information About Cisco TrustSec SXP</td>
<td>6-103</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>6-103</td>
</tr>
<tr>
<td>Configuring Cisco TrustSec SXP (GUI)</td>
<td>6-104</td>
</tr>
<tr>
<td>Creating a New SXP Connection (GUI)</td>
<td>6-105</td>
</tr>
<tr>
<td>Configuring Cisco TrustSec SXP (CLI)</td>
<td>6-105</td>
</tr>
<tr>
<td>Configuring Cisco Intrusion Detection System</td>
<td>6-106</td>
</tr>
<tr>
<td>Information About Cisco Intrusion Detection System</td>
<td>6-106</td>
</tr>
<tr>
<td>Additional Information</td>
<td>6-107</td>
</tr>
<tr>
<td>Configuring IDS Sensors (GUI)</td>
<td>6-107</td>
</tr>
<tr>
<td>Viewing Shunned Clients (GUI)</td>
<td>6-108</td>
</tr>
<tr>
<td>Configuring IDS Sensors (CLI)</td>
<td>6-108</td>
</tr>
<tr>
<td>Viewing Shunned Clients (CLI)</td>
<td>6-110</td>
</tr>
<tr>
<td>Configuring IDS Signatures</td>
<td>6-110</td>
</tr>
<tr>
<td>Information About IDS Signatures</td>
<td>6-111</td>
</tr>
<tr>
<td>Configuring IDS Signatures (GUI)</td>
<td>6-113</td>
</tr>
<tr>
<td>Uploading or Downloading IDS Signatures</td>
<td>6-113</td>
</tr>
<tr>
<td>Enabling or Disabling IDS Signatures</td>
<td>6-115</td>
</tr>
</tbody>
</table>
Contents

Viewing IDS Signature Events (GUI) 6-116
Configure IDS Signatures (CLI) 6-118
Viewing IDS Signature Events (CLI) 6-119

Configuring wIPS 6-121
Information About wIPS 6-121
Guidelines and Limitations 6-124
Additional References 6-124
Configuring wIPS on an Access Point (GUI) 6-124
Configuring wIPS on an Access Point (CLI) 6-124
Viewing wIPS Information (CLI) 6-126

Configuring Wi-Fi Direct Client Policy 6-127
Information About Wi-Fi Direct Client Policy 6-127
Guidelines and Limitations 6-127
Configuring Wi-Fi Direct Client Policy (GUI) 6-127
Configuring Wi-Fi Direct Client Policy (CLI) 6-128
Monitoring and Troubleshooting Wi-Fi Direct Client Policy (CLI) 6-128

Configuring Web Auth Proxy 6-128
Information About Web Auth Proxy 6-128
Configuring Web Auth Proxy (GUI) 6-129
Configuring Web Auth Proxy (CLI) 6-130

Detecting Active Exploits 6-130

CHAPTER 7

Working with WLANs 7-1
Information About WLANs 7-1
Guidelines and Limitations 7-1
Creating WLANs 7-3
Creating and Removing WLANs (GUI) 7-3
Enabling and Disabling WLANs (GUI) 7-6
Creating and Deleting WLANs (CLI) 7-6
Viewing WLANs (CLI) 7-7
Enabling and Disabling WLANs (CLI) 7-7

Searching WLANs 7-8
Searching WLANs (GUI) 7-8
Setting the Client Count per WLAN 7-9
Information About Setting Client Count per WLAN 7-9
Guidelines and Limitations 7-9
Configuring Client Count per WLAN (GUI) 7-9
Configuring Maximum Number of Clients per WLAN (CLI) 7-10
Configuring Maximum Number of Clients per AP Radio Per WLAN (GUI) 7-10
Configuring Maximum Number of Clients per AP Radio Per WLAN (CLI)  7-10

Configuring WLANs  7-10
  Configuring DHCP  7-11
  Internal DHCP Server  7-12
  External DHCP Servers  7-12
  DHCP Assignment  7-13
    Security Considerations  7-13
    Guidelines and Limitations  7-14
  Configuring DHCP  7-14
    Configuring DHCP (GUI)  7-14
    Configuring DHCP (CLI)  7-15
    Debugging DHCP (CLI)  7-15
  Configuring DHCP Scopes  7-16
    Configuring DHCP Scopes (GUI)  7-16
    Configuring DHCP Scopes (CLI)  7-18
  Configuring MAC Filtering for WLANs  7-19
  Configuring Local MAC Filters  7-19
    Information About Local MAC Filters  7-20
    Configuring Local MAC Filters (CLI)  7-20
    Guidelines and Limitations  7-20
    Configuring a Timeout for Disabled Clients  7-20
    Configuring a Timeout for Disabled Clients (CLI)  7-20
  Assigning WLANs to Interfaces  7-21
  Configuring the DTIM Period  7-21
    Information About the DTIM Period  7-21
    Guidelines and Limitations  7-22
    Configuring the DTIM Period  7-22
  Configuring Peer-to-Peer Blocking  7-24
    Information About Peer-to-Peer Blocking  7-24
    Guidelines and Limitations  7-25
    Configuring Peer-to-Peer Blocking  7-26
  Configuring Layer 2 Security  7-27
    Configuring Static WEP Keys (CLI)  7-28
    Configuring Dynamic 802.1X Keys and Authorization (CLI)  7-28
  Configuring a WLAN for Both Static and Dynamic WEP  7-28
    Information About WLAN for Both Static and Dynamic WEP  7-29
    WPA1 and WPA2  7-29
    Guidelines and Limitations  7-30
  Configuring WPA1+WPA2  7-30
    Configuring WPA1+WPA2 (GUI)  7-30
Configuring WPA1+WPA2 (CLI) 7-32
Configuring Sticky PMK ID Caching 7-33
  Information About Sticky PMK ID Caching 7-33
  Guidelines and Limitations 7-33
  Configuring Sticky PMK ID Caching (CLI) 7-33
Configuring CKIP 7-34
  Information About CKIP 7-35
  Configuring CKIP 7-35
Configuring Session Timeouts 7-37
  Configuring a Session Timeout (GUI) 7-37
  Configuring a Session Timeout (CLI) 7-37
Configuring Layer 3 Security Using VPN Passthrough 7-38
  Information About VPN Passthrough 7-38
  Guidelines and Limitations 7-38
  Configuring VPN Passthrough 7-38
Configuring Layer 3 Security Using Web Authentication 7-39
  Information About Web Authentication 7-39
  Guidelines and Limitations 7-39
  Configuring Web Authentication 7-40
Configuring WISPr Bypassing 7-41
  Information about WISPr 7-41
  Configuring WISPr Bypassing 7-42
  Configuring WISPr Bypassing (CLI) 7-42
Configuring a Fallback Policy with MAC Filtering and Web Authentication 7-42
  Information About Fallback Policy with MAC Filtering and Web Authentication 7-42
  Configuring a Fallback Policy with MAC Filtering and Web Authentication 7-42
Assigning a QoS Profile to a WLAN 7-44
  Information About QoS Profiles 7-44
  Assigning QoS Profiles 7-45
Configuring QoS Enhanced BSS 7-46
  Information About QoS Enhanced BSS 7-46
  Guidelines and Limitations 7-47
  Configuring QBSS 7-48
Configuring Media Session Snooping and Reporting 7-49
  Information About Media Session Snooping and Reporting 7-50
  Guidelines and Limitations 7-50
  Configuring Media Session Snooping 7-50
Configuring Key Telephone System-Based CAC 7-55
  Information About Key Telephone System-Based CAC 7-56
  Guidelines and Limitations 7-56
Configuring KTS-based CAC 7-56
Configuring Reanchoring of Roaming Voice Clients 7-58
    Information About Reanchoring of Roaming Voice Clients 7-58
    Guidelines and Limitations 7-58
    Configuring Reanchoring of Roaming Voice Clients 7-58
Configuring Seamless IPv6 Mobility 7-60
    Information About Seamless IPv6 Mobility 7-60
    Guidelines and Limitations 7-60
Configuring RA Guard for IPv6 Clients 7-61
    Information About RA Guard 7-61
    Configuring RA Guard (GUI) 7-61
    Configuring RA Guard (CLI) 7-62
Configuring RA Throttling for IPv6 Clients 7-62
    Information About RA Throttling 7-62
    Configuring RA Throttling (GUI) 7-63
    Configuring RA Throttle Policy (CLI) 7-64
Configuring IPv6 Neighbor Discovery Caching 7-64
    Information About IPv6 Neighbor Discovery 7-64
    Configuring Neighbor Binding Timers (GUI) 7-65
    Configure Neighbor Binding Timers (CLI) 7-66
Configuring Unknown Address NS Multicast Forwarding 7-66
    Configuring NS Multicast Forwarding (CLI) 7-66
Configuring Cisco Client Extensions 7-67
    Information About Cisco Client Extensions 7-67
    Guidelines and Limitations 7-67
    Configuring CCX Aironet IEs 7-67
Configuring AP Groups 7-70
    Information About Access Point Groups 7-70
    Guidelines and Limitations 7-72
    Configuring Access Point Groups 7-72
Configuring RF Profiles 7-76
    Information About RF Profiles 7-77
    Guidelines and Limitations 7-77
    Configuring RF Profiles 7-77
Configuring Web Redirect with 802.1X Authentication 7-81
    Information About Web Redirect with 802.1X Authentication 7-81
    Configuring Web Redirect 7-83
Configuring NAC Out-of-Band Integration 7-87
    Information About NAC Out-of-Band Integration 7-87
    Guidelines and Limitations 7-88
## Chapter 8: Controlling Lightweight Access Points

### Configuring Per-WLAN RADIUS Source Support
- Information About Per-WLAN RADIUS Source Support
- Guidelines and Limitations
- Configuring Per-WLAN RADIUS Source Support

### Configuring Remote LANs
- Guidelines and Limitations
- Configuring Remote LANs

### Configuring Data Encryption
- Information About Data Encryption
- Guidelines and Limitations

### Upgrading or Downgrading DTLS Images for Cisco 5500 Series Controllers

### Viewing CAPWAP Maximum Transmission Unit Information

### Debugging CAPWAP

### Controller Discovery Process
- Guidelines and Limitations

### Verifying that Access Points Join the Controller
- Guidelines and Limitations

### Searching for Access Points
- Information About Searching for Access Points
- Filtering the AP Search (GUI)

### Monitoring the Interface Details (GUI)

### Searching for Access Point Radios
- Information About Searching for Access Point Radios
- Searching for Access Point Radios (GUI)

### Configuring Global Credentials for Access Points
- Information About Configuring Global Credentials for Access Points

### Guidelines and Limitations
Viewing the AP Crash Log Information 8-47
  Viewing the AP Crash Log information (GUI) 8-47
  Viewing the AP Crash Log information (CLI) 8-48
Displaying MAC Addresses for Converted Access Points 8-48
Disabling the Reset Button on Access Points Converted to Lightweight Mode 8-48
Configuring a Static IP Address on a Lightweight Access Point 8-48
  Configuring a Static IP Address (GUI) 8-49
  Configuring a Static IP Address (CLI) 8-50
Supporting Oversized Access Point Images 8-51
  Recovering the Access Point (Using the TFTP Recovery Procedure) 8-51
Configuring OfficeExtend Access Points 8-51
  Information About OfficeExtend Access Points 8-52
OEAP 600 Series Access Points 8-52
  Supported Controller Platforms 8-53
OEAP in Local Mode 8-53
Supported WLAN Settings for 600 Series OfficeExtend Access Point 8-54
  WLAN Security Settings for the 600 Series OfficeExtend Access Point 8-55
  Authentication Settings 8-58
  Supported User Count on 600 Series OfficeExtend Access Point 8-58
Remote LAN Settings 8-59
  Channel Management and Settings 8-60
  Additional Caveats 8-61
Implementing Security 8-61
Licensing for an OfficeExtend Access Point 8-62
Configuring OfficeExtend Access Points 8-62
  Configuring OfficeExtend Access Points (GUI) 8-62
  Configuring OfficeExtend Access Points (CLI) 8-65
Configuring a Personal SSID on an OfficeExtend Access Point 8-67
Viewing OfficeExtend Access Point Statistics 8-69
  Additional References 8-70
Using Cisco Workgroup Bridges 8-70
  Information About Cisco Workgroup Bridges 8-70
Guidelines and Limitations 8-71
WGB Configuration Example 8-73
Viewing the Status of Workgroup Bridges 8-73
  Viewing the Status of Workgroup Bridges (GUI) 8-73
  Viewing the Status of Workgroup Bridges (CLI) 8-74
Debugging WGB Issues (CLI) 8-75
Configuring Non-Cisco Workgroup Bridges 8-75
Contents

Configuring Probe Request Forwarding (CLI) 8-100

Retrieving the Unique Device Identifier on Controllers and Access Points 8-101

Information About Retrieving the Unique Device Identifier on Controllers and Access Points 8-101

Retrieving the Unique Device Identifier on Controllers and Access Points 8-101

Retrieving the Unique Device Identifier on Controllers and Access Points (GUI) 8-101

Retrieving the Unique Device Identifier on Controllers and Access Points (CLI) 8-102

Performing a Link Test 8-102

Information About Performing a Link Test 8-103

Performing a Link Test 8-103

Performing a Link Test (GUI) 8-104

Performing a Link Test (CLI) 8-105

Configuring Link Latency 8-105

Information About Configuring Link Latency 8-106

Guidelines and Limitations 8-106

Configuring Link Latency 8-106

Configuring Link Latency (GUI) 8-106

Configuring Link Latency (CLI) 8-107

Configuring the TCP MSS 8-108

Information About Configuring the TCP MSS 8-109

Configuring TCP MSS 8-109

Configuring TCP MSS (GUI) 8-109

Configuring TCP MSS (CLI) 8-109

Configuring Power over Ethernet 8-110

Information About Configuring Power over Ethernet 8-110

Guidelines and Limitations 8-110

Configuring Power over Ethernet 8-111

Configuring Power over Ethernet (GUI) 8-111

Configuring Power over Ethernet (CLI) 8-113

Configuring Flashing LEDs 8-114

Information About Configuring Flashing LEDs 8-114

Configuring Flashing LEDs (CLI) 8-114

Viewing Clients 8-115

Viewing Clients (GUI) 8-115

Viewing Clients (CLI) 8-119

Configuring LED States for Access Points 8-120

Guidelines and Limitations 8-120

Configuring LED State of Access Point in a Network Globally (GUI) 8-120

Configuring LED State of Access Point in a Network Globally (CLI) 8-120

Configuring LED State on an Access Point (GUI) 8-120
| Contents |
|-----------------|------|
| Configuring Backup Controllers (CLI)  | 9-26 |
| Configuring External Authentication and Authorization Using a RADIUS Server | 9-28 |
| Configuring RADIUS Servers | 9-29 |
| Adding a Username to a RADIUS Server | 9-29 |
| Enabling External Authentication of Mesh Access Points | 9-30 |
| Viewing Security Statistics | 9-31 |
| Configuring Global Mesh Parameters | 9-31 |
| Information About Configuring Global Mesh Parameters | 9-31 |
| Configuring Global Mesh Parameters (GUI) | 9-32 |
| Configuring Global Mesh Parameters (CLI) | 9-36 |
| Viewing Global Mesh Parameter Settings (CLI) | 9-37 |
| Configuring Local Mesh Parameters | 9-38 |
| Configuring Wireless Backhaul Data Rate | 9-38 |
| Configuring Ethernet Bridging | 9-43 |
| Configuring Bridge Group Names | 9-45 |
| Configuring Public Safety Band Settings | 9-46 |
| Configuring Interoperability with Cisco 3200 | 9-48 |
| Configuring Power and Channel Settings | 9-51 |
| Configuring Antenna Gain | 9-54 |
| Backhaul Channel Deselection on Serial Backhaul Access Point | 9-55 |
| Configuring Dynamic Channel Assignment (GUI) | 9-60 |
| Configuring Advanced Features | 9-63 |
| Using the 2.4-GHz Radio for Backhaul | 9-64 |
| Changing the Backhaul from 5 GHz to 2.4 GHz | 9-64 |
| Changing the Backhaul from 2.4 GHz to 5 GHz | 9-65 |
| Verifying the Current Backhaul in Use | 9-65 |
| Universal Client Access | 9-66 |
| Configuring Universal Client Access (GUI) | 9-66 |
| Configuring Universal Client Access (CLI) | 9-66 |
| Universal Client Access on Serial Backhaul Access Points | 9-67 |
| Configuring Extended Universal Access (GUI) | 9-67 |
| Configuring Extended Universal Access (CLI) | 9-70 |
| Configuring Extended Universal Access from the Wireless Control System (WCS) | 9-71 |
| Configuring Ethernet VLAN Tagging | 9-71 |
| Ethernet Port Notes | 9-72 |
| Ethernet VLAN Tagging Guidelines | 9-73 |
| VLAN Registration | 9-75 |
| Enabling Ethernet VLAN Tagging (GUI) | 9-75 |
| Configuring Ethernet VLAN Tagging (CLI) | 9-77 |
| Viewing Ethernet VLAN Tagging Configuration Details (CLI) | 9-78 |
Contents

Chapter 9
Guidelines and Limitations 9-111
Configuring a Preferred Parent 9-111
Co-Channel Interference 9-113
Viewing Mesh Statistics for a Mesh Access Point 9-113
Viewing Mesh Statistics for a Mesh Access Point (GUI) 9-113
Viewing Mesh Statistics for an Mesh Access Point (CLI) 9-117
Viewing Neighbor Statistics for a Mesh Access Point 9-118
Viewing Neighbor Statistics for a Mesh Access Point (GUI) 9-118
Viewing the Neighbor Statistics for a Mesh Access Point (CLI) 9-121
Converting Indoor Access Points to Mesh Access Points 9-122
Changing MAP and RAP Roles for Indoor Mesh Access Points 9-122
Changing MAP and RAP Roles for Indoor Mesh Access Points (GUI) 9-123
Changing MAP and RAP Roles for Indoor Mesh Access Points (CLI) 9-123
Converting Indoor Mesh Access Points to Nonmesh Lightweight Access Points (1130AG, 1240AG) 9-123
Configuring Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers 9-124
Guidelines and Limitations 9-125
Enabling Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers (GUI) 9-125
Enabling Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers (CLI) 9-126

Chapter 10
Managing Controller Software and Configurations 10-1
Upgrading the Controller Software 10-1
Information About Upgrading the Controller Software 10-1
Guidelines and Limitations 10-2
Upgrading Controller Software 10-5
Upgrading Controller Software (GUI) 10-5
Upgrading Controller Software (CLI) 10-7
Predownloading an Image to an Access Point 10-10
Information About Predownloading an Image to an Access Point 10-10
Access Point Predownload Process 10-11
Guidelines and Limitations 10-12
Predownloading an Image to an Access Point 10-12
Configuring Predownload Image to Access Points- Global Configuration (GUI) 10-12
Configuring Predownload Image to an Access Point (GUI) 10-13
Predownloading an Image to Access Points (CLI) 10-13
Transferring Files to and from a Controller 10-15
Downloading a Login Banner File 10-15
Information About Downloading a Login Banner File 10-16
Downloading a Login Banner File 10-16
Clearing the Login Banner (GUI) 10-18
CHAPTER 10

Managing User Accounts 11-1

Creating Guest User Accounts 11-1
  Information About Creating Guest Accounts 11-1
  Guidelines and Limitations 11-2
  Creating a Lobby Ambassador Account 11-2
    Creating a Lobby Ambassador Account (GUI) 11-2
    Creating a Lobby Ambassador Account (CLI) 11-3
    Creating Guest User Accounts as a Lobby Ambassador (GUI) 11-3
  Viewing Guest User Accounts 11-5
    Viewing the Guest Accounts (GUI) 11-5
    Viewing the Guest Accounts (CLI) 11-6
  Additional References 11-6

Obtaining a Web Authentication Certificate 11-6
  Information About Web Authentication Certificate 11-6
  Support for Chained Certificate 11-6
  Obtaining Web Authentication Certificates 11-6
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtaining a Web Authentication Certificate (GUI)</td>
<td>11-7</td>
</tr>
<tr>
<td>Obtaining a Web Authentication Certificate (CLI)</td>
<td>11-8</td>
</tr>
<tr>
<td>Web Authentication Process</td>
<td>11-9</td>
</tr>
<tr>
<td>Information About Web Authentication Process</td>
<td>11-9</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>11-9</td>
</tr>
<tr>
<td>Choosing the Default Web Authentication Login Page</td>
<td>11-12</td>
</tr>
<tr>
<td>Information About Default Web Authentication Login Page</td>
<td>11-12</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>11-13</td>
</tr>
<tr>
<td>Choosing the Default Web Authentication Login Page (GUI)</td>
<td>11-13</td>
</tr>
<tr>
<td>Choosing the Default Web Authentication Login Page (CLI)</td>
<td>11-14</td>
</tr>
<tr>
<td>Example: Modified Default Web Authentication Login Page Example</td>
<td>11-16</td>
</tr>
<tr>
<td>Example: Creating a Customized Web Authentication Login Page</td>
<td>11-17</td>
</tr>
<tr>
<td>Choosing a Customized Web Authentication Login Page from an External Web Server</td>
<td>11-19</td>
</tr>
<tr>
<td>Information About Customized Web Authentication Login Page</td>
<td>11-20</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>11-20</td>
</tr>
<tr>
<td>Choosing a Customized Web Authentication Login Page from An External Web Server</td>
<td>11-20</td>
</tr>
<tr>
<td>Choosing a Customized Web Authentication Login Page from an External Web Server (GUI)</td>
<td>11-20</td>
</tr>
<tr>
<td>Choosing a Customized Web Authentication Login Page from an External Web Server (CLI)</td>
<td>11-21</td>
</tr>
<tr>
<td>Additional References</td>
<td>11-21</td>
</tr>
<tr>
<td>Downloading a Customized Web Authentication Login Page</td>
<td>11-21</td>
</tr>
<tr>
<td>Information About Downloading Customized Web Authentication Login Page</td>
<td>11-22</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>11-22</td>
</tr>
<tr>
<td>Additional References</td>
<td>11-22</td>
</tr>
<tr>
<td>Downloading a Customized Web Authentication Login Page (GUI)</td>
<td>11-23</td>
</tr>
<tr>
<td>Downloading a Customized Web Authentication Login Page (CLI)</td>
<td>11-24</td>
</tr>
<tr>
<td>Additional References</td>
<td>11-24</td>
</tr>
<tr>
<td>Example: Customized Web Authentication Login Page</td>
<td>11-25</td>
</tr>
<tr>
<td>Verifying the Web Authentication Login Page Settings (CLI)</td>
<td>11-25</td>
</tr>
<tr>
<td>Assigning Login, Login Failure, and Logout Pages per WLAN</td>
<td>11-25</td>
</tr>
<tr>
<td>Information About Assigning Login, Login Failure, and Logout Pages per WLAN</td>
<td>11-26</td>
</tr>
<tr>
<td>Assigning Login, Login Failure, and Logout Pages per WLAN (GUI)</td>
<td>11-26</td>
</tr>
<tr>
<td>Assigning Login, Login Failure, and Logout Pages per WLAN (CLI)</td>
<td>11-27</td>
</tr>
<tr>
<td>Configuring Wired Guest Access</td>
<td>11-28</td>
</tr>
<tr>
<td>Information About Wired Guest Access</td>
<td>11-28</td>
</tr>
<tr>
<td>Prerequisites for Configuring Wired Guest Access</td>
<td>11-30</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>11-30</td>
</tr>
<tr>
<td>Configuring Wired Guest Access</td>
<td>11-31</td>
</tr>
</tbody>
</table>
### Configuring Radio Resource Management

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring RRM</td>
<td>12-1</td>
</tr>
<tr>
<td>Configuring the RF Group Mode (GUI)</td>
<td>12-6</td>
</tr>
<tr>
<td>Configuring the RF Group Mode (CLI)</td>
<td>12-7</td>
</tr>
<tr>
<td>Configuring Transmit Power Control (GUI)</td>
<td>12-7</td>
</tr>
<tr>
<td>Configuring Off-Channel Scanning Defer</td>
<td>12-9</td>
</tr>
<tr>
<td>Information About Off-Channel Scanning Defer</td>
<td>12-9</td>
</tr>
<tr>
<td>Configuring Off-Channel Scanning Defer for WLANs</td>
<td>12-9</td>
</tr>
<tr>
<td>Configuring RRM Neighbor Discovery Packets</td>
<td>12-25</td>
</tr>
<tr>
<td>Important About RRM NDP and RF Grouping</td>
<td>12-25</td>
</tr>
<tr>
<td>Configuring RRM NDP (CLI)</td>
<td>12-26</td>
</tr>
<tr>
<td>Configuring RF Groups</td>
<td>12-26</td>
</tr>
<tr>
<td>Information About RF Groups</td>
<td>12-26</td>
</tr>
<tr>
<td>RF Group Leader</td>
<td>12-27</td>
</tr>
<tr>
<td>RF Group Name</td>
<td>12-28</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>12-28</td>
</tr>
<tr>
<td>Configuring RF Groups</td>
<td>12-29</td>
</tr>
<tr>
<td>Configuring an RF Group Name (GUI)</td>
<td>12-29</td>
</tr>
<tr>
<td>Configuring an RF Group Name (CLI)</td>
<td>12-30</td>
</tr>
<tr>
<td>Viewing the RF Group Status</td>
<td>12-30</td>
</tr>
<tr>
<td>Viewing RF Group Status (GUI)</td>
<td>12-30</td>
</tr>
<tr>
<td>Viewing RF Group Status (CLI)</td>
<td>12-31</td>
</tr>
<tr>
<td>Overriding RRM</td>
<td>12-32</td>
</tr>
<tr>
<td>Information About Overriding RRM</td>
<td>12-32</td>
</tr>
<tr>
<td>Guidelines and Limitations</td>
<td>12-33</td>
</tr>
<tr>
<td>Statically Assigning Channel and Transmit Power Settings to Access Point Radios</td>
<td>12-33</td>
</tr>
<tr>
<td>Statically Assigning Channel and Transmit Power Settings (GUI)</td>
<td>12-33</td>
</tr>
<tr>
<td>Statically Assigning Channel and Transmit Power Settings (CLI)</td>
<td>12-37</td>
</tr>
</tbody>
</table>
Cisco Wireless LAN Controller Configuration Guide

CHAPTER 13 Configuring Cisco CleanAir

Information About CleanAir
Role of the Controller in a Cisco CleanAir System
Interference Types that Cisco CleanAir can Detect
Persistent Devices
Persistent Devices Detection
Persistent Devices Propagation
Guidelines and Limitations
Configuring Cisco CleanAir
Configuring Cisco CleanAir on the Controller
Configuring Cisco CleanAir on the Controller (GUI)
Configuring Cisco CleanAir on the Controller (CLI)
Configuring Cisco CleanAir on an Access Point
Configuring Cisco CleanAir on an Access Point (GUI)
Configuring Cisco CleanAir on an Access Point (CLI)
Monitoring the Interference Devices
Prerequisites for Monitoring the Interference Devices
Monitoring the Interference Device (GUI)
Monitoring the Interference Device (CLI)
Detecting Interferers by an Access Point
Detecting Interferers by Device Type  13-17
Detecting Persistent Sources of Interference  13-17
Monitoring Persistent Devices (GUI)  13-18
Monitoring Persistent Devices (CLI)  13-18
Monitoring the Air Quality of Radio Bands  13-19
Monitoring the Air Quality of Radio Bands (GUI)  13-19
Monitoring the Air Quality of Radio Bands (CLI)  13-20
Viewing a Summary of the Air Quality  13-20
Viewing Air Quality for all Access Points on a Radio Band  13-20
Viewing Air Quality for an Access Point on a Radio Band  13-21
Monitoring the Worst Air Quality of Radio Bands (GUI)  13-21
Monitoring the Worst Air Quality of Radio Bands (CLI)  13-22
Viewing a Summary of the Air Quality (CLI)  13-22
Viewing Worst Air Quality Information for all Access Points on a Radio Band (CLI)  13-22
Viewing Air Quality for an Access Point on a Radio Band (CLI)  13-23
Viewing Air Quality for an Access Point by Device Type (CLI)  13-23
Detecting Persistent Sources of Interference (CLI)  13-24
Configuring a Spectrum Expert Connection  13-24
Additional References  13-26
Related Documents  13-27
Feature History for Configuring CleanAir  13-27

CHAPTER 14
Configuring Mobility Groups  14-1
Information About Mobility  14-1
Information About Mobility Groups  14-4
   Determining When to Include Controllers in a Mobility Group  14-7
   Messaging Among Mobility Groups  14-7
   Using Mobility Groups with NAT Devices  14-7
Configuring Mobility Groups  14-9
   Prerequisites for Configuring Mobility Groups  14-9
   Configuring Mobility Groups (GUI)  14-11
   Configuring Mobility Groups (CLI)  14-15
Viewing Mobility Group Statistics  14-16
   Viewing Mobility Group Statistics (GUI)  14-16
   Viewing Mobility Group Statistics (CLI)  14-19
Configuring Auto-Anchor Mobility  14-19
   Information About Auto-Anchor Mobility  14-19
   Guidelines and Limitations  14-20
   Configuring Auto-Anchor Mobility (GUI)  14-20
Configuring Auto-Anchor Mobility (CLI) 14-21
Validating WLAN Mobility Security Values 14-23
   Information About WLAN Mobility Security Values 14-23
Using Symmetric Mobility Tunneling 14-24
   Information About Symmetric Mobility Tunneling 14-24
   Guidelines and Limitations 14-26
Verifying Symmetric Mobility Tunneling 14-26
   Verifying Symmetric Mobility Tunneling (GUI) 14-26
   Verifying if Symmetric Mobility Tunneling is Enabled (CLI) 14-26
Running Mobility Ping Tests 14-27
   Information About Mobility Ping Tests 14-27
   Guidelines and Limitations 14-27
   Running Mobility Ping Tests (CLI) 14-28
Configuring Dynamic Anchoring for Clients with Static IP Addresses 14-28
   Information About Dynamic Anchoring for Clients with Static IP 14-28
      How Dynamic Anchoring of Static IP Clients Works 14-29
      Guidelines and Limitations 14-29
   Configuring Dynamic Anchoring of Static IP Clients (GUI) 14-30
   Configuring Dynamic Anchoring of Static IP Clients (CLI) 14-30
Configuring Foreign Mappings 14-30
   Information About Foreign Mappings 14-30
   Configuring Foreign Controller MAC Mapping (GUI) 14-30
   Configuring Foreign Controller MAC Mapping (CLI) 14-31

CHAPTER 15
Configuring FlexConnect 15-1
   Information About FlexConnect 15-1
      FlexConnect Authentication Process 15-2
      Guidelines and Limitations 15-5
   Configuring FlexConnect 15-7
      Configuring the Switch at the Remote Site 15-7
      Configuring the Controller for FlexConnect 15-8
         Configuring the Controller for FlexConnect (GUI) 15-8
         Configuring the Controller for FlexConnect (CLI) 15-11
      Configuring an Access Point for FlexConnect 15-12
         Configuring an Access Point for FlexConnect (GUI) 15-12
         Configuring an Access Point for FlexConnect (CLI) 15-13
      Configuring an Access Point for Local Authentication on a WLAN (GUI) 15-14
      Configuring an Access Point for Local Authentication on a WLAN (CLI) 15-15
   Connecting Client Devices to WLANs 15-15
Contents

Configuring FlexConnect ACLs 15-16
  Information About Access Control Lists 15-16
  Guidelines and Limitations 15-16
Configuring FlexConnect ACLs 15-17
  Configuring FlexConnect ACLs (GUI) 15-17
  Configuring FlexConnect ACLs (CLI) 15-19
  Viewing and Debugging FlexConnect ACLs (CLI) 15-19

Configuring FlexConnect Groups 15-20
  Information About FlexConnect Groups 15-20
  FlexConnect Groups and Backup RADIUS Servers 15-21
  FlexConnect Groups and CCKM 15-21
  FlexConnect Groups and Opportunistic Key Caching 15-21
  FlexConnect Groups and Local Authentication 15-22
Configuring FlexConnect Groups 15-22
  Configuring FlexConnect Groups (GUI) 15-22
  Configuring FlexConnect Groups (CLI) 15-25
  Configuring VLAN-ACL Mapping on FlexConnect Groups (GUI) 15-27
  Configuring VLAN-ACL Mapping on FlexConnect Groups (CLI) 15-27
  Viewing VLAN-ACL Mappings (CLI) 15-27

Configuring AAA Overrides for FlexConnect 15-28
  Information About AAA Overrides 15-28
  Guidelines and Limitations 15-29
  Configuring AAA Override for FlexConnect on an Access Point (GUI) 15-29
  Configuring VLAN Overrides for FlexConnect on an Access Point (CLI) 15-30

Configuring Efficient AP Image Upgrades for FlexConnect Access Points 15-30
  Information About Efficient AP Image Upgrades 15-31
  Guidelines and Limitations 15-31
  Configuring Efficient AP Image Upgrades on FlexConnect APs (GUI) 15-31
  Configuring Efficient AP Image Upgrades (CLI) 15-32

CHAPTER 16
Configuring Mobile Concierge 16-1
  Information About 802.11u 16-1
  Guidelines and Limitations 16-1
Configuring 802.11u 16-1
  Configuring 802.11u (GUI) 16-2
  Configuring 802.11u (CLI) 16-3
  Configuring Venue Details on Access Points (GUI) 16-6
  Configuring Venue Details on Access Points (CLI) 16-7
  Information About 802.11u M SAP 16-10
Configuring 802.11u MSAP  16-10
   Configuring 802.11u MSAP(GUI)  16-11
   Configuring 802.11u MSAP(CLI)  16-11
Information About Hotspot 2.0  16-11
Configuring Hotspot 2.0  16-11
   Configuring Hotspot 2.0 (GUI)  16-12
   Configuring Hotspot 2.0 (CLI)  16-13

**APPENDIX A**

Troubleshooting  A-1
   Information About Troubleshooting  A-1
   Interpreting LEDs  A-2
      Information About Interpreting LEDs  A-2
      Interpreting Controller LEDs  A-2
      Interpreting Lightweight Access Point LEDs  A-2
   System Messages  A-3
      Information About System Messages  A-3
   Viewing System Resources  A-6
      Information About Viewing System Resources  A-6
      Guidelines and Limitations  A-6
      Viewing System Resources (GUI)  A-6
      Viewing System Resources (CLI)  A-7
   Using the CLI to Troubleshoot Problems  A-8
   Configuring System and Message Logging  A-9
      Information About System and Message Logging  A-9
      Configuring System and Message Logging (GUI)  A-10
      Viewing Message Logs (GUI)  A-12
      Configuring System and Message Logging (CLI)  A-12
      Viewing System and Message Logs (CLI)  A-15
   Viewing Access Point Event Logs  A-16
      Information About Access Point Event Logs  A-17
      Viewing Access Point Event Logs (CLI)  A-17
   Uploading Logs and Crash Files  A-17
      Prerequisites to Upload Logs and Crash Files  A-18
      Uploading Logs and Crash Files (GUI)  A-18
      Uploading Logs and Crash Files (CLI)  A-19
   Uploading Core Dumps from the Controller  A-20
      Information About Uploading Core Dumps from the Controller  A-20
      Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (GUI)  A-20
Interpreting OfficeExtend LEDs A-53
Positioning OfficeExtend Access Points for Optimal RF Coverage A-53
Troubleshooting Common Problems A-53
Troubleshooting Mesh Access Points A-55
Mesh MAP Backhaul Deselection on Ethernet Backhaul at Runtime A-55
Preface

This preface describes the audience, organization, and conventions of the Cisco Wireless LAN Controller Configuration Guide, Release 7.2. It also provides information on how to obtain other documentation. This chapter includes the following sections:

- Audience, page 2
- Purpose, page 2
- Organization, page 2
- Conventions, page 3
- Related Documentation, page 5
- Obtaining Documentation and Submitting a Service Request, page 6
Audience

This publication is for experienced network administrators or management users who configure and maintain Cisco wireless LAN controllers and Cisco lightweight access points.

Purpose

This guide provides the information you need to set up and configure wireless LAN controllers.

Note

This version of the *Cisco Wireless LAN Controller Configuration Guide* pertains specifically to controller software release 7.2. If you are using an earlier version of software, you will notice differences in features, functionality, and GUI pages.

Organization

This guide is organized into these chapters:

<table>
<thead>
<tr>
<th>Chapter Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 2, “Overview”</td>
<td>Provides an overview of the network roles and features of wireless LAN controllers.</td>
</tr>
<tr>
<td>Chapter 3, “Using the Web-Browser and CLI Interfaces”</td>
<td>Describes how to initially configure and log into the controller.</td>
</tr>
<tr>
<td>Chapter 4, “Configuring Ports and Interfaces”</td>
<td>Describes the controller’s physical ports and interfaces and provides instructions for configuring them.</td>
</tr>
<tr>
<td>Chapter 4, “Configuring Controller Settings”</td>
<td>Describes how to configure settings on the controllers.</td>
</tr>
<tr>
<td>Chapter 6, “Configuring VideoStream”</td>
<td>Describes how to configure VideoStream settings on the controller.</td>
</tr>
<tr>
<td>Chapter 7, “Configuring Security Solutions”</td>
<td>Describes application-specific solutions for wireless LANs.</td>
</tr>
<tr>
<td>Chapter 8, “Working with WLANs”</td>
<td>Describes how to configure wireless LANs and SSIDs on your system.</td>
</tr>
<tr>
<td>Chapter 9, “Controlling Lightweight Access Points”</td>
<td>Explains how to connect lightweight access points to the controller and manage access point settings.</td>
</tr>
<tr>
<td>Chapter 10, “Controlling Mesh Access Points”</td>
<td>Explains how to connect mesh access points to the controller and manage access point settings.</td>
</tr>
<tr>
<td>Chapter 11, “Managing Controller Software and Configurations”</td>
<td>Describes how to upgrade and manage controller software and configurations.</td>
</tr>
</tbody>
</table>
### Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>Courier font</strong></td>
<td>Terminal sessions and information the system displays appear in <strong>courier font</strong>.</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>&lt; &gt;</code></td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td><code>[ ]</code></td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td><code>!</code>, <code>#</code></td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Note**  
Means reader take note.

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

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

**Timesaver**  
Means the described action saves time. You can save time by performing the action described in the paragraph.

**Warning**  
This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix “Translated Safety Warnings.”)

**Waarschuwing**  
Dit waarschuwingsymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel “Translated Safety Warnings” (Vertalingen van veiligheidsvoorschriften) raadplegen.)

**Varoitus**  
Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä varoista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännöksiä löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)

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

- Cisco 5500 Series Wireless Controller Installation Guide
- Cisco Wireless LAN Controller Command Reference
- Cisco Wireless Control System Configuration Guide
- Release Noted for Cisco Wireless LAN Controllers and Lightweight Access Points, Release 7.2.100.0
- Quick Start Guide: Cisco Wireless Control System

Click this link to browse to user documentation for the Cisco Unified Wireless Network solution:

Obtaining Documentation and Submitting a Service Request

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


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

This chapter describes the controller components and features. It contains these sections:

- Cisco Unified Wireless Network Solution Overview, page 2-1
- Operating System Software, page 2-4
- Operating System Security, page 2-4
- Layer 2 and Layer 3 Operation, page 2-5
- Cisco Wireless LAN Controllers, page 2-6
- Controller Platforms, page 2-7
- Cisco UWN Solution Wired Connections, page 2-11
- Cisco UWN Solution WLANs, page 2-11
- File Transfers, page 2-12
- Power Over Ethernet, page 2-12
- Cisco Wireless LAN Controller Memory, page 2-12
- Cisco Wireless LAN Controller Failover Protection, page 2-13

Cisco Unified Wireless Network Solution Overview

The Cisco Unified Wireless Network (Cisco UWN) solution is designed to provide 802.11 wireless networking solutions for enterprises and service providers. The Cisco UWN solution simplifies deploying and managing large-scale wireless LANs and enables a unique best-in-class security infrastructure. The operating system manages all data client, communications, and system administration functions, performs radio resource management (RRM) functions, manages system-wide mobility policies using the operating system security solution, and coordinates all security functions using the operating system security framework.

The Cisco UWN solution consists of Cisco wireless LAN controllers and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the operating system user interfaces:

- An HTTP and/or HTTPS full-featured Web User Interface hosted by Cisco wireless LAN controllers can be used to configure and monitor individual controllers. See Chapter 3, “Using the Web-Browser and CLI Interfaces.”
- A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco wireless LAN controllers. See Chapter 3, “Using the Web-Browser and CLI Interfaces.”
• The Network Control System (NCS), which you use to configure and monitor one or more Cisco wireless LAN controllers and associated access points. NCS has tools to facilitate large-system monitoring and control. WCS runs on Windows 2000, Windows 2003, and Red Hat Enterprise Linux ES servers.

**Note**
NCS software release 1.1, must be used with controllers that run controller software release 7.2.

• An industry-standard SNMP V1, V2c, and V3 interface can be used with any SNMP-compliant third-party network management system.

The Cisco UWN solution supports client data services, client monitoring and control, and all rogue access point detection, monitoring, and containment functions. It uses lightweight access points, Cisco wireless LAN controllers, and the optional Cisco WCS to provide wireless services to enterprises and service providers.

**Note**
Unless otherwise noted in this publication, all of the Cisco wireless LAN controllers are referred to as controllers, and all of the Cisco lightweight access points are referred to as access points.

Figure 2-1 shows the Cisco wireless LAN controller components, which can be simultaneously deployed across multiple floors and buildings.
**Single-Controller Deployments**

A standalone controller can support lightweight access points across multiple floors and buildings simultaneously and support the following features:

- Autodetecting and autoconfiguring lightweight access points as they are added to the network.
- Full control of lightweight access points.
- Lightweight access points connect to controllers through the network. The network equipment may or may not provide Power over Ethernet (PoE) to the access points.

Some controllers use redundant Gigabit Ethernet connections to bypass single network failures.

---

**Note**

Some controllers can connect through multiple physical ports to multiple subnets in the network. This feature can be helpful when you want to confine multiple VLANs to separate subnets.

Figure 2-2 shows a typical single-controller deployment.

![Figure 2-2 Single-Controller Deployment](image)

**Multiple-Controller Deployments**

Each controller can support lightweight access points across multiple floors and buildings simultaneously. However, full functionality of the Cisco wireless LAN solution occurs when it includes multiple controllers. A multiple-controller system has the following additional features:

- Autodetecting and autoconfiguring RF parameters as the controllers are added to the network.
- Same-subnet (Layer 2) roaming and inter-subnet (Layer 3) roaming.
- Automatic access point failover to any redundant controller with a reduced access point load (see the Cisco Wireless LAN Controller Failover Protection, page 2-13).

Figure 2-3 shows a typical multiple-controller deployment. The figure also shows an optional dedicated management network and the three physical connection types between the network and the controllers.
Operating System Software

The operating system software controls controllers and lightweight access points. It includes full operating system security and radio resource management (RRM) features.

Operating System Security

Operating system security bundles Layer 1, Layer 2, and Layer 3 security components into a simple, Cisco WLAN solution-wide policy manager that creates independent security policies for each of up to 16 wireless LANs. See “Cisco UWN Solution WLANs” section on page 2-11.

The 802.11 Static WEP weaknesses can be overcome using the following robust industry-standard security solutions:

- 802.1X dynamic keys with extensible authentication protocol (EAP).
- Wi-Fi protected access (WPA) dynamic keys. The Cisco WLAN solution WPA implementation includes:
  - Temporal key integrity protocol (TKIP) and message integrity code checksum dynamic keys
  - WEP keys, with or without a preshared key passphrase
- RSN with or without a preshared key
Optional MAC filtering  
The WEP problem can be further solved using the following industry-standard Layer 3 security solutions:

- Passthrough VPNs  
- Local and RADIUS MAC address filtering  
- Local and RADIUS user/password authentication

- Manual and automated disabling to block access to network services. In manual disabling, you block access using client MAC addresses. In automated disabling, which is always active, the operating system software automatically blocks access to network services for a user-defined period of time when a client fails to authenticate for a fixed number of consecutive attempts. This feature can be used to deter brute-force login attacks.

These and other security features use industry-standard authorization and authentication methods to ensure the highest possible security for your business-critical wireless LAN traffic.

Cisco WLAN Solution Wired Security

Each controller and lightweight access point is manufactured with a unique, signed X.509 certificate. These signed certificates are used to verify downloaded code before it is loaded, ensuring that hackers do not download malicious code into any controller or lightweight access point.

The controllers and lightweight access points also use the signed certificates to verify the downloaded code before it is loaded, ensuring that hackers do not download malicious code into any Cisco wireless controller or lightweight access point.

Layer 2 and Layer 3 Operation

Lightweight Access Point Protocol (LWAPP) communications between the controller and lightweight access points can be conducted at Layer 2 or Layer 3. Control and Provisioning of Wireless Access Points protocol (CAPWAP) communications between the controller and lightweight access points are conducted at Layer 3. Layer 2 mode does not support CAPWAP.

Note  
Controller software release 5.2 or later releases support only Layer 3 CAPWAP mode, controller software releases 5.0 and 5.1 support only Layer 3 LWAPP mode, and controller software releases prior to 5.0 support Layer 2 or Layer 3 LWAPP mode.

Note  
The IPv4 network layer protocol is supported for transport through a CAPWAP or LWAPP controller system. IPv6 (for clients only) and Appletalk are also supported but only on Cisco 5500 Series Controllers, and the Cisco WiSM. Other Layer 3 protocols (such as IPX, DECnet Phase IV, OSI CLNP, and so on) and Layer 2 (bridged) protocols (such as LAT and NetBeui) are not supported.
Operational Requirements

The requirement for Layer 3 LWAPP communications is that the controller and lightweight access points can be connected through Layer 2 devices on the same subnet or connected through Layer 3 devices across subnets. Another requirement is that the IP addresses of access points should be either statically assigned or dynamically assigned through an external DHCP server.

The requirement for Layer 3 CAPWAP communications across subnets is that the controller and lightweight access points are connected through Layer 3 devices. Another requirement is that the IP addresses of access points should be either statically assigned or dynamically assigned through an external DHCP server.

Configuration Requirements

When you are operating the Cisco wireless LAN solution in Layer 2 mode, you must configure a management interface to control your Layer 2 communications.

When you are operating the Cisco wireless LAN solution in Layer 3 mode, you must configure an AP-manager interface to control lightweight access points and a management interface as configured for Layer 2 mode.

Cisco Wireless LAN Controllers

When you are adding lightweight access points to a multiple-controller deployment network, it is convenient to have all lightweight access points associate with one master controller on the same subnet. That way, you do not have to log into multiple controllers to find out which controller newly-added lightweight access points are associated with.

One controller in each subnet can be assigned as the master controller while adding lightweight access points. As long as a master controller is active on the same subnet, all new access points without a primary, secondary, and tertiary controller assigned automatically attempt to associate with the master controller. This process is described in the “Cisco Wireless LAN Controller Failover Protection” section on page 2-13.

You can monitor the master controller using the WCS Web User Interface and watch as access points associate with the master controller. You can then verify the access point configuration and assign a primary, secondary, and tertiary controller to the access point, and reboot the access point so it reassociates with its primary, secondary, or tertiary controller.

Note

Lightweight access points without a primary, secondary, and tertiary controller assigned always search for a master controller first upon reboot. After adding lightweight access points through the master controller, you should assign primary, secondary, and tertiary controllers to each access point. We recommend that you disable the master setting on all controllers after initial configuration.
Client Location

When you use Cisco WCS in your Cisco wireless LAN solution, controllers periodically determine the client, rogue access point, rogue access point client, radio frequency ID (RFID) tag location and store the locations in the Cisco WCS database. For more information on location solutions, see these documents:

*Cisco Wireless Control System Configuration Guide:*

*Cisco Location Appliance Configuration Guide:*

Cisco 3300 Series Mobility Services Engine Configuration Guide:

Controller Platforms

Controllers are enterprise-class high-performance wireless switching platforms that support 802.11a/n and 802.11b/g/n protocols. They operate under control of the operating system, which includes the radio resource management (RRM), creating a Cisco UWN 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.

The following controllers are supported in software release 7.2:

- Cisco 2500 Series Controller
- Cisco 5500 Series Controller
- Catalyst 6500 series switch Wireless Services Module (WiSM2s)
- Cisco Flex 7500 Series Controller

Cisco 2500 Series Controller

The Cisco 2500 Series Wireless Controller works in conjunction with Cisco lightweight access points and the Cisco Wireless Control System (WCS) to provide system-wide wireless LAN functions. As a component of the Cisco Unified Wireless Network (CUWN), the Cisco 2500 Series controller provides real-time communication between a wireless access points and other devices to deliver centralized security policies, guest access, wireless intrusion prevention system (wIPS), context-aware (location), RF management, quality of services for mobility services such as voice and video, and OEAP support for the teleworker solution.

Cisco 2500 Series Wireless Controllers support up to 50 lightweight access points in increments of 5 and 25 access points with a minimum of 5 access points.

The Cisco 2500 Series Controller offers robust coverage with 802.11 a/b/g or delivers reliability using 802.11n and Cisco Next-Generation Wireless Solutions and Cisco Enterprise Wireless Mesh.
Features Not Supported

- Wired guest access
- Cannot be configured as an auto anchor controller. However you can configure it as a foreign controller
- Bandwidth contract
- Access points in direct connect mode
- Service port
- Apple Talk Bridging
- LAG

Cisco 5500 Series Controllers

The Cisco 5500 Series Wireless LAN Controller is currently available in one model: 5508. The 5508 controller supports up to 500 lightweight access points and 7000 wireless clients (or 5000 wireless clients and 2500 RFID tags when using the client location feature), making it ideal for large enterprises and high-density applications.

The Cisco 5500 Series Controller can be equipped with one or two power supplies. When the controller is equipped with two power supplies, the power supplies are redundant, and either power supply can continue to power the controller if the other power supply fails.

Features Not Supported

- Static AP-manager interface

**Note** For Cisco 5500 Series Controllers, you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default, and the access points can join on this interface.

- Asymmetric mobility tunneling
- Spanning Tree Protocol (STP)
- Port mirroring
- Layer 2 access control list (ACL) support
- VPN termination (such as IPsec and L2TP)
- VPN passthrough option

**Note** You can replicate this functionality on a Cisco 5500 Series Controller by creating an open WLAN using an ACL.

- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)

**Note** The Cisco 5500 Series Controllers bridge these packets by default. If desired, you can use ACLs to block the bridging of these protocols.
Cisco Flex 7500 Series Controller

The Cisco Flex 7500 Series Controller enables you to deploy full featured, scalable, and secure FlexConnect network services across geographic locations. Cisco Flex 7500 Series Controller virtualizes the complex security, management, configuration and troubleshooting operations within the data center and then transparently extends those services to each store. Deployments using Cisco Flex 7500 Series Controller are easier for IT to set up, manage and scale.

The Cisco Flex 7500 Series Controller is designed to meet the scaling requirements to deploy the FlexConnect solution in branch networks. Cisco Unified Wireless Solution supports two major deployment models: FlexConnect and monitor mode. FlexConnect is designed to support wireless branch networks by allowing the data to be switched locally while the access points are being controlled and managed by a centralized controller. It aims at delivering a cost effective FlexConnect solution on a large scale.

The Cisco Flex 7500 Series Controller supports the following access points: 1140, 3500, 3600, 1250, 1260, 1040, 1130, 1240, 800 and the Cisco Aironet 600 Series OfficeExtend Access Point.

The Cisco Flex 7500 Series Controller provides the following features:

- Increases scalability with 3000 AP support.
- Increased resiliency using controller redundancy and FlexConnect Fault Tolerance.
- Increased traffic segmentation using FlexConnect (central and local switching).
- Increased security (PCI compliance) by supporting Enhanced wIPS for FlexConnect (ELM).
- Replicates store designs using AP groups and FlexConnect groups.

Note

The Cisco 7500 Flex Controller detects the power supply status by periodically probing the system in intervals of 10 minutes. As a result, there is a delay of 10 minutes to detect the actual power supply status on a Cisco 7500 Flex Controller.

Features Not Supported

These software features are not supported on Cisco Flex 7500 Series Controllers:

- L3 Roaming
- VideoStream
- TrustSec SXP
- IPv6
- WGB
- Multicast
- Client rate limiting for centrally switched clients

Cisco Wireless Services Module 2

The Cisco Wireless Services Module 2 (WiSM2) provides medium-sized to large single-site WLAN deployments with exceptional performance, security, and scalability to support mission-critical wireless business communications. It helps to lower hardware costs and offers flexible configuration options that can reduce the total cost of operations and ownership for wireless networks. Features include:
- Connections for up to 1000 access points and 15,000 clients
- Support for higher client density than other wireless LAN controllers
- Ability to update 500 access points at once
- Layer 3 mobility services for video, voice, guest, location, Enterprise Wireless Mesh, and teleworking
- Advanced wireless security, with Layer 1 wireless intrusion prevention system (wIPS) capabilities

**Features Not Supported**

- Static AP-manager interface
- Asymmetric mobility tunneling
- Spanning Tree Protocol (STP)
- Port mirroring
- Layer 2 access control list (ACL) support
- VPN termination (such as IPsec and L2TP)
- VPN passthrough option
- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)
- Fragmented pings on any interface

**Cisco Wireless Controller on Cisco Services-Ready Engine (SRE)**

The Cisco Wireless Controller application on the Cisco Services-Ready Engine (SRE) enables systemwide wireless functions in small to medium-sized enterprises and branch offices. Delivering 802.11n performance and scalability, the Cisco Wireless Controller on the SRE is an entry-level controller that provides low total cost of ownership and investment protection by integrating seamlessly with the existing network. The Cisco SRE Modules are router blades for the Cisco Integrated Services Routers Generation 2 (ISR G2), which allows you to provision the Cisco Wireless Controller applications on the module remotely at any time. This can help your organization to quickly deploy wireless on-demand, reduce operating costs, and consolidate the branch office infrastructure.

As a component of the Cisco Unified Wireless Network, this controller provides real-time communication between Cisco Aironet access points, the Cisco Wireless Control System (WCS), and the Cisco Mobility Services Engine (MSE) to deliver centralized security policies, wireless intrusion prevention system (wIPS) capabilities, award-winning RF management, context-aware capabilities for location tracking, and quality of service (QoS) for voice and video.

The Cisco Wireless LAN Controller on the Cisco SRE supports from five to 50 access points, and additional access point support may be added in increments of five or 25. The licensing structure supports a variety of business mobility needs as part of the basic feature set, including Enterprise Wireless Mesh, which allows access points to dynamically establish wireless connections in locations where it may be difficult or impossible to physically connect to the wired network.

The Cisco Wireless Controller application is available for Cisco SRE Internal Services Module (ISM) 300 and the Cisco SRE Service Module (SM) 700 and SM 900, with flexible licensing and deployment options.
Features Not Supported

- Wired guest access
- Cannot be configured as an auto anchor controller. However, you can configure it as a foreign controller.
- Bandwidth contract
- Access points in direct connect mode
- Service port support
- AppleTalk Bridging
- LAG

Cisco UWN Solution Wired Connections

The Cisco UWN solution components communicate with each other using industry-standard Ethernet cables and connectors. Details of the wired connections are as follows:

- The Cisco 5500 Series Controllers connect to the network using up to eight fiber-optic Gigabit Ethernet cables.
- The Cisco Flex 7500 Series Controllers support 2 x 10 Gigabit Ethernet interfaces.
- The Cisco 2500 Series Controllers support four 1 Gbps Ethernet.
- Cisco lightweight access points connect to the network using 10/100BASE-T Ethernet cables. The standard CAT-5 cable can also be used to conduct power for the lightweight access points from a network device equipped with Power over Ethernet (PoE) capability. This power distribution plan can be used to reduce the cost of individual AP power supplies and related cabling.

Cisco UWN Solution WLANs

The Cisco UWN solution can control up to 512 WLANs for lightweight access points. Each WLAN has a separate WLAN ID (1 through 512), a separate profile name, and a WLAN SSID and can be assigned with unique security policies. The lightweight access points broadcast all active Cisco UWN solution WLAN SSIDs and enforce the policies defined for each WLAN.

Note

We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers operate with optimum performance and ease of management.

If management over wireless is enabled across the Cisco UWN solution, you can manage the system across the enabled WLAN using CLI and Telnet, http/https, and SNMP.

To configure WLANs, see Chapter 8, “Working with WLANs.”
### File Transfers

You can upload and download operating system code, configuration, and certificate files to and from the controller using the GUI, CLI, or Cisco WCS as follows:

- To use the controller GUI or CLI, see Chapter 11, “Managing Controller Software and Configurations.”
- To use Cisco WCS to upgrade software, see the *Cisco Wireless Control System Configuration Guide*. Click this URL to browse to this document:
  

### Power Over Ethernet

Lightweight access points can receive power through their Ethernet cables from 802.3af-compatible Power over Ethernet (PoE) devices, which can reduce the cost of discrete power supplies, additional wiring, conduits, outlets, and installation time. PoE frees you from having to mount lightweight access points or other powered equipment near AC outlets, which provides greater flexibility in positioning the access points for maximum coverage.

When you are using PoE, you run a single CAT-5 cable from each lightweight access point to PoE-equipped network elements, such as a PoE power hub or a Cisco WLAN Solution single-line PoE injector. When the PoE equipment determines that the lightweight access point is PoE-enabled, it sends 48 VDC over the unused pairs in the Ethernet cable to power the access point.

The PoE cable length is limited by the 100BASE-T or 10BASE-T specification to 100 m or 200 m, respectively.

Lightweight access points can receive power from an 802.3af-compliant device or from the external power supply.

### Cisco Wireless LAN Controller Memory

The controller contains two kinds of memory: volatile RAM, which holds the current, active controller configuration, and NVRAM (nonvolatile RAM), which holds the reboot configuration. When you are configuring the operating system in controller, you are modifying volatile RAM; you must save the configuration from the volatile RAM to the NVRAM to ensure that the controller reboots in the current configuration.

Knowing which memory you are modifying is important when you are doing the following tasks:

- Using the configuration wizard
- Clearing the controller configuration
- Saving configurations
- Resetting the controller
- Logging out of the CLI
Cisco Wireless LAN Controller Failover Protection

During installation, we recommend that you connect all lightweight access points to a dedicated controller, and configure each lightweight access point for final operation. This step configures each lightweight access point for a primary, secondary, and tertiary controller and allows it to store the configured mobility group information.

During failover recovery, the following tasks are performed:

- The configured access point attempts to contact the primary, secondary, and tertiary controllers, and then attempts to contact the IP addresses of the other controllers in the mobility group.
- DNS is resolved with controller IP address.
- DHCP servers get the controller IP Addresses (vendor specific option 43 in DHCP offer).

In multiple-controller deployments, if one controller fails, the access points perform the following tasks:

- If the lightweight access point has a primary, secondary, and tertiary controller assigned, it attempts to associate with that controller.
- If the access point has no primary, secondary, or tertiary controllers assigned or if its primary, secondary, or tertiary controllers are unavailable, it attempts to associate with a master controller.
- If the access point finds no master controller, it attempts to contact stored mobility group members by the IP address.
- If the mobility group members are available, and if the lightweight access point has no primary, secondary, and tertiary controllers assigned and there is no master controller active, it attempts to associate with the least-loaded controller to respond to its discovery messages.

When sufficient controllers are deployed, if one controller fails, active access point client sessions are momentarily dropped while the dropped access point associates with another controller, allowing the client device to immediately reassociate and reauthenticate.

To know more about high availability, see http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a00809a3f5d.shtml
Using the Web-Browser and CLI Interfaces

This chapter describes how to initially configure and log into the controller. It contains these sections:

- Configuring the Controller Using the GUI Configuration Wizard, page 3-1
- Configuring the Controller Using the CLI Configuration Wizard, page 3-13
- Using the Controller Web GUI, page 3-16
- Loading an Externally Generated SSL Certificate, page 3-20
- Using the Controller CLI, page 3-22
- Using the AutoInstall Feature for Controllers Without a Configuration, page 3-26
- Managing the Controller System Date and Time, page 3-30
- Configuring Telnet and SSH Sessions, page 3-35
- Managing the Controller Wirelessly, page 3-37

Configuring the Controller Using the GUI Configuration Wizard

The configuration wizard enables you to configure basic settings on the controller. You can run the wizard after you receive the controller from the factory or after the controller has been reset to factory defaults. The configuration wizard is available in GUI or CLI format.

This section contains the following topics:

- Connecting the Controller’s Console Port, page 3-1
- Configuring the Controller (GUI), page 3-2
- Additional References, page 3-13

Connecting the Controller’s Console Port

Before you can configure the controller for basic operations, you need to connect it to a PC that uses a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip).
Chapter 3      Using the Web-Browser and CLI Interfaces

Configuring the Controller Using the GUI Configuration Wizard

Note

On Cisco 5500 Series Controllers, you can use either the RJ-45 console port or the USB console port. If you use the USB console port, plug the 5-pin mini Type B connector into the controller’s USB console port and the other end of the cable into the PC’s USB Type A port. The first time that you connect a Windows PC to the USB console port, you are prompted to install the USB console driver. Follow the installation prompts to install the driver. The USB console driver maps to a COM port on your PC; you then need to map the terminal emulator application to the COM port.

Step 1  Connect one end of a null-modem serial cable to the controller’s console port and the other end to your PC’s serial port.

Step 2  Start the PC’s VT-100 terminal emulation program.

Step 3  Configure the terminal emulation program for these parameters:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control

Step 4  Plug the AC power cord into the controller and a grounded 100 to 240 VAC, 50/60-Hz electrical outlet. Turn on the power supply. The bootup script displays operating system software initialization (code download and power-on self test verification) and basic configuration.

If the controller passes the power-on self test, the bootup script runs the configuration wizard, which prompts you for basic configuration input.

Configuring the Controller (GUI)

Step 1  Connect your PC to the service port and configure it to use the same subnet as the controller (for example, 209.165.200.225).

Step 2  Start Internet Explorer 6.0 SP1 (or later) or Firefox 2.0.0.11 (or later) on your PC and browse to http://209.165.200.225. The configuration wizard appears.
Step 3  In the System Name text box, enter the name that you want to assign to this controller. You can enter up to 31 ASCII characters.

Step 4  In the User Name text box, enter the administrative username to be assigned to this controller. You can enter up to 24 ASCII characters. The default username is admin.

Step 5  In the Password and Confirm Password text boxes, enter the administrative password to be assigned to this controller. You can enter up to 24 ASCII characters. The default password is admin.

Starting in release 7.0.116.0, the following password policy has been implemented:

- The password must contain characters from at least three of the following classes:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters.
- No character in the password must be repeated more than three times consecutively.
- The new password must not be the same as the associated username and not be the username reversed.
- The password must not be cisco, ocsic, or any variant obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

Step 6  Click Next. The SNMP Summary screen appears.
Step 7 If you want to enable Simple Network Management Protocol (SNMP) v1 mode for this controller, choose **Enable** from the SNMP v1 Mode drop-down list. Otherwise, leave this parameter set to **Disable**.

**Note** SNMP manages nodes (servers, workstations, routers, switches, and so on) on an IP network. Currently, there are three versions of SNMP: SNMPv1, SNMPv2c, and SNMPv3.

Step 8 If you want to enable SNMPv2c mode for this controller, leave this parameter set to **Enable**. Otherwise, choose **Disable** from the SNVP v2c Mode drop-down list.

Step 9 If you want to enable SNMPv3 mode for this controller, leave this parameter set to **Enable**. Otherwise, choose **Disable** from the SNVP v3 Mode drop-down list.

Step 10 Click **Next**.

Step 11 When the following message appears, click **OK**:

> Default values are present for v1/v2c community strings. Please make sure to create new v1/v2c community strings once the system comes up. Please make sure to create new v3 users once the system comes up.

The Service Interface Configuration screen appears.
Step 12  If you want the controller’s service-port interface to obtain an IP address from a DHCP server, select the **DHCP Protocol Enabled** check box. If you do not want to use the service port or if you want to assign a static IP address to the service port, leave the check box unselected.

**Note**  The service-port interface controls communications through the service port. Its IP address must be on a different subnet from the management interface. This configuration enables you to manage the controller directly or through a dedicated management network to ensure service access during network downtime.

Step 13  Perform one of the following:

- If you enabled DHCP in Step 12, clear out any entries in the IP Address and Netmask text boxes, leaving them blank.
- If you disabled DHCP in Step 12, enter the static IP address and netmask for the service port in the IP Address and Netmask text boxes.

Step 14  Click Next. The LAG Configuration screen appears.
Step 15 To enable link aggregation (LAG), choose Enabled from the Link Aggregation (LAG) Mode drop-down list. To disable LAG, leave this text box set to Disabled.

Step 16 Click Next. The Management Interface Configuration screen appears.

Note The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers.
**Step 17** In the VLAN Identifier text box, enter the VLAN identifier of the management interface (either a valid VLAN identifier or 0 for an untagged VLAN). The VLAN identifier should be set to match the switch interface configuration.

**Step 18** In the IP Address text box, enter the IP address of the management interface.

**Step 19** In the Netmask text box, enter the IP address of the management interface netmask.

**Step 20** In the Gateway text box, enter the IP address of the default gateway.

**Step 21** In the Port Number text box, enter the number of the port assigned to the management interface. Each interface is mapped to at least one primary port.

**Step 22** In the Backup Port text box, enter the number of the backup port assigned to the management interface. If the primary port for the management interface fails, the interface automatically moves to the backup port.

**Step 23** In the Primary DHCP Server text box, enter the IP address of the default DHCP server that will supply IP addresses to clients, the controller’s management interface, and optionally, the service port interface.

**Step 24** In the Secondary DHCP Server text box, enter the IP address of an optional secondary DHCP server that will supply IP addresses to clients, the controller’s management interface, and optionally, the service port interface.

**Step 25** Click Next. The AP-Manager Interface Configuration screen appears.

---

**Note** This screen does not appear for Cisco 5500 Series Controllers because you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

**Step 26** In the IP Address text box, enter the IP address of the AP-manager interface.

**Step 27** Click Next. The Miscellaneous Configuration screen appears.

**Figure 3-6 Configuration Wizard — Miscellaneous Configuration Screen**

**Step 28** In the RF Mobility Domain Name text box, enter the name of the mobility group/RF group to which you want the controller to belong.
Configuring the Controller Using the GUI Configuration Wizard

Chapter 3 Using the Web-Browser and CLI Interfaces

Note
Although the name that you enter here is assigned to both the mobility group and the RF group, these groups are not identical. Both groups define clusters of controllers, but they have different purposes. All of the controllers in an RF group are usually also in the same mobility group and vice versa. However, a mobility group facilitates scalable, system-wide mobility and controller redundancy while an RF group facilitates scalable, system-wide dynamic RF management.

Step 29
The Configured Country Code(s) text box shows the code for the country in which the controller will be used. If you want to change the country of operation, select the check box for the desired country.

Note
You can choose more than one country code if you want to manage access points in multiple countries from a single controller. After the configuration wizard runs, you need to assign each access point joined to the controller to a specific country. See the “Configuring Country Codes” section on page 9-87 for instructions.

Step 30
Click Next.

Step 31
When the following message appears, click OK:

Warning! To maintain regulatory compliance functionality, the country code setting may only be modified by a network administrator or qualified IT professional. Ensure that proper country codes are selected before proceeding.

The Virtual Interface Configuration screen appears.

Figure 3-7 Configuration Wizard — Virtual Interface Configuration Screen

Step 32
In the IP Address text box, enter the IP address of the controller’s virtual interface. You should enter a fictitious, unassigned IP address.

Note
The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.
Step 33 In the DNS Host Name text box, enter the name of the Domain Name System (DNS) gateway used to verify the source of certificates when Layer 3 web authorization is enabled.

**Note** To ensure connectivity and web authentication, the DNS server should always point to the virtual interface. If a DNS host name is configured for the virtual interface, then the same DNS host name must be configured on the DNS servers used by the client.

Step 34 Click Next. The WLAN Configuration screen appears.

**Figure 3-8 Configuration Wizard — WLAN Configuration Screen**

Step 35 In the Profile Name text box, enter up to 32 alphanumeric characters for the profile name to be assigned to this WLAN.

Step 36 In the WLAN SSID text box, enter up to 32 alphanumeric characters for the network name, or service set identifier (SSID). The SSID enables basic functionality of the controller and allows access points that have joined the controller to enable their radios.

Step 37 Click Next.

Step 38 When the following message appears, click OK:

Default Security applied to WLAN is: [WPA2(AES)][Auth(802.1x)]. You can change this after the wizard is complete and the system is rebooted.

The RADIUS Server Configuration screen appears.
Step 39  In the Server IP Address text box, enter the IP address of the RADIUS server.

Step 40  From the Shared Secret Format drop-down list, choose **ASCII** or **Hex** to specify the format of the shared secret.

**Note**  Due to security reasons, the RADIUS shared secret key reverts to ASCII mode even if you have selected HEX as the shared secret format from the Shared Secret Format drop-down list.

Step 41  In the Shared Secret and Confirm Shared Secret text boxes, enter the secret key used by the RADIUS server.

Step 42  In the Port Number text box, enter the communication port of the RADIUS server. The default value is 1812.

Step 43  To enable the RADIUS server, choose **Enabled** from the Server Status drop-down list. To disable the RADIUS server, leave this text box set to **Disabled**.

Step 44  Click **Apply**. The 802.11 Configuration screen appears.
Figure 3-10  Configuration Wizard — 802.11 Configuration Screen

Step 45  To enable the 802.11a, 802.11b, and 802.11g lightweight access point networks, leave the 802.11a Network Status, 802.11b Network Status, and 802.11g Network Status check boxes selected. To disable support for any of these networks, unselect the check boxes.

Step 46  To enable the controller’s radio resource management (RRM) auto-RF feature, leave the Auto RF check box selected. To disable support for the auto-RF feature, unselect this check box.

Note  The auto-RF feature enables the controller to automatically form an RF group with other controllers. The group dynamically elects a leader to optimize RRM parameter settings, such as channel and transmit power assignment, for the group.

Step 47  Click Next. The Set Time screen appears.
Figure 3-11  Configuration Wizard — Set Time Screen

Step 48  To manually configure the system time on your controller, enter the current date in Month/DD/YYYY format and the current time in HH:MM:SS format.

Step 49  To manually set the time zone so that Daylight Saving Time (DST) is not set automatically, enter the local hour difference from Greenwich Mean Time (GMT) in the Delta Hours text box and the local minute difference from GMT in the Delta Mins text box.

Note  When manually setting the time zone, enter the time difference of the local current time zone with respect to GMT (+/–). For example, Pacific time in the United States is 8 hours behind GMT. Therefore, it is entered as –8.

Step 50  Click Next. The Configuration Wizard Completed screen appears.
Step 51  Click **Save and Reboot** to save your configuration and reboot the controller.

Step 52  When the following message appears, click **OK**:

Configuration will be saved and the controller will be rebooted. Click ok to confirm.

Step 53  The controller saves your configuration, reboots, and prompts you to log in. Follow the instructions in the “Using the Controller Web GUI” section on page 3-16 to log into the controller.

Additional References

- “Resetting the Controller to Default Settings” section on page 4-116 for instructions on returning the controller to factory defaults.
- Chapter 13, “Configuring Radio Resource Management,”
- Chapter 15, “Configuring Mobility Groups,”
- See the “SNMP Community Strings” section on page 4-40 and the “Changing the Default Values for SNMP v3 Users” section on page 4-42.

Configuring the Controller Using the CLI Configuration Wizard

This section contains the following topics:

- Guidelines and Limitations, page 3-14
- Configuring the Controller (CLI), page 3-14
Chapter 3  Using the Web-Browser and CLI Interfaces

Guidelines and Limitations

- The available options appear in brackets after each configuration parameter. The default value appears in all uppercase letters.
- If you enter an incorrect response, the controller provides you with an appropriate error message, such as “Invalid Response,” and returns you to the wizard prompt.
- Press the hyphen key if you ever need to return to the previous command line.

Configuring the Controller (CLI)

### Step 1
When prompted to terminate the AutoInstall process, enter **yes**. If you do not enter **yes**, the AutoInstall process begins after 30 seconds.

*Note*  The AutoInstall feature downloads a configuration file from a TFTP server and then loads the configuration onto the controller automatically. See the “Using the AutoInstall Feature for Controllers Without a Configuration” section on page 3-26 for more information.

### Step 2
Enter the system name, which is the name that you want to assign to the controller. You can enter up to 31 ASCII characters.

### Step 3
Enter the administrative username and password to be assigned to this controller. You can enter up to 24 ASCII characters for each.

Starting in release 7.0.116.0, the following password policy has been implemented:

- The password must contain characters from at least three of the following classes:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters.
- No character in the password must be repeated more than three times consecutively.
- The new password must not be the same as the associated username and not be the username reversed.
- The password must not be cisco, ocsic, or any variant obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

### Step 4
If you want the controller’s service-port interface to obtain an IP address from a DHCP server, enter **DHCP**. If you do not want to use the service port or if you want to assign a static IP address to the service port, enter **none**.

*Note*  The service-port interface controls communications through the service port. Its IP address must be on a different subnet from the management interface. This configuration enables you to manage the controller directly or through a dedicated management network to ensure service access during network downtime.

### Step 5
If you entered **none** in Step 4, enter the IP address and netmask for the service-port interface on the next two lines.
Step 6 Enable or disable link aggregation (LAG) by choosing yes or NO.
Step 7 Enter the IP address of the management interface.

Note The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers.

Step 8 Enter the IP address of the management interface netmask.
Step 9 Enter the IP address of the default router.
Step 10 Enter the VLAN identifier of the management interface (either a valid VLAN identifier or 0 for an untagged VLAN). The VLAN identifier should be set to match the switch interface configuration.

Note This prompt does not appear for Cisco 5500 Series Controllers because you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

Step 11 Enter the IP address of the default DHCP server that will supply IP addresses to clients, the controller’s management interface, and optionally, the service port interface. Enter the IP address of the AP-manager interface.

Note This prompt does not appear for Cisco 5500 Series Controllers because you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

Step 12 Enter the IP address of the controller’s virtual interface. You should enter a fictitious unassigned IP address.

Note The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.

Step 13 If desired, enter the name of the mobility group/RF group to which you want the controller to belong.

Note Although the name that you enter here is assigned to both the mobility group and the RF group, these groups are not identical. Both groups define clusters of controllers, but they have different purposes. All of the controllers in an RF group are usually also in the same mobility group and vice versa. However, a mobility group facilitates scalable, system-wide mobility and controller redundancy while an RF group facilitates scalable, system-wide dynamic RF management.

Step 14 Enter the network name or service set identifier (SSID). The SSID enables basic functionality of the controller and allows access points that have joined the controller to enable their radios.

Step 15 Enter YES to allow clients to assign their own IP address or no to require clients to request an IP address from a DHCP server.

Step 16 To configure a RADIUS server now, enter YES and then enter the IP address, communication port, and secret key of the RADIUS server. Otherwise, enter no. If you enter no, the following message appears: “Warning! The default WLAN security policy requires a RADIUS server. Please see the documentation for more details.”

Step 17 Enter the code for the country in which the controller will be used.

Note Enter help to view the list of available country codes.
Note: You can enter more than one country code if you want to manage access points in multiple
countries from a single controller. To do so, separate the country codes with a comma (for
example, US,CA,MX). After the configuration wizard runs, you need to assign each access point
joined to the controller to a specific country.

Step 18 Enable or disable the 802.11b, 802.11a, and 802.11g lightweight access point networks by entering YES
or no.

Step 19 Enable or disable the controller’s radio resource management (RRM) auto-RF feature by entering YES
or no.

Note: The auto-RF feature enables the controller to automatically form an RF group with other
controllers. The group dynamically elects a leader to optimize RRM parameter settings, such as
channel and transmit power assignment, for the group.

Step 20 If you want the controller to receive its time setting from an external Network Time Protocol (NTP)
server when it powers up, enter YES to configure an NTP server. Otherwise, enter no.

Note: The controller network module installed in a Cisco Integrated Services Router does not have a
battery and cannot save a time setting. Therefore, it must receive a time setting from an external
NTP server when it powers up.

Step 21 If you entered no in Step 20 and want to manually configure the system time on your controller now,
enter YES. If you do not want to configure the system time now, enter no.

Step 22 If you entered YES in Step 21, enter the current date in MM/DD/YY format and the current time in
HH:MM:SS format.

Step 23 When prompted to verify that the configuration is correct, enter yes or NO.
The controller saves your configuration, reboots, and prompts you to log in. Follow the instructions in
the “Using the Controller CLI” section on page 3-22 to log into the controller.

Using the Controller Web GUI

A web browser, or graphical user interface (GUI), is built into each controller. It allows up to five users
to simultaneously browse into the controller HTTP or HTTPS (HTTP + SSL) management pages to
configure parameters and monitor the operational status for the controller and its associated access
points.

This section contains the following topics:

- Guidelines and Limitations, page 3-17
- Logging On to the GUI, page 3-17
- Logging Out of the GUI, page 3-17
- Enabling Web and Secure Web Modes, page 3-18
Guidelines and Limitations

Follow these guidelines when using the controller GUI:

- The GUI must be used on a PC running Windows XP SP1 (or later) or Windows 2000 SP4 (or later).
- The GUI is fully compatible with Microsoft Internet Explorer version 6.0 SP1 (or later) or Mozilla Firefox 2.0.0.11 (or later). Internet Explorer 6.0 SP1 (or later) and Mozilla Firefox 2.0.0.11 (or later) are the only browsers supported for accessing the controller GUI and for using web authentication.
- Opera is not supported.
- You can use either the service port interface or the management interface to access the GUI. We recommend that you use the service-port interface. See Chapter 4, “Configuring Ports and Interfaces,” for instructions on configuring the service port interface.
- Click Help at the top of any page in the GUI to display online help. You might need to disable your browser’s pop-up blocker to view the online help.
- We recommend that you enable the HTTPS interface and disable the HTTP interface to ensure more robust security for your Cisco UWN solution.

Logging On to the GUI

**Step 1** Enter the controller IP address in your browser’s address line. For a secure connection, enter `https://ip-address`. For a less secure connection, enter `http://ip-address`.

**Note** See the “Enabling Web and Secure Web Modes” section on page 3-18 for instructions on setting up HTTPS.

**Step 2** When prompted, enter a valid username and password and click **OK**. The controller Summary page appears.

**Note** The administrative username and password that you created in the configuration wizard are case sensitive. The default username is `admin`, and the default password is `admin`.

Logging Out of the GUI

**Step 1** Click **Logout** in the top right corner of the page.

**Step 2** Click **Close** to complete the logoff process and prevent unauthorized users from accessing the controller GUI.

**Step 3** When prompted to confirm your decision, click **Yes**.
Enabling Web and Secure Web Modes

This section provides instructions for enabling the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Socket Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You also have the option of downloading an externally generated certificate. This section contains the following topics:

- Enabling Web and Secure Web Modes (GUI), page 3-18
- Enabling Web and Secure Web Modes (CLI), page 3-19

Enabling Web and Secure Web Modes (GUI)

Step 1 Choose Management > HTTP to open the HTTP Configuration page.

Step 2 To enable web mode, which allows users to access the controller GUI using “http://ip-address,” choose Enabled from the HTTP Access drop-down list. Otherwise, choose Disabled. The default value is Disabled. Web mode is not a secure connection.

Step 3 To enable secure web mode, which allows users to access the controller GUI using “https://ip-address,” choose Enabled from the HTTPS Access drop-down list. Otherwise, choose Disabled. The default value is Enabled. Secure web mode is a secure connection.

Step 4 In the Web Session Timeout text box, enter the amount of time (in minutes) before the web session times out due to inactivity. You can enter a value between 30 and 160 minutes (inclusive), and the default value is 30 minutes.

Step 5 Click Apply to commit your changes.
**Step 6**
If you enabled secure web mode in Step 3, the controller generates a local web administration SSL certificate and automatically applies it to the GUI. The details of the current certificate appear in the middle of the HTTP Configuration page.

*Note*
If you want to download your own SSL certificate to the controller, follow the instructions in the “Loading an Externally Generated SSL Certificate” section on page 3-20.

*Note*
If desired, you can delete the current certificate by clicking **Delete Certificate** and have the controller generate a new certificate by clicking **Regenerate Certificate**.

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

---

**Enabling Web and Secure Web Modes (CLI)**

**Step 1**
To enable or disable web mode, enter this command:

```
config network webmode {enable | disable}
```

This command allows users to access the controller GUI using “http://ip-address.” The default value is disabled. Web mode is not a secure connection.

**Step 2**
To enable or disable secure web mode, enter this command:

```
config network secureweb {enable | disable}
```

This command allows users to access the controller GUI using “https://ip-address.” The default value is enabled. Secure web mode is a secure connection.

**Step 3**
To enable or disable secure web mode with increased security, enter this command:

```
config network secureweb cipher-option high {enable | disable}
```

This command allows users to access the controller GUI using “https://ip-address” but only from browsers that support 128-bit (or larger) ciphers. The default value is disabled.

**Step 4**
To enable or disable SSLv2 for web administration, enter this command:

```
config network secureweb cipher-option sslv2 {enable | disable}
```

If you disable SSLv2, users cannot connect using a browser configured with SSLv2 only. They must use a browser that is configured to use a more secure protocol such as SSLv3 or later. The default value is enabled.

**Step 5**
To verify that the controller has generated a certificate, enter this command:

```
show certificate summary
```

Information similar to the following appears:

```
Web Administration Certificate................. Locally Generated
Web Authentication Certificate................. Locally Generated
Certificate compatibility mode:............... off
```

*Note*
If you want to download your own SSL certificate to the controller, follow the instructions in the “Loading an Externally Generated SSL Certificate” section on page 3-20.
Loading an Externally Generated SSL Certificate

You can use a TFTP server to download an externally generated SSL certificate to the controller.

This section contains the following topics:

- Guidelines and Limitations, page 3-20
- Loading an SSL Certificate, page 3-20

Guidelines and Limitations

- If you load the certificate through the service port, the TFTP server must be on the same subnet as the controller because the service port is not routable, or you must create static routes on the controller. Also, if you load the certificate through the distribution system network port, the TFTP server can be on any subnet.
- A third-party TFTP server cannot run on the same PC as the Cisco WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.
- Chained certificates are supported for web authentication only and not for the management certificate.
- Every HTTPS certificate contains an embedded RSA key. The length of the key can vary from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you obtain a new certificate from a Certificate Authority, make sure that the RSA key embedded in the certificate is at least 768 bits long.

Loading an SSL Certificate

This section contains the following topics:

- Loading an SSL Certificate (GUI), page 3-20
- Loading an SSL Certificate (CLI), page 3-21

Loading an SSL Certificate (GUI)

Step 1  On the HTTP Configuration page, select the Download SSL Certificate check box.
Figure 3-14   HTTP Configuration Page

Step 2  In the Server IP Address text box, enter the IP address of the TFTP server.
Step 3  In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.
Step 4  In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.
Step 5  In the Certificate File Path text box, enter the directory path of the certificate.
Step 6  In the Certificate File Name text box, enter the name of the certificate (*webadmincert_name*.pem).
Step 7  (Optional) In the Certificate Password text box, enter a password to encrypt the certificate.
Step 8  Click **Apply** to commit your changes.
Step 9  Click **Save Configuration** to save your changes.
Step 10  To reboot the controller for your changes to take effect, choose **Commands > Reboot > Reboot > Save and Reboot**.

---

**Loading an SSL Certificate (CLI)**

Step 1  Use a password to encrypt the HTTPS certificate in a .PEM-encoded file. The PEM-encoded file is called a web administration certificate file (*webadmincert_name*.pem).
Step 2  Move the *webadmincert_name*.pem file to the default directory on your TFTP server.
Step 3  To view the current download settings, enter this command and answer **n** to the prompt:

```
transfer download start
```

Information similar to the following appears:

```
Mode........................................... TFTP
Data Type...................................... Admin Cert
TFTP Server IP................................. xxx.xxx.xxx.xxx
TFTP Path...................................... <directory path>
```
Step 4  Use these commands to change the download settings:

- `transfer download mode tftp`
- `transfer download datatype webadmcert`
- `transfer download serverip TFTP_server IP_address`
- `transfer download path absolute_TFTP_server_path_to_the_update_file`
- `transfer download filename webadmincert_name.pem`

Step 5  To set the password for the .PEM file so that the operating system can decrypt the web administration SSL key and certificate, enter this command:

- `transfer download certpassword private_key_password`

Step 6  To confirm the current download settings and start the certificate and key download, enter this command and answer `y` to the prompt:

- `transfer download start`

Information similar to the following appears:

- Mode........................................... TFTP
- Data Type..................................... Site Cert
- TFTP Server IP.............................. xxx.xxx.xxx.xxx
- TFTP Path.................................... directory path
- TFTP Filename............................... webadmincert_name

Are you sure you want to start? (y/n)  **y**

TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.

Step 7  To save the SSL certificate, key, and secure web password to NVRAM so that your changes are retained across reboots, enter this command:

- `save config`

Step 8  To reboot the controller, enter this command:

- `reset system`

### Using the Controller CLI

This section contains the following topics:

- **Information About the Controller CLI**, page 3-23
- **Guidelines and Limitations**, page 3-23
- **Logging on to the Controller CLI**, page 3-23
- **Using a Local Serial Connection**, page 3-23
- **Using a Remote Ethernet Connection**, page 3-24
- **Logging Out of the CLI**, page 3-25
- **Navigating the CLI**, page 3-25
Information About the Controller CLI

A Cisco UWN solution command-line interface (CLI) is built into each controller. The CLI enables you to use a VT-100 terminal emulation program to locally or remotely configure, monitor, and control individual controllers and its associated lightweight access points. The CLI is a simple text-based, tree-structured interface that allows up to five users with Telnet-capable terminal emulation programs to access the controller.

Guidelines and Limitations

- On Cisco 5500 Series Controllers, you can use either the RJ-45 console port or the USB console port. If you use the USB console port, plug the 5-pin mini Type B connector into the controller’s USB console port and the other end of the cable into the PC’s USB Type A port. The first time that you connect a Windows PC to the USB console port, you are prompted to install the USB console driver. Follow the installation prompts to install the driver. The USB console driver maps to a COM port on your PC; you then need to map the terminal emulator application to the COM port.
- If you want to input any strings from the XML configuration into CLI commands, you must enclose the strings in quotation marks.

Logging on to the Controller CLI

You access the controller CLI using one of two methods:
- A direct serial connection to the controller console port
- A remote console session over Ethernet through the preconfigured service port or the distribution system ports

Before you log on to the CLI, configure your connectivity and environment variables based on the type of connection you use.

Using a Local Serial Connection

You need these items to connect to the serial port:
- A PC that is running a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip)
- A null-modem serial cable

To log into the controller CLI through the serial port, follow these steps:

**Step 1** Connect one end of a null-modem serial cable to the controller’s console port and the other end to your PC’s serial port.

**Step 2** Start the PC’s VT-100 terminal emulation program. Configure the terminal emulation program for these parameters:
- 9600 baud
Chapter 3      Using the Web-Browser and CLI Interfaces

Using the Controller CLI

- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control

**Note**
The controller serial port is set for a 9600 baud rate and a short timeout. If you would like to change either of these values, enter `config serial baudrate baudrate` and `config serial timeout timeout` to make your changes. If you enter `config serial timeout 0`, serial sessions never time out.

**Step 3**
When prompted, enter a valid username and password to log into the controller. The administrative username and password that you created in the configuration wizard are case sensitive.

**Note**
The default username is `admin`, and the default password is `admin`.

The CLI displays the root level system prompt:

```
#(system prompt)>
```

**Note**
The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the `config prompt` command.

---

Using a Remote Ethernet Connection

You need these items to connect to a controller remotely:

- A PC with access to the controller over the Ethernet network
- The IP address of the controller
- A VT-100 terminal emulation program or a DOS shell for the Telnet session

**Note**
By default, controllers block Telnet sessions. You must use a local connection to the serial port to enable Telnet sessions.

To log into the controller CLI through a remote Ethernet connection, follow these steps:

**Step 1**
Verify that your VT-100 terminal emulation program or DOS shell interface is configured with these parameters:

- Ethernet address
- Port 23

**Step 2**
Use the controller IP address to Telnet to the CLI.
Step 3  When prompted, enter a valid username and password to log into the controller. The administrative username and password that you created in the configuration wizard are case sensitive.

Note  The default username is *admin*, and the default password is *admin*.

The CLI displays the root level system prompt:

```
# (system prompt)>
```

Note  The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the `config prompt` command.

---

## Logging Out of the CLI

When you finish using the CLI, navigate to the root level and enter `logout`. The system prompts you to save any changes you made to the volatile RAM.

Note  The CLI automatically logs you out without saving any changes after 5 minutes of inactivity. You can set the automatic logout from 0 (never log out) to 160 minutes using the `config serial timeout` command.

---

## Navigating the CLI

The CLI is organized around five levels:

- Root Level
- Level 2
- Level 3
- Level 4
- Level 5

When you log into the CLI, you are at the root level. From the root level, you can enter any full command without first navigating to the correct command level. Table 3-1 lists commands you use to navigate the CLI and to perform common tasks.

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>At the root level, view system wide navigation commands</td>
</tr>
<tr>
<td>?</td>
<td>View commands available at the current level</td>
</tr>
<tr>
<td>command ?</td>
<td>View parameters for a specific command</td>
</tr>
<tr>
<td>exit</td>
<td>Move down one level</td>
</tr>
<tr>
<td>Ctrl-Z</td>
<td>Return from any level to the root level</td>
</tr>
</tbody>
</table>
Using the AutoInstall Feature for Controllers Without a Configuration

This section contains the following topics:

- Information About the AutoInstall Feature, page 3-26
- Guidelines and Limitations, page 3-27
- Obtaining an IP Address Through DHCP and Downloading a Configuration File from a TFTP Server, page 3-27
- Selecting a Configuration File, page 3-28
- Example: AutoInstall Operation, page 3-29
- Additional References, page 3-30

Information About the AutoInstall Feature

When you boot up a controller that does not have a configuration, the AutoInstall feature can download a configuration file from a TFTP server and then load the configuration onto the controller automatically.

If you create a configuration file on a controller that is already on the network (or through a WCS filter), place that configuration file on a TFTP server, and configure a DHCP server so that a new controller can get an IP address and TFTP server information, the AutoInstall feature can obtain the configuration file for the new controller automatically.

When the controller boots, the AutoInstall process starts. The controller does not take any action until AutoInstall is notified that the configuration wizard has started. If the wizard has not started, the controller has a valid configuration.

If AutoInstall is notified that the configuration wizard has started (which means that the controller does not have a configuration), AutoInstall waits for an additional 30 seconds. This time period gives you an opportunity to respond to the first prompt from the configuration wizard:

Would you like to terminate autoinstall? [yes]:

Table 3-1 Commands for CLI Navigation and Common Tasks

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>save config</td>
<td>At the root level, save configuration changes from active working RAM (NVRAM) so they are retained after reboot</td>
</tr>
<tr>
<td>reset system</td>
<td>At the root level, reset the controller without logging out</td>
</tr>
</tbody>
</table>

Additional References

- See the *Cisco Wireless LAN Controller Command Reference* for information on specific commands.
- See the “Configuring Telnet and SSH Sessions” section on page 3-35 for information on enabling Telnet sessions.
When the 30-second abort timeout expires, AutoInstall starts the DHCP client. You can abort the AutoInstall task even after this 30-second timeout if you enter Yes at the prompt. However, AutoInstall cannot be aborted if the TFTP task has locked the flash and is in the process of downloading and installing a valid configuration file.

**Guidelines and Limitations**

AutoInstall uses the following interfaces:

- Cisco 5500 Series Controllers
  - eth0—Service port (untagged)
  - dtl0—Gigabit port 1 through the NPU (untagged)

**Obtaining an IP Address Through DHCP and Downloading a Configuration File from a TFTP Server**

AutoInstall attempts to obtain an IP address from the DHCP server until the DHCP process is successful or until you abort the AutoInstall process. The first interface to successfully obtain an IP address from the DHCP server registers with the AutoInstall task. The registration of this interface causes AutoInstall to begin the process of obtaining TFTP server information and downloading the configuration file.

Following the acquisition of the DHCP IP address for an interface, AutoInstall begins a short sequence of events to determine the host name of the controller and the IP address of the TFTP server. Each phase of this sequence gives preference to explicitly configured information over default or implied information and to explicit host names over explicit IP addresses.

The process is as follows:

- If at least one Domain Name System (DNS) server IP address is learned through DHCP, AutoInstall creates a /etc/resolv.conf file. This file includes the domain name and the list of DNS servers that have been received. The Domain Name Server option provides the list of DNS servers, and the Domain Name option provides the domain name.
- If the domain servers are not on the same subnet as the controller, static route entries are installed for each domain server. These static routes point to the gateway that is learned through the DHCP Router option.
- The host name of the controller is determined in this order by one of the following:
  - If the DHCP Host Name option was received, this information (truncated at the first period [.]) is used as the host name for the controller.
  - A reverse DNS lookup is performed on the controller IP address. If DNS returns a hostname, this name (truncated at the first period [.]) is used as the hostname for the controller.
- The IP address of the TFTP server is determined in this order by one of the following:
  - If AutoInstall received the DHCP TFTP Server Name option, AutoInstall performs a DNS lookup on this server name. If the DNS lookup is successful, the returned IP address is used as the IP address of the TFTP server.
  - If the DHCP Server Host Name (sname) text box is valid, AutoInstall performs a DNS lookup on this name. If the DNS lookup is successful, the IP address that is returned is used as the IP address of the TFTP server.
Using the AutoInstall Feature for Controllers Without a Configuration

- If AutoInstall received the DHCP TFTP Server Address option, this address is used as the IP address of the TFTP server.
- AutoInstall performs a DNS lookup on the default TFTP server name (cisco-wlc-tftp). If the DNS lookup is successful, the IP address that is received is used as the IP address of the TFTP server.
- If the DHCP server IP address (siaddr) text box is nonzero, this address is used as the IP address of the TFTP server.
- The limited broadcast address (255.255.255.255) is used as the IP address of the TFTP server.
- If the TFTP server is not on the same subnet as the controller, a static route (/32) is installed for the IP address of the TFTP server. This static route points to the gateway that is learned through the DHCP Router option.

Selecting a Configuration File

After the hostname and TFTP server have been determined, AutoInstall attempts to download a configuration file. AutoInstall performs three full download iterations on each interface that obtains a DHCP IP address. For example, if a Cisco 4400 Series Controller obtains DHCP IP addresses on both eth0 and dtl0, each interface tries to download a configuration. If the interface cannot download a configuration file successfully after three attempts, the interface does not attempt further.

The first configuration file that is downloaded and installed successfully triggers a reboot of the controller. After the reboot, the controller runs the newly downloaded configuration.

AutoInstall searches for configuration files in the order in which the names are listed:

- The filename that is provided by the DHCP Boot File Name option
- The filename that is provided by the DHCP File text box
- host name-config
- host name.cfg
- base MAC address-config (for example, 0011.2233.4455-config)
- serial number-config
- ciscowlc-config
- ciscowlc.cfg

AutoInstall runs through this list until it finds a configuration file. It stops running if it does not find a configuration file after it cycles through this list three times on each registered interface.

---

**Note**

The downloaded configuration file can be a complete configuration, or it can be a minimal configuration that provides enough information for the controller to be managed by WCS. Full configuration can then be deployed directly from WCS.

---

**Note**

The autoinstall does not expect the switch connected to the controller to be configured for either channels. Autoinstall works with service port in lag-configuration.
For information about creating and uploading a configuration file that AutoInstall can obtain from a TFTP server, see Chapter 11, “Managing Controller Software and Configurations.”

WCS release 5.0 and later releases provide AutoInstall capabilities for controllers. A WCS administrator can create a filter that includes the host name, the MAC address, or the serial number of the controller and associate a group of templates (a configuration group) to this filter rule. WCS pushes the initial configuration to the controller when the controller boots up initially. After the controller is discovered, WCS pushes the templates that are defined in the configuration group. For more information about the AutoInstall feature and WCS, see Chapter 15 of the Cisco Wireless Control System Configuration Guide, Release 7.0.172.0.

Example: AutoInstall Operation

The following is an example of an AutoInstall process from start to finish:

Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:
AUTO-INSTALL: starting now...
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Filename ==> 'abcd-confg'
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Server IP ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'service-port' - setting DHCP yiaddr ==> 172.19.29.253
AUTO-INSTALL: interface 'service-port' - setting DHCP Netmask ==> 255.255.255.0
AUTO-INSTALL: interface 'service-port' - setting DHCP Gateway ==> 172.19.29.1
AUTO-INSTALL: interface 'service-port' registered
AUTO-INSTALL: interaction 1 -- interface 'service-port'
AUTO-INSTALL: DNS reverse lookup 172.19.29.253 ==> 'wlc-1'
AUTO-INSTALL: hostname 'wlc-1'
AUTO-INSTALL: TFTP server 1.100.108.2 (from DHCP Option 150)
AUTO-INSTALL: attempting download of 'abcd-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: interface 'management' - setting DHCP file ==> 'bootfile1'
AUTO-INSTALL: interface 'management' - setting DHCP TFTP Filename ==> 'bootfile2-confg'
AUTO-INSTALL: interface 'management' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[1] ==> 1.100.108.3
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[2] ==> 1.100.108.4
AUTO-INSTALL: interface 'management' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'management' - setting DHCP yiaddr ==> 1.100.108.238
AUTO-INSTALL: interface 'management' - setting DHCP Netmask ==> 255.255.255.0
AUTO-INSTALL: interface 'management' - setting DHCP Gateway ==> 1.100.108.1
AUTO-INSTALL: interface 'management' registered
AUTO-INSTALL: TFTP status - 'Config file transfer failed - Error from server: File not found' (3)
AUTO-INSTALL: attempting download of 'wlc-1-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... updating configuration.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... storing in flash.' (2)
AUTO-INSTALL: TFTP status - 'System being reset.' (2)
Resetting system
Managing the Controller System Date and Time

This section contains the following topics:

- Information About Controller System Date and Time, page 3-30
- Guidelines and Limitations, page 3-30
- Configuring an NTP Server to Obtain the Date and Time, page 3-30
- Configuring NTP Authentication, page 3-31
- Configuring the Date and Time, page 3-32

Information About Controller System Date and Time

You can configure the controller system date and time at the time of configuring the controller using the configuration wizard. If you did not configure the system date and time through the configuration wizard or if you want to change your configuration, you can follow the instructions in this section to configure the controller to obtain the date and time from a Network Time Protocol (NTP) server or to configure the date and time manually. Greenwich Mean Time (GMT) is used as the standard for setting the time zone on the controller.

You can also configure an authentication mechanism between various NTP servers.

Guidelines and Limitations

- If you are configuring wIPS, you must set the controller time zone to UTC.
- Cisco Aironet lightweight access points might not connect to the controller if the date and time are not set properly. Set the current date and time on the controller before allowing the access points to connect to it.
- Starting in the 7.0.116.0 release, you can configure an authentication channel between the controller and the NTP server.

Configuring an NTP Server to Obtain the Date and Time

Each NTP server IP address is added to the controller database. Each controller searches for an NTP server and obtains the current time upon reboot and at each user-defined polling interval (daily to weekly).
Use these commands to configure an NTP server to obtain the date and time:
- To specify the NTP server for the controller, enter this command:
  \[
  \text{config time ntp server index ip\_address}
  \]
- To specify the polling interval (in seconds), enter this command:
  \[
  \text{config time ntp interval}
  \]

### Configuring NTP Authentication

This section contains the following topics:
- Configuring NTP Authentication (GUI), page 3-31
- Configuring NTP Authentication (CLI), page 3-31

#### Configuring NTP Authentication (GUI)

1. **Step 1** Choose **Controller > NTP > Servers** to open the NTP Servers page.
2. **Step 2** Click **New** to add an NTP server.
   - The NTP Servers > New page appears
3. **Step 3** Select a server priority from the Server Index (Priority) from the drop-down list.
4. **Step 4** Enter the NTP server IP Address in the Server IP Address text box.
5. **Step 5** Enable NTP server authentication by selecting the **NTP Server Authentication** check box.
6. **Step 6** Click **Apply**.
7. **Step 7** Choose **Controller > NTP > Keys**.
8. **Step 8** Click **New** to create a key.
9. **Step 9** Enter the key index in the Key Index text box.
10. **Step 10** Select the key format from the Key Format drop-down list.
11. **Step 11** Enter the Key in the Key text box.
12. **Step 12** Click **Apply**.

#### Configuring NTP Authentication (CLI)

**Note**
- By default, MD5 is used.
- \[
  \text{config time ntp auth enable server-index key-index}
  \]
- \[
  \text{config time ntp auth disable server-index}
  \]
- \[
  \text{config time ntp key-auth add key-index md5 key-format key}
  \]
- To delete an authentication key, use the following command:
  \[
  \text{config time ntp key-auth delete key-index}
  \]
To view the list of NTP key Indices, use the following command:

```plaintext
show ntp-keys
```

### Configuring the Date and Time

This section contains the following topics:
- **Configuring the Date and Time (GUI), page 3-32**
- **Configuring the Date and Time (CLI), page 3-33**

#### Configuring the Date and Time (GUI)

**Step 1**  
Choose **Commands > Set Time** to open the Set Time page.

#### Figure 3-15  
**Set Time Page**

The current date and time appear at the top of the page.

**Step 2**  
In the Timezone area, choose your local time zone from the Location drop-down list.

**Note**  
When you choose a time zone that uses Daylight Saving Time (DST), the controller automatically sets its system clock to reflect the time change when DST occurs. In the United States, DST starts on the second Sunday in March and ends on the first Sunday in November.

**Note**  
You cannot set the time zone delta on the controller GUI. However, if you do so on the controller CLI, the change is reflected in the Delta Hours and Mins text boxes on the controller GUI.

**Step 3**  
Click **Set Timezone** to apply your changes.

**Step 4**  
In the Date area, choose the current local month and day from the Month and Day drop-down lists, and enter the year in the Year text box.
Step 5  In the Time area, choose the current local hour from the Hour drop-down list, and enter the minutes and seconds in the Minutes and Seconds text boxes.

Note  If you change the time zone location after setting the date and time, the values in the Time area are updated to reflect the time in the new time zone location. For example, if the controller is currently configured for noon Eastern time and you change the time zone to Pacific time, the time automatically changes to 9:00 a.m.

Step 6  Click Set Date and Time to apply your changes.

Step 7  Click Save Configuration to save your changes.

Configuring the Date and Time (CLI)

Step 1  To configure the current local date and time in GMT on the controller, enter this command:

```
config time manual mm/dd/yy hh:mm:ss
```

Note  When setting the time, the current local time is entered in terms of GMT and as a value between 00:00 and 24:00. For example, if it is 8:00 a.m. Pacific time in the United States, you would enter 16:00 because the Pacific time zone is 8 hours behind GMT.

Step 2  Perform one of the following to set the time zone for the controller:

- To set the time zone location in order to have Daylight Saving Time (DST) set automatically when it occurs, enter this command:

```
config time timezone location location_index
```

where `location_index` is a number representing one of the following time zone locations:

1. (GMT-12:00) International Date Line West
2. (GMT-11:00) Samoa
3. (GMT-10:00) Hawaii
4. (GMT-9:00) Alaska
5. (GMT-8:00) Pacific Time (US and Canada)
6. (GMT-7:00) Mountain Time (US and Canada)
7. (GMT-6:00) Central Time (US and Canada)
8. (GMT-5:00) Eastern Time (US and Canada)
9. (GMT-4:00) Atlantic Time (Canada)
10. (GMT-3:00) Buenos Aires (Argentina)
11. (GMT-2:00) Mid-Atlantic
12. (GMT-1:00) Azores
13. (GMT) London, Lisbon, Dublin, Edinburgh (default value)
14. (GMT +1:00) Amsterdam, Berlin, Rome, Vienna
15. (GMT +2:00) Jerusalem
16. (GMT +3:00) Baghdad
17. (GMT +4:00) Muscat, Abu Dhabi
18. (GMT +4:30) Kabul
19. (GMT +5:00) Karachi, Islamabad, Tashkent
20. (GMT +5:30) Colombo, Kolkata, Mumbai, New Delhi
21. (GMT +5:45) Katmandu
22. (GMT +6:00) Almaty, Novosibirsk
23. (GMT +6:30) Rangoon
24. (GMT +7:00) Saigon, Hanoi, Bangkok, Jakarta
25. (GMT +8:00) Hong Kong, Beijing, Chongqing
26. (GMT +9:00) Tokyo, Osaka, Sapporo
27. (GMT +9:30) Darwin
28. (GMT+10:00) Sydney, Melbourne, Canberra
29. (GMT+11:00) Magadan, Solomon Is., New Caledonia
30. (GMT+12:00) Kamchatka, Marshall Is., Fiji
31. (GMT+12:00) Auckland (New Zealand)

Note: If you enter this command, the controller automatically sets its system clock to reflect DST when it occurs. In the United States, DST starts on the second Sunday in March and ends on the first Sunday in November.

• To manually set the time zone so that DST is not set automatically, enter this command:

  \texttt{config timezone delta\_hours delta\_mins}

  where \texttt{delta\_hours} is the local hour difference from GMT, and \texttt{delta\_mins} is the local minute difference from GMT.

  When manually setting the time zone, enter the time difference of the local current time zone with respect to GMT (+/–). For example, Pacific time in the United States is 8 hours behind GMT. Therefore, it is entered as –8.

Note: You can manually set the time zone and prevent DST from being set only on the controller CLI.

Step 3 To save your changes, enter this command:

\texttt{save config}

Step 4 To verify that the controller shows the current local time with respect to the local time zone, enter this command:

\texttt{show time}

Information similar to the following appears:

Time: Thu Apr 7 13:56:37 2011
Timezone delta: 0:0
Timezone location: (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
Configuring Telnet and SSH Sessions

This section contains the following topics:

- Information About Telnet and SSH, page 3-35
- Guidelines and Limitations, page 3-35
- Configuring Telnet and SSH Sessions, page 3-35
- Additional References, page 3-37

Information About Telnet and SSH

Telnet is a network protocol used to provide access to the controller’s CLI. Secure Shell (SSH) is a more secure version of Telnet that uses data encryption and a secure channel for data transfer. You can use the controller GUI or CLI to configure Telnet and SSH sessions.

Guidelines and Limitations

- Only the FIPS approved algorithm aes128-cbc is supported when using SSH to control WLANs.
- The controller does not support raw Telnet mode.

Configuring Telnet and SSH Sessions

This section contains the following topics:

- Configuring Telnet and SSH Sessions (GUI), page 3-35
- Configuring Telnet and SSH Sessions (CLI), page 3-36

Configuring Telnet and SSH Sessions (GUI)

Step 1 Choose Management > Telnet-SSH to open the Telnet-SSH Configuration page.
Configuring Telnet and SSH Sessions

**Step 2**  In the Telnet Login Timeout text box, enter the number of minutes that a Telnet session is allowed to remain inactive before being terminated. The valid range is 0 to 160 minutes (inclusive), and the default value is 5 minutes. A value of 0 indicates no timeout.

**Step 3**  From the Maximum Number of Sessions drop-down list, choose the number of simultaneous Telnet or SSH sessions allowed. The valid range is 0 to 5 sessions (inclusive), and the default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.

**Step 4**  From the Allow New Telnet Sessions drop-down list, choose **Yes** or **No** to allow or disallow new Telnet sessions on the controller. The default value is No.

**Step 5**  From the Allow New SSH Sessions drop-down list, choose **Yes** or **No** to allow or disallow new SSH sessions on the controller. The default value is Yes.

**Step 6**  Click **Apply** to commit your changes.

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

**Step 8**  To see a summary of the Telnet configuration settings, choose **Management > Summary**. The Summary page appears.

This page shows whether additional Telnet and SSH sessions are permitted.

---

**Configuring Telnet and SSH Sessions (CLI)**

**Step 1**  To allow or disallow new Telnet sessions on the controller, enter this command:

```
config network telnet {enable | disable}
```

The default value is disabled.

**Step 2**  To allow or disallow new SSH sessions on the controller, enter this command:

```
config network ssh {enable | disable}
```

The default value is enabled.

**Step 3**  To specify the number of minutes that a Telnet session is allowed to remain inactive before being terminated, enter this command:

```
config sessions timeout timeout
```
where \textit{timeout} is a value between 0 and 160 minutes (inclusive). The default value is 5 minutes. A value of 0 indicates no timeout.

**Step 4**

To specify the number of simultaneous Telnet or SSH sessions allowed, enter this command:

\texttt{config sessions maxsessions session\_num}

where \textit{session\_num} is a value between 0 and 5 (inclusive). The default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.

**Step 5**

To save your changes, enter this command:

\texttt{save config}

**Step 6**

To see the Telnet and SSH configuration settings, enter this command:

\texttt{show network summary}

Information similar to the following appears:

\begin{verbatim}
RF-Network Name............................. TestNetwork1
Web Mode..................................... Enable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High....... Disable
Secure Web Mode Cipher-Option SSLv2...... Enable
Secure Shell (ssh).......................... Enable
Telnet..................................... Disable
...
\end{verbatim}

**Step 7**

To see the Telnet session configuration settings, enter this command:

\texttt{show sessions}

Information similar to the following appears:

\begin{verbatim}
CLI Login Timeout (minutes)............ 5
Maximum Number of CLI Sessions...... 5
\end{verbatim}

**Step 8**

To see all active Telnet sessions, enter this command:

\texttt{show loginsession}

Information similar to the following appears:

<table>
<thead>
<tr>
<th>ID</th>
<th>User Name</th>
<th>Connection From</th>
<th>Idle Time</th>
<th>Session Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>admin</td>
<td>EIA-232</td>
<td>00:00:00</td>
<td>00:19:04</td>
</tr>
</tbody>
</table>

**Step 9**

If you ever want to close all active Telnet sessions or a specific Telnet session, enter this command:

\texttt{config loginsession close \{all | session\_id\}}

---

**Additional References**

See the “Troubleshooting” section on page 18-1 for instructions on using Telnet or SSH to troubleshoot lightweight access points.

**Managing the Controller Wirelessly**

This section contains the following topics:
Managing the Controller Wirelessly

You can monitor and configure controllers using a wireless client. This feature is supported for all management tasks except uploads from and downloads to the controller.

Before you can open the GUI or the CLI from a wireless client device, you must configure the controller to allow the connection.

Enabling Wireless Connections

This section contains the following topics:

- Enabling Wireless Connections (GUI), page 3-38
- Enabling Wireless Connections (CLI), page 3-38

Enabling Wireless Connections (GUI)

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log on to the controller GUI.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose Management &gt; Mgmt Via Wireless page.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enable the Enable Controller Management to be accessible from Wireless Clients checkbox.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Apply.</td>
</tr>
</tbody>
</table>

Enabling Wireless Connections (CLI)

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log on to the controller CLI.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter the config network mgmt-via-wireless enable command.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Use a wireless client to associate to a lightweight access point connected to the controller.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the wireless client, open a Telnet session to the controller, or browse to the controller GUI.</td>
</tr>
</tbody>
</table>
Configuring Ports and Interfaces

This chapter contains these sections:

- Information About Ports, page 4-1
- Information About Interfaces, page 4-3
- Configuring the Management Interface, page 4-4
- Configuring the AP-Manager Interface, page 4-8
- Configuring Virtual Interfaces, page 4-11
- Configuring Service-Port Interfaces, page 4-13
- Configuring Dynamic Interfaces, page 4-15
- Information About Dynamic AP Management, page 4-20
- Information About WLANs, page 4-20
- Configuring Ports, page 4-22
- Using the Cisco 5500 Series Controller USB Console Port, page 4-24
- Choosing Between Link Aggregation and Multiple AP-Manager Interfaces, page 4-26
- Configuring Link Aggregation, page 4-26
- Configuring Multiple AP-Manager Interfaces, page 4-32
- Configuration Example: Configuring AP-Manager on a Cisco 5500 Series Controller, page 4-37
- Configuring VLAN Select, page 4-39
- Configuring Interface Groups, page 4-40
- Multicast Optimization, page 4-42

Information About Ports

A port is a physical entity that is used for connections on the controller platform. Controllers have two types of ports: distribution system ports and a service port. Figure 4-1 shows the ports available on a 5500 series controller as an example.
Chapter 4  Configuring Ports and Interfaces

Information About Ports

This section contains the following topics:

- Information About Distribution System Ports, page 4-2
- Information About Service Ports, page 4-3
- Additional References, page 4-4

Information About Distribution System Ports

A distribution system port connects the controller to a neighbor switch and serves as the data path between these two devices.

Guidelines and Limitations

- Cisco 5508 Controllers have eight Gigabit Ethernet distribution system ports, through which the Controller can manage multiple access points. The 5508-12, 5508-25, 5508-50, 5508-100, and 5508-250 models allow a total of 12, 25, 50, 100, or 250 access points to join the controller. Cisco 5508 controllers have no restrictions on the number of access points per port. However, we recommend using link aggregation (LAG) or configuring dynamic AP-manager interfaces on each Gigabit Ethernet port to automatically balance the load. If more than 100 access points are connected to the Cisco 5500 Series Controller, make sure that more than one Gigabit Ethernet interface is connected to the upstream switch.
Information About Interfaces

Note

The Gigabit Ethernet ports on the Cisco 5508 Controllers accept these SX/LC/T small form-factor plug-in (SFP) modules:
- 1000BASE-SX SFP modules, which provide a 1000-Mbps wired connection to a network through an 850nM (SX) fiber-optic link using an LC physical connector
- 1000BASE-LX SFP modules, which provide a 1000-Mbps wired connection to a network through a 1300nM (LX/LH) fiber-optic link using an LC physical connector
- 1000BASE-T SFP modules, which provide a 1000-Mbps wired connection to a network through a copper link using an RJ-45 physical connector

Each distribution system port is, by default, an 802.1Q VLAN trunk port. The VLAN trunking characteristics of the port are not configurable.

Information About Service Ports

Cisco 5500 Series Controllers also have a 10/100/1000 copper Ethernet service port. The service port is controlled by the service-port interface and is reserved for out-of-band management of the controller and system recovery and maintenance in the event of a network failure. It is also the only port that is active when the controller is in boot mode. The service port is not capable of carrying 802.1Q tags, so it must be connected to an access port on the neighbor switch. Use of the service port is optional.

Guidelines and Limitations

- The Cisco WiSM2 uses the service port for internal protocol communication between the controllers and the Supervisor 720.
- The service port is not autosensing. You must use the correct straight-through or crossover Ethernet cable to communicate with the service port.
- Do not configure wired clients in the same VLAN or subnet of the service port of the controller on the network. If you configure wired clients on the same subnet or VLAN as the service port, it is not possible to access the management interface of the controller.

Information About Interfaces

An interface is a logical entity on the controller. An interface has multiple parameters associated with it, including an IP address, default gateway (for the IP subnet), primary physical port, secondary physical port, VLAN identifier, and DHCP server.

These five types of interfaces are available on the controller. Four of these are static and are configured at setup time:

- Management interface (static and configured at setup time; mandatory)
- AP-manager interface (static and configured at setup time; mandatory)

Note

You are not required to configure an AP-manager interface on Cisco 5500 Series Controllers.

- Virtual interface (static and configured at setup time; mandatory)
• Service-port interface (static and configured at setup time; optional)
• Dynamic interface (user-defined)

Each interface is mapped to at least one primary port, and some interfaces (management and dynamic) can be mapped to an optional secondary (or backup) port. If the primary port for an interface fails, the interface automatically moves to the backup port. In addition, multiple interfaces can be mapped to a single controller port.

Guidelines and Limitations

Note
For Cisco 5500 Series Controllers in a non-link-aggregation (non-LAG) configuration, the management interface must be on a different VLAN than any dynamic AP-manager interface. Otherwise, the management interface cannot fail over to the port that the AP-manager is on.

Note
Cisco 5500 Series Controllers do not support fragmented pings on any interface.

Additional References

See the “Configuring Link Aggregation” section on page 4-26 if you want to configure the controller to dynamically map the interfaces to a single port channel rather than having to configure primary and secondary ports for each interface.

Configuring the Management Interface

This section contains the following topics:
• Information About the Management Interface, page 4-4
• Guidelines and Limitations, page 4-5
• Configuring the Management Interface (GUI), page 4-5
• Configuring the Management Interface (CLI), page 4-7

Information About the Management Interface

The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers. It is also used for communications between the controller and access points. The management interface has the only consistently “pingable” in-band interface IP address on the controller. You can access the controller’s GUI by entering the controller’s management interface IP address in Internet Explorer’s or Mozilla Firefox’s address field.

For CAPWAP, the controller requires one management interface to control all inter-controller communications and one AP-manager interface to control all controller-to-access point communications, regardless of the number of ports.
Guidelines and Limitations

- For CAPWAP, the controller requires one management interface to control all inter-controller communications and one AP-manager interface to control all controller-to-access point communications, regardless of the number of ports.
- If the service port is in use, the management interface must be on a different supernet from the service-port interface.
- Do not map a guest WLAN to the management interface. If the EoIP tunnel breaks, the client could obtain an IP and be placed on the management subnet.
- Do not configure wired clients in the same VLAN or subnet of the service port of the controller on the network. If you configure wired clients on the same subnet or VLAN as the service port, it is not possible to access the management interface of the controller.
- Typically, you define the management, AP-manager, virtual, and service-port interface parameters using the Startup Wizard. However, you can display and configure interface parameters through either the GUI or CLI after the controller is running.

Configuring the Management Interface

This section contains the following topics:
- Configuring the Management Interface (GUI), page 4-5
- Configuring the Management Interface (CLI), page 4-7

Configuring the Management Interface (GUI)

**Step 1** Choose Controller > Interfaces to open the Interfaces page.

**Step 2** Click management link. The Interfaces > Edit page appears.

**Step 3** Set the management interface parameters:

- Quarantine and quarantine VLAN ID, if applicable

Note: The management interface uses the controller’s factory-set distribution system MAC address.
Chapter 4  Configuring Ports and Interfaces

Note Select the Quarantine check box if you want to configure this VLAN as unhealthy or you want to configure network access control (NAC) out-of-band integration. Doing so causes the data traffic of any client that is assigned to this VLAN to pass through the controller. See Chapter 8, “Working with WLANs,” for more information about NAC out-of-band integration.

- NAT address (only Cisco 2500 Series Controllers and Cisco 5500 Series Controllers are configured for dynamic AP management)

Note Select the Enable NAT Address check box and enter the external NAT IP address if you want to be able to deploy your Cisco 2500 Series Controllers or Cisco 5500 Series Controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller’s intranet IP addresses to a corresponding external address. The controller’s dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

Note The NAT parameters are supported for use only with one-to-one-mapping NAT, where each private client has a direct and fixed mapping to a global address. The NAT parameters do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

Note If a Cisco 2500 Series Controllers or Cisco 5500 Series Controller is configured with an external NAT IP address under the management interface, the APs in local mode cannot associate with the controller. The workaround is to either ensure that the management interface has a globally valid IP address or ensure that external NAT IP address is valid internally for the local APs.

- VLAN identifier

Note Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the management interface.

- Fixed IP address, IP netmask, and default gateway
- Dynamic AP management (for Cisco 5500 Series Controllers only)

Note For Cisco 2500 Series Controllers or Cisco 5500 Series Controllers, the management interface acts like an AP-manager interface by default. If desired, you can disable the management interface as an AP-manager interface and create another dynamic interface as an AP manager.

- Physical port assignment (for all controllers except the Cisco 5500 Series Controller)
- Primary and secondary DHCP servers
• Access control list (ACL) setting, if required

**Note** To create ACLs, follow the instructions in Chapter 7, “Configuring Security Solutions.”

---

**Step 4** Click **Save Configuration** to save your changes.

**Step 5** If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.

---

**Configuring the Management Interface (CLI)**

**Step 1** Enter the **show interface detailed management** command to view the current management interface settings.

**Note** The management interface uses the controller’s factory-set distribution system MAC address.

**Step 2** Enter the **config wlan disable wlan-number** command to disable each WLAN that uses the management interface for distribution system communication.

**Step 3** Enter these commands to define the management interface:

- **config interface address management** *ip-addr* *ip-netmask* *gateway*
- **config interface quarantine vlan management** *vlan_id*

**Note** Use the **config interface quarantine vlan management** *vlan_id* command to configure a quarantine VLAN on the management interface.

- **config interface port management** *physical-ds-port-number* (for all controllers except the 5500 series)
- **config interface dhcp management** *ip-address-of-primary-dhcp-server* [*ip-address-of-secondary-dhcp-server*]
Step 4  Enter these commands if you want to be able to deploy your Cisco 5500 Series Controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT):

- `config interface nat-address management {enable | disable}`
- `config interface nat-address management set public_IP_address`

NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller’s intranet IP addresses to a corresponding external address. The controller’s dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

**(Note)** These NAT commands can be used only on Cisco 5500 Series Controllers and only if the management interface is configured for dynamic AP management.

**(Note)** These commands are supported for use only with one-to-one-mapping NAT, where each private client has a direct and fixed mapping to a global address. These commands do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

Step 5  Enter the `save config` command to save your changes.

Step 6  Enter the `show interface detailed management` command to verify that your changes have been saved.

Step 7  If you made any changes to the management interface, enter the `reset system` command to reboot the controller in order for the changes to take effect.
Guidelines and Limitations

- The Controller does not support transmitting the jumbo frames. To avoid having the controller transmit CAPWAP packets to the AP that will necessitate fragmentation and reassembly, reduce MTU/MSS on the client side.

- The AP-manager interface communicates through any distribution system port by listening across the Layer 3 network for access point CAPWAP or LWAPP join messages to associate and communicate with as many lightweight access points as possible.

- For Cisco 5500 Series Controllers, you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default, and the access points can join on this interface.

- With the 7.0.116.0 release onwards, the MAC address of the management interface and the AP-manager interface is the same as the base LAG MAC address.

- If only one distribution system port can be used, you should use distribution system port 1.

- If link aggregation (LAG) is enabled, there can be only one AP-manager interface. But when LAG is disabled, one or more AP-manager interfaces can be created, generally one per physical port.

- Port redundancy for the AP-manager interface is not supported. You cannot map the AP-manager interface to a backup port.

- Typically, you define the management, AP-manager, virtual, and service-port interface parameters using the Startup Wizard. However, you can display and configure interface parameters through either the GUI or CLI after the controller is running.

Configuring the AP-Manager Interface

This section contains the following topics:

- Configuring the AP-Manager Interface (GUI), page 4-9
- Configuring the AP-Manager Interface (CLI), page 4-10

Configuring the AP-Manager Interface (GUI)

**Step 1** Choose Controller > Interfaces to open the Interfaces page.

**Figure 4-3 Interfaces Page**

This page shows the current controller interface settings.

**Step 2** Click AP-Manager Interface. The Interface > Edit page appears.

**Step 3** Set the AP-Manager Interface parameters:
Chapter 4      Configuring Ports and Interfaces

Configuring the AP-Manager Interface

- Physical port assignment
- VLAN identifier

**Note** Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the AP-manager interface.

- Fixed IP address, IP netmask, and default gateway

**Note** The AP-manager interface’s IP address must be different from the management interface’s IP address and may or may not be on the same subnet as the management interface. However, we recommend that both interfaces be on the same subnet for optimum access point association.

- Primary and secondary DHCP servers
- Access control list (ACL) name, if required

**Note** To create ACLs, follow the instructions in Chapter 7, “Configuring Security Solutions.”

**Step 4** Click **Save Configuration** to save your changes.

**Step 5** If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.

Configuring the AP-Manager Interface (CLI)

**Step 1** Enter the **show interface summary** command to view the current interfaces.

**Note** If the system is operating in Layer 2 mode, the AP-manager interface is not listed.

**Step 2** Enter the **show interface detailed ap-manager** command to view the current AP-manager interface settings.

**Step 3** Enter the **config wlan disable wlan-number** command to disable each WLAN that uses the AP-manager interface for distribution system communication.

**Step 4** Enter these commands to define the AP-manager interface:

- **config interface address ap-manager** ip-addr ip-netmask gateway
- **config interface vlan ap-manager** {vlan-id | 0}

**Note** Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the AP-manager interface.

- **config interface port ap-manager** physical-ds-port-number
Configuring Virtual Interfaces

This section contains the following topics:

- Information About Virtual Interfaces, page 4-11
- Guidelines and Limitations, page 4-11
- Configuring Virtual Interfaces, page 4-12

Information About Virtual Interfaces

A virtual interface is used to support mobility management, Dynamic Host Configuration Protocol (DHCP) relay, and embedded Layer 3 security such as guest web authentication and VPN termination. It also maintains the DNS gateway host name used by Layer 3 security and mobility managers to verify the source of certificates when Layer 3 web authorization is enabled.

Specifically, a virtual interface plays these two primary roles:

- Acts as the DHCP server placeholder for wireless clients that obtain their IP address from a DHCP server.
- Serves as the redirect address for the web authentication login page.

Guidelines and Limitations

- A virtual interface IP address is used only in communications between the controller and wireless clients. It never appears as the source or destination address of a packet that goes out a distribution system port and onto the switched network. For the system to operate correctly, a virtual interface
IP address must be set (it cannot be 0.0.0.0), and no other device on the network can have the same address as the virtual interface. A virtual interface must be configured with an unassigned and unused gateway IP address. A virtual interface IP address is not pingable and should not exist in any routing table in your network. In addition, a virtual interface cannot be mapped to a backup port.

- All controllers within a mobility group must be configured with the same virtual interface IP address. Otherwise, inter-controller roaming may appear to work, but the handoff does not complete, and the client loses connectivity for a period of time.

**Configuring Virtual Interfaces**

This section contains the following topics:

- Configuring Virtual Interfaces (GUI), page 4-12
- Configuring Virtual Interfaces (CLI), page 4-13

**Configuring Virtual Interfaces (GUI)**

**Step 1** Choose **Controller** > **Interfaces** to open the Interfaces page.

**Figure 4-4 Interfaces Page**

This page shows the current controller interface settings.

**Step 2** Click Virtual. The Interfaces > Edit page appears.

**Step 3** Enter the following parameters:

- Any fictitious, unassigned, and unused gateway IP address
- DNS gateway hostname

**Note**

To ensure connectivity and web authentication, the DNS server should always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then the same DNS host name must be configured on the DNS server(s) used by the client.

**Step 4** Click **Save Configuration** to save your changes.

**Step 5** If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.
Configuring Virtual Interfaces (CLI)

**Step 1** Enter the `show interface detailed virtual` command to view the current virtual interface settings.

**Step 2** Enter the `config wlan disable wlan-number` command to disable each WLAN that uses the virtual interface for distribution system communication.

**Step 3** Enter these commands to define the virtual interface:

- `config interface address virtual ip-address`

  **Note** For `ip-address`, enter any fictitious, unassigned, and unused gateway IP address.

- `config interface hostname virtual dns-host-name`

**Step 4** Enter the `reset system` command. At the confirmation prompt, enter Y to save your configuration changes to NVRAM. The controller reboots.

**Step 5** Enter the `show interface detailed virtual` command to verify that your changes have been saved.

Configuring Service-Port Interfaces

This section contains the following topics:

- Information About Service-Port Interfaces, page 4-13
- Guidelines and Limitations, page 4-13
- Configuring Service-Port Interfaces, page 4-13

Information About Service-Port Interfaces

A service-port interface controls communications through and is statically mapped by the system to the service port. The service port can obtain an IP address using DHCP, or it can be assigned a static IP address, but a default gateway cannot be assigned to the service-port interface. Static routes can be defined through the controller for remote network access to the service port.

Guidelines and Limitations

- Only Cisco 5500 Series Controller and Cisco 7500 Series Controller have service-port interfaces.
- You must configure an IP address on the service-port interface of both Cisco WiSM controllers. Otherwise, the neighbor switch is unable to check the status of each controller.

Configuring Service-Port Interfaces

This section contains the following topics:

- Configuring Service-Port Interfaces (GUI), page 4-14
Configuring Service-Port Interfaces (GUI)

Step 1 Choose Controller > Interfaces to open the Interfaces page.

Figure 4-5 Interfaces Page

This page shows the current controller interface settings.

Step 2 Click the service-port link to open the Interfaces > Edit page.

Step 3 Enter the Service-Port Interface parameters:

Note The service-port interface uses the factory-set service-port MAC address of the controller.

- DHCP protocol (enabled)
- DHCP protocol (disabled) and IP address and IP netmask

Step 4 Click Save Configuration to save your changes.

Step 5 If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.

Configuring Service-Port Interfaces (CLI)

Step 1 Enter the `show interface detailed service-port` command to view the current service-port interface settings.

Note The service-port interface uses the controller’s factory-set service-port MAC address.

Step 2 Enter these commands to define the service-port interface:

- To configure the DHCP server: `config interface dhcp service-port ip-address-of-primary-dhcp-server [ip-address-of-secondary-dhcp-server]`
- To disable the DHCP server: `config interface dhcp service-port none`
- To configure the IP address: `config interface address service-port ip-addr ip-netmask`
Chapter 4 Configuring Ports and Interfaces

Configuring Dynamic Interfaces

This section contains the following topics:

- Information About Dynamic Interfaces, page 4-15
- Guidelines and Limitations, page 4-15
- Configuring Dynamic Interfaces, page 4-16

Information About Dynamic Interfaces

Dynamic interfaces, also known as VLAN interfaces, are created by users and designed to be analogous to VLANs for wireless LAN clients. A controller can support up to 512 dynamic interfaces (VLANs). Each dynamic interface is individually configured and allows separate communication streams to exist on any or all of a controller’s distribution system ports. Each dynamic interface controls VLANs and other communications between controllers and all other network devices, and each acts as a DHCP relay for wireless clients associated to WLANs mapped to the interface. You can assign dynamic interfaces to distribution system ports, WLANs, the Layer 2 management interface, and the Layer 3 AP-manager interface, and you can map the dynamic interface to a backup port.

You can configure zero, one, or multiple dynamic interfaces on a distribution system port. However, all dynamic interfaces must be on a different VLAN or IP subnet from all other interfaces configured on the port. If the port is untagged, all dynamic interfaces must be on a different IP subnet from any other interface configured on the port.

Guidelines and Limitations

- If you are using DHCP proxy and/or a RADIUS source interface, ensure that the dynamic interface has a valid routable address. Duplicate or overlapping addresses across controller interfaces are not supported.
- We recommend using tagged VLANs for dynamic interfaces.
- You must not configure a dynamic interface in the same sub-network as a server that should be reachable by the controller CPU, like a RADIUS server, as it might cause asymmetric routing issues.
- For SNMP requests that come from a subnet that is configured as a dynamic interface, the controller responds but the response does not reach the device that initiated the conversation.
- Wired clients cannot access management interface of the Cisco WLC 2500 series using the IP address of the AP Manager interface – when dynamic AP management is enabled on dynamic VLAN.
Configuring Dynamic Interfaces

This section contains the following topics:

- Configuring Dynamic Interfaces (GUI), page 4-16
- Configuring Dynamic Interfaces (CLI), page 4-18

Configuring Dynamic Interfaces (GUI)

Step 1  Choose Controller > Interfaces to open the Interfaces page.

Step 2  Perform one of the following:

- To create a new dynamic interface, click New. The Interfaces > New page appears. Go to Step 3.
- To modify the settings of an existing dynamic interface, click the name of the interface. The Interfaces > Edit page for that interface appears. Go to Step 5.
- To delete an existing dynamic interface, hover your cursor over the blue drop-down arrow for the desired interface and choose Remove.

Step 3  Enter an interface name and a VLAN identifier, as shown in Figure 4-6.

Step 4  Click Apply to commit your changes. The Interfaces > Edit page appears.

Step 5  Configure the following parameters:

- Guest LAN, if applicable
- Quarantine and quarantine VLAN ID, if applicable

Note  Select the Quarantine check box if you want to configure this VLAN as unhealthy or you want to configure network access control (NAC) out-of-band integration. Doing so causes the data traffic of any client that is assigned to this VLAN to pass through the controller. See Chapter 8, “Working with WLANs,” for more information about NAC out-of-band integration.

- Physical port assignment (for all controllers except the 5500 series)
- NAT address (only for Cisco 5500 Series Controllers configured for dynamic AP management)
Select the **Enable NAT Address** check box and enter the external NAT IP address if you want to be able to deploy your Cisco 5500 Series Controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller’s intranet IP addresses to a corresponding external address. The controller’s dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

The NAT parameters are supported for use only with one-to-one-mapping NAT, where each private client has a direct and fixed mapping to a global address. The NAT parameters do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

**Dynamic AP management**

When you enable this feature, this dynamic interface is configured as an AP-manager interface (only one AP-manager interface is allowed per physical port). A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

Set the APs in a VLAN that is different than the dynamic interface configured on the controller. If the APs are in the same VLAN as the dynamic interface, the APs are not registered on the controller and the “LWAPP discovery rejected” and “Layer 3 discovery request not received on management VLAN” errors are logged on the controller.

- **VLAN identifier**
- **Fixed IP address, IP netmask, and default gateway**
- **Primary and secondary DHCP servers**
- **Access control list (ACL) name, if required**

See Chapter 7, “Configuring Security Solutions,” for more information on ACLs.

To ensure proper operation, you must set the Port Number and Primary DHCP Server parameters.

**Step 6** Click **Save Configuration** to save your changes.

**Step 7** Repeat this procedure for each dynamic interface that you want to create or edit.
**Configuring Dynamic Interfaces**

**Note**  
When you apply a flow policer or an aggregate policer at the ingress of a Dynamic Interface VLAN for the Upstream (wireless to wired) traffic, it is not possible to police because the VLAN based policy has no effect and no policing occurs. When the traffic comes out of the WiSM LAG (L2) and hits the Switch Virtual Interface (SVI) (L3), the QoS policy applied is a VLAN-based policy that has no effect on the policing.

To enable an ingress L3 VLAN-based policy on the SVI, you must enable a VLAN-based QoS equivalent to the `mls qos-vlan-based` command on the WiSM LAG. All the previous 12.2(33)SX releases, which support Auto LAG for WiSM only, such as 12.2(33)SX1, 12.2(33)SX11, 12.2(33)SX12a, 12.2(33)SX13, and so on, do not have this WiSM CLI. Therefore, the VLAN-based QoS policy applied at the ingress of the SVI for wireless to wired traffic never polices any traffic coming out of the WiSM LAG that hits the SVI. The commands that are equivalent to the `mls qos-vlan-based` command are as follows:

**Standalone:**  
`tacacs module module_no controller controller_no qos-vlan-based`

**Virtual Switching System:**  
`wism switch switch_no module module_no controller controller_no qos-vlan-based`

### Configuring Dynamic Interfaces (CLI)

**Step 1**  
Enter the `show interface summary` command to view the current dynamic interfaces.

**Step 2**  
View the details of a specific dynamic interface by entering this command:

```plaintext
show interface detailed operator_defined_interface_name.
```

**Note**  
Interface names that contain spaces must be enclosed in double quotes. For example:  
`config interface create "vlan 25".`

**Step 3**  
Enter the `config wlan disable wlan_id` command to disable each WLAN that uses the dynamic interface for distribution system communication.

**Step 4**  
Enter these commands to configure dynamic interfaces:

- `config interface create operator_defined_interface_name {vlan_id | x}`
- `config interface address operator_defined_interface_name ip_addr ip_netmask [gateway]`
- `config interface vlan operator_defined_interface_name {vlan_id | 0}`
- `config interface port operator_defined_interface_name physical_ds_port_number`
- `config interface ap-manager operator_defined_interface_name {enable | disable}`

**Note**  
Use the `config interface ap-manager operator_defined_interface_name {enable | disable}` command to enable or disable dynamic AP management. When you enable this feature, this dynamic interface is configured as an AP-manager interface (only one AP-manager interface is allowed per physical port). A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

- `config interface dhcp operator_defined_interface_name ip_address_of_primary_dhcp_server [ip_address_of_secondary_dhcp_server]`
Chapter 4 Configuring Ports and Interfaces

Configuring Dynamic Interfaces

- `config interface quarantine vlan interface_name vlan_id`

  **Note**  Use the `config interface quarantine vlan interface_name vlan_id` command to configure a quarantine VLAN on any interface.

- `config interface acl operator_defined_interface_name access_control_list_name`

  **Note**  See Chapter 7, “Configuring Security Solutions,” for more information on ACLs.

**Step 5** Enter these commands if you want to be able to deploy your Cisco 5500 Series Controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT):

- `config interface nat-address dynamic-interface operator_defined_interface_name { enable | disable }

- `config interface nat-address dynamic-interface operator_defined_interface_name set public_IP_address`

NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller’s intranet IP addresses to a corresponding external address. The controller’s dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

  **Note**  These NAT commands can be used only on Cisco 5500 Series Controllers and only if the dynamic interface is configured for dynamic AP management.

  **Note**  These commands are supported for use only with one-to-one-mapping NAT, whereby each private client has a direct and fixed mapping to a global address. These commands do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

**Step 6** Enter the `config wlan enable wlan_id` command to reenable each WLAN that uses the dynamic interface for distribution system communication.

**Step 7** Enter the `save config` command to save your changes.

**Step 8** Enter the `show interface detailed operator_defined_interface_name` command and `show interface summary` command to verify that your changes have been saved.

  **Note**  If desired, you can enter the `config interface delete operator_defined_interface_name` command to delete a dynamic interface.
Information About Dynamic AP Management

A dynamic interface is created as a WLAN interface by default. However, any dynamic interface can be configured as an AP-manager interface, with one AP-manager interface allowed per physical port. A dynamic interface with the Dynamic AP Management option enabled is used as the tunnel source for packets from the controller to the access point and as the destination for CAPWAP packets from the access point to the controller. The dynamic interfaces for AP management must have a unique IP address and are usually configured on the same subnet as the management interface.

Note

If link aggregation (LAG) is enabled, there can be only one AP-manager interface.

We recommend having a separate dynamic AP-manager interface per controller port. See the “Configuring Multiple AP-Manager Interfaces” section on page 4-32 for instructions on configuring multiple dynamic AP-manager interfaces.

Information About WLANs

A WLAN associates a service set identifier (SSID) to an interface. It is configured with security, quality of service (QoS), radio policies, and other wireless network parameters. Up to 512 access point WLANs can be configured per controller.

Figure 4-7 shows the relationship between ports, interfaces, and WLANs.
As shown in Figure 4-7, each controller port connection is an 802.1Q trunk and should be configured as such on the neighbor switch. On Cisco switches, the native VLAN of an 802.1Q trunk is an untagged VLAN. If you configure an interface to use the native VLAN on a neighboring Cisco switch, make sure you configure the interface on the controller to be untagged.

**Note**

A zero value for the VLAN identifier (on the Controller > Interfaces page) means that the interface is untagged.

The default (untagged) native VLAN on Cisco switches is VLAN 1. When controller interfaces are configured as tagged (meaning that the VLAN identifier is set to a nonzero value), the VLAN must be allowed on the 802.1Q trunk configuration on the neighbor switch and not be the native untagged VLAN.

We recommend that tagged VLANs be used on the controller. You should also allow only relevant VLANs on the neighbor switch’s 802.1Q trunk connections to controller ports. All other VLANs should be disallowed or pruned in the switch port trunk configuration. This practice is extremely important for optimal performance of the controller.
Note: We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers properly route VLAN traffic.

Configuring Ports

This section contains the following topics:

- Information About Configuring Ports, page 4-22
- Configuring Ports (GUI), page 4-22

Information About Configuring Ports

The ports of the controller are preconfigured with factory-default settings designed to make the ports of the controller operational without additional configuration. However, you can view the status of the ports of the controller and edit their configuration parameters at any time.

Configuring Ports (GUI)

Step 1

Choose Controller > Ports to open the Ports page.

Figure 4-8 Ports Page

This page shows the current configuration for each of the controller’s ports.

If you want to change the settings of any port, click the number for that specific port. The Port > Configure page appears.

Note: If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.
Note  The number of parameters available on the Port > Configure page depends on your controller type.

The following show the current status of the port:

- Port Number—Number of the current port.
- Admin Status—Current state of the port. Values: Enable or Disable
- Physical Mode—Configuration of the port physical interface. The mode varies by the controller type. Values: Auto, 100 Mbps Full Duplex, 100 Mbps Half Duplex, 10 Mbps Full Duplex, or 10 Mbps Half Duplex

Note  In Cisco Wireless LAN Controller Module (NM-AIR-WLC6-K9), Cisco 5500 Series Controller, and Cisco Flex 7500 Series Controllers, the physical mode is always set to auto.

- Physical Status—The data rate being used by the port. The available data rates vary based on controller type. The following options are available:
  - 5500 series—1000 Mbps full duplex
  - WiSM—1000 Mbps full duplex
  - Controller network module—100 Mbps full duplex
  - Catalyst 3750G Integrated Wireless LAN Controller Switch—1000 Mbps full duplex
- Link Status—Port's link status. Values: Link Up or Link Down
- Link Trap—Whether the port is set to send a trap when the link status changes. Values: Enable or Disable
- Power over Ethernet (PoE)—If the connecting device is equipped to receive power through the Ethernet cable and if so, provides −48 VDC. Values: Enable or Disable

Note  Some older Cisco access points do not draw PoE even if it is enabled on the controller port. In such cases, contact the Cisco Technical Assistance Center (TAC).

Note  The controller in the Catalyst 3750G Integrated Wireless LAN Controller Switch supports PoE on all ports.

Step 2  The following is a list of the port’s configurable parameters.

- Admin Status—Enables or disables the flow of traffic through the port. Options: Enable or Disable. Default: Enable.

Note  Administratively disabling the port on a controller does not affect the port’s link status. The link can be brought down only by other Cisco devices. On other Cisco products, however, administratively disabling a port brings the link down.
Chapter 4  Configuring Ports and Interfaces

Using the Cisco 5500 Series Controller USB Console Port

The USB console port on the Cisco 5500 Series Controllers connects directly to the USB connector of a PC using a USB Type A-to-5-pin mini Type B cable.

Note  The 4-pin mini Type B connector is easily confused with the 5-pin mini Type B connector. They are not compatible. Only the 5-pin mini Type B connector can be used.

For operation with Microsoft Windows, the Cisco Windows USB console driver must be installed on any PC connected to the console port. With this driver, you can plug and unplug the USB cable into and from the console port without affecting Windows HyperTerminal operations.

Step 3  Click Apply to commit your changes.
Step 4  Click Save Configuration to save your changes.
Step 5  Click Back to return to the Ports page and review your changes.
Step 6  Repeat this procedure for each additional port that you want to configure.
Only one console port can be active at a time. When a cable is plugged into the USB console port, the RJ-45 port becomes inactive. Conversely, when the USB cable is removed from the USB port, the RJ-45 port becomes active.

**USB Console OS Compatibility**

These operating systems are compatible with the USB console:

- Microsoft Windows 2000, XP, Vista (Cisco Windows USB console driver required)
- Apple Mac OS X 10.5.2 (no driver required)
- Linux (no driver required)

### Installing the Cisco Windows USB Console Driver

**Step 1**

Download the USB_Console.inf driver file as follows:

a. Click this URL to go to the Software Center:
   

b. Click **Wireless LAN Controllers**.

c. Click **Standalone Controllers**.

d. Click **Cisco 5500 Series Wireless LAN Controllers**.

e. Click **Cisco 5508 Wireless LAN Controller**.

f. Choose the USB driver file.

g. Save the file to your hard drive.

**Step 2**

Connect the Type A connector to a USB port on your PC.

**Step 3**

Connect the mini Type B connector to the USB console port on the controller.

**Step 4**

When prompted for a driver, browse to the USB_Console.inf file on your PC. Follow the prompts to install the USB driver.

---

Some systems might also require an additional system file. You can download the Usbser.sys file from this URL:

http://support.microsoft.com/kb/918365

---

### Changing the Cisco USB Systems Management Console COM Port to an Unused Port

The USB driver is mapped to COM port 6. Some terminal emulation programs do not recognize a port higher than COM 4. If necessary, change the Cisco USB systems management console COM port to an unused port of COM 4 or lower.
Choosing Between Link Aggregation and Multiple AP-Manager Interfaces

Cisco 5500 Series Controllers have no restrictions on the number of access points per port, but we recommend using link aggregation (LAG) or multiple AP-manager interfaces on each Gigabit Ethernet port to automatically balance the load.

The following factors should help you decide which method to use if your controller is set for Layer 3 operation:

• With LAG, all of the controller ports need to connect to the same neighbor switch. If the neighbor switch goes down, the controller loses connectivity.

• With multiple AP-manager interfaces, you can connect your ports to different neighbor devices. If one of the neighbor switches goes down, the controller still has connectivity. However, using multiple AP-manager interfaces presents certain challenges (as discussed in the “Configuring Multiple AP-Manager Interfaces” section) when port redundancy is a concern.

Follow the instructions on the page indicated for the method you want to use:

• Configuring Link Aggregation, page 4-26
• Configuring Multiple AP-Manager Interfaces, page 4-32

Configuring Link Aggregation

This section contains the following topics:

• Information About Link Aggregation, page 4-27
• Guidelines and Limitations, page 4-27
• Enabling Link Aggregation, page 4-30
• Verifying Link Aggregation Settings (CLI), page 4-31
• Configuring Neighbor Devices to Support Link Aggregation, page 4-31
Information About Link Aggregation

Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller’s distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances access points transparently to the user.

Figure 4-9 shows LAG.

Figure 4-9  Link Aggregation

LAG simplifies controller configuration because you no longer need to configure primary and secondary ports for each interface. If any of the controller ports fail, traffic is automatically migrated to one of the other ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data.

Note
LAG is supported across switches.

Guidelines and Limitations

- You can bundle all eight ports on a Cisco 5508 Controller into a single link.
- Cisco 5500 Series Controllers support LAG in software release 6.0 or later releases, Catalyst 3750G Integrated Wireless LAN Controller Switch. With LAG enabled, the logical port on the Catalyst 3750G Integrated Wireless LAN Controller Switch and on each Cisco WiSM controller supports up to 150 access points.
- Terminating on two different modules within a single Catalyst 6500 series switch provides redundancy and ensures that connectivity between the switch and the controller is maintained when one module fails. Figure 4-10 shows this use of redundant modules. A Cisco 4402-50 Controller is
connected to two different Gigabit modules (slots 2 and 3) within the Catalyst 6500 Series Switch. The controller’s port 1 is connected to Gigabit interface 3/1, and the controller’s port 2 is connected to Gigabit interface 2/1 on the Catalyst 6500 series switch. Both switch ports are assigned to the same channel group.

When a Cisco 5500 Series Controller LAG port is connected to a Catalyst 3750G or a 6500 or 7600 channel group employing load balancing, note the following:

- LAG requires the EtherChannel to be configured for the on mode on both the controller and the Catalyst switch.
- Once the EtherChannel is configured as on at both ends of the link, it does not matter if the Catalyst switch is configured for either Link Aggregation Control Protocol (LACP) or Cisco proprietary Port Aggregation Protocol (PAgP) because no channel negotiation is done between the controller and the switch. Additionally, LACP and PAgP are not supported on the controller.
- The load-balancing method configured on the Catalyst switch must be a load-balancing method that terminates all IP datagram fragments on a single controller port. Not following this recommendation may result in problems with access point association.
- The recommended load-balancing method for Catalyst switches is `src-dst-ip` (enter the `port-channel load-balance src-dst-ip` command).
- The Catalyst 6500 series switches running in PFC3 or PFC3CXL mode implement enhanced EtherChannel load balancing. The enhanced EtherChannel load balancing adds the VLAN number to the hash function, which is incompatible with LAG. From Release 12.2(33)SXH and later releases, Catalyst 6500 IOS software offers the `exclude vlan` keyword to the `port-channel load-balance` command to implement `src-dst-ip` load distribution. See the Cisco IOS Interface and Hardware Component Command Reference for more information.
- Enter the `show platform hardware pfc mode` command on the Catalyst 6500 switch to confirm the PFC operating mode.

The following example shows a Catalyst 6500 series switch in PFC3B mode when you enter the global configuration `port-channel load-balance src-dst-ip` command for proper LAG functionality:

```bash
# show platform hardware pfc mode
PFC operating mode: PFC3B
# show EtherChannel load-balance
EtherChannel Load-Balancing Configuration:
src-dst-ip
```

The following example shows Catalyst 6500 series switch in PFC3C mode when you enter the `exclude vlan` keyword in the `port-channel load-balance src-dst-ip exclude vlan` command:

```bash
# show platform hardware pfc mode
PFC operating mode: PFC3C
# show EtherChannel load-balance
EtherChannel Load-Balancing Configuration:
src-ip enhanced
# mpls label-ip
```

- If the recommended load-balancing method cannot be configured on the Catalyst switch, then configure the LAG connection as a single member link or disable LAG on the controller.
You cannot configure the controller’s ports into separate LAG groups. Only one LAG group is supported per controller. Therefore, you can connect a controller in LAG mode to only one neighbor device.

**Note** The two internal Gigabit ports on the controller within the Catalyst 3750G Integrated Wireless LAN Controller Switch are always assigned to the same LAG group.

- When you enable LAG or make any changes to the LAG configuration, you must immediately reboot the controller.
- When you enable LAG, you can configure only one AP-manager interface because only one logical port is needed. LAG removes the requirement for supporting multiple AP-manager interfaces.
- 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. Also, the management, static AP-manager, and VLAN-tagged dynamic interfaces are moved to the LAG port.
- Multiple untagged interfaces to the same port are not allowed.
- When you enable LAG, you cannot create interfaces with a primary port other than 29.
- When you enable LAG, all ports participate in LAG by default. You must configure LAG for all of the connected ports in the neighbor switch.
- When you enable LAG, if any single link goes down, traffic migrates to the other links.
- When you enable LAG, only one functional physical port is needed for the controller to pass client traffic.
- When you enable LAG, access points remain connected to the switch, and data service for users continues uninterrupted.
- When you enable LAG, you eliminate the need to configure primary and secondary ports for each interface.
• When you enable LAG, the controller sends packets out on the same port on which it received them. If a CAPWAP packet from an access point enters the controller on physical port 1, the controller removes the CAPWAP wrapper, processes the packet, and forwards it to the network on physical port 1. This may not be the case if you disable LAG.

• When you disable LAG, the management, static AP-manager, and dynamic interfaces are moved to port 1.

• When you disable LAG, you must configure primary and secondary ports for all interfaces.

• When you disable LAG, you must assign an AP-manager interface to each port on the controller. Otherwise, access points are unable to join.

• Cisco 5500 Series Controllers support a single static link aggregation bundle.

• LAG is typically configured using the Startup Wizard, but you can enable or disable it at any time through either the GUI or CLI.

Note: LAG is enabled by default and is the only option on the Catalyst 3750G Integrated Wireless LAN Controller Switch.

Enabling Link Aggregation

This section contains the following topics:

- Enabling Link Aggregation (GUI), page 4-30
- Enabling Link Aggregation (CLI), page 4-31

Enabling Link Aggregation (GUI)

Step 1 Choose Controller > General to open the General page.

Figure 4-11   General Page
Step 2  Set the LAG Mode on Next Reboot parameter to **Enabled**.

**Note**  Choose **Disabled** if you want to disable LAG. LAG is disabled by default on the Cisco 5500 but enabled by default on the Catalyst 3750G Integrated Wireless LAN Controller Switch.

Step 3  Click **Apply** to commit your changes.
Step 4  Click **Save Configuration** to save your changes.
Step 5  Reboot the controller.
Step 6  Assign the WLAN to the appropriate VLAN.

---

**Enabling Link Aggregation (CLI)**

Step 1  Enter the `config lag enable` command to enable LAG.

**Note**  Enter the `config lag disable` command if you want to disable LAG.

Step 2  Enter the `save config` command to save your settings.
Step 3  Reboot the controller.

---

**Verifying Link Aggregation Settings (CLI)**

To verify your LAG settings, enter this command:

```
show lag summary
```

Information similar to the following appears:

```
LAG Enabled
```

---

**Configuring Neighbor Devices to Support Link Aggregation**

The controller’s neighbor devices must also be properly configured to support LAG.

- Each neighbor port to which the controller is connected should be configured as follows:

  ```
  interface GigabitEthernet <interface id>
  switchport
  channel-group <id> mode on
  no shutdown
  ```

- The port channel on the neighbor switch should be configured as follows:

  ```
  interface port-channel <id>
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk native vlan <native vlan id>
  switchport trunk allowed vlan <allowed vlans>
  switchport mode trunk
  no shutdown
  ```
Configuring Multiple AP-Manager Interfaces

This section contains the following topics:

- Information About Multiple AP-Manager Interfaces, page 4-32
- Guidelines and Limitations, page 4-33
- Creating Multiple AP-Manager Interfaces, page 4-35

Information About Multiple AP-Manager Interfaces

When you create two or more AP-manager interfaces, each one is mapped to a different port (see Figure 4-12). The ports should be configured in sequential order so that AP-manager interface 2 is on port 2, AP-manager interface 3 is on port 3, and AP-manager interface 4 is on port 4.

Before an access point joins a controller, it sends out a discovery request. From the discovery response that it receives, the access point can tell the number of AP-manager interfaces on the controller and the number of access points on each AP-manager interface. The access point generally joins the AP-manager with the least number of access points. In this way, the access point load is dynamically distributed across the multiple AP-manager interfaces.

Note

Access points may not be distributed completely evenly across all of the AP-manager interfaces, but a certain level of load balancing occurs.

Figure 4-12 Three AP-Manager Interfaces
This configuration has the advantage of load balancing all 100 access points evenly across all four AP-manager interfaces. If one of the AP-manager interfaces fails, all of the access points connected to the controller would be evenly distributed among the three available AP-manager interfaces. For example, if AP-manager interface 2 fails, the remaining AP-manager interfaces (1, 3, and 4) would each manage approximately 33 access points.

**Guidelines and Limitations**

- Only Cisco 2500 and 5500 Series Controllers support the use of multiple AP-manager interfaces.
- AP-manager interfaces do not need to be on the same VLAN or IP subnet, and they may or may not be on the same VLAN or IP subnet as the management interface. However, we recommend that you configure all AP-manager interfaces on the same VLAN or IP subnet.
- You must assign an AP-manager interface to each port on the controller.
- Before implementing multiple AP-manager interfaces, you should consider how they would impact your controller's port redundancy.

Examples:

- The Cisco 4404-100 Controller supports up to 100 access points and has four ports. To support the maximum number of access points, you would need to create three (or more) AP-manager interfaces (see Figure 4-14). If the port of one of the AP-manager interfaces fails, the controller clears the access points’ state, and the access points must reboot to reestablish communication with the controller using the normal controller join process. The controller no longer includes the failed AP-manager interface in the CAPWAP or LWAPP discovery responses. The access points then rejoin the controller and are load balanced among the available AP-manager interfaces.
Chapter 4      Configuring Ports and Interfaces

Figure 4-13 Two AP-Manager Interfaces

Figure 4-14 Four AP-Manager Interfaces
Creating Multiple AP-Manager Interfaces

This section contains the following topics:

- Creating Multiple AP-Manager Interfaces (GUI), page 4-35
- Creating Multiple AP-Manager Interfaces (CLI), page 4-37

Creating Multiple AP-Manager Interfaces (GUI)

**Step 1** Choose Controller > Interfaces to open the Interfaces page.

**Step 2** Click New. The Interfaces > New page appears.

**Figure 4-15 Interfaces > New Page**

```
Controller Interfaces > New
General
Inventory
Interfaces:
  Interface Name: ap-manager 2
  VLANId: 3
```

**Step 3** Enter an AP-manager interface name and a VLAN identifier.

**Step 4** Click Apply to commit your changes. The Interfaces > Edit page appears.
Step 5  Enter the appropriate interface parameters.

**Note**  Do not define a backup port for an AP-manager interface. Port redundancy is not supported for AP-manager interfaces. If the AP-manager interface fails, all of the access points connected to the controller through that interface are evenly distributed among the other configured AP-manager interfaces.

Step 6  To make this interface an AP-manager interface, select the Enable Dynamic AP Management check box.

**Note**  Only one AP-manager interface is allowed per physical port. A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

Step 7  Click Save Configuration to save your settings.

Step 8  Repeat this procedure for each additional AP-manager interface that you want to create.
Creating Multiple AP-Manager Interfaces (CLI)

Step 1
Enter these commands to create a new interface:

- `config interface create operator_defined_interface_name {vlan_id | x}
- `config interface address operator_defined_interface_name ip_addr ip_netmask [gateway]
- `config interface vlan operator_defined_interface_name {vlan_id | 0}
- `config interface port operator_defined_interface_name physical_ds_port_number
- `config interface dhcp operator_defined_interface_name ip_address_of_primary_dhcp_server [ip_address_of_secondary_dhcp_server]
- `config interface quarantine vlan interface_name vlan_id

Note: Use this command to configure a quarantine VLAN on any interface.

- `config interface acl operator_defined_interface_name access_control_list_name

Note: See Chapter 7, “Configuring Security Solutions,” for more information on ACLs.

Step 2
To make this interface an AP-manager interface, enter this command:

`config interface ap-manager operator_defined_interface_name {enable | disable}

Note: Only one AP-manager interface is allowed per physical port. A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

Step 3
To save your changes, enter this command:

`save config

Step 4
Repeat this procedure for each additional AP-manager interface that you want to create.

Configuration Example: Configuring AP-Manager on a Cisco 5500 Series Controller

For a Cisco 5500 Series Controller, we recommend having eight dynamic AP-manager interfaces and associating them to the controller’s eight Gigabit ports. If you are using the management interface, which acts like an AP-manager interface by default, you need to create only seven more dynamic AP-manager interfaces and associate them to the remaining seven Gigabit ports. For example, Figure 4-17 shows a dynamic interface that is enabled as a dynamic AP-manager interface and associated to port number 2, and Figure 4-18 shows a Cisco 5500 Series Controller with LAG disabled, the management interface used as one dynamic AP-manager interface, and seven additional dynamic AP-manager interfaces, each mapped to a different Gigabit port.
Configuration Example: Configuring AP-Manager on a Cisco 5500 Series Controller

Figure 4-17 Dynamic Interface Example with Dynamic AP Management

Figure 4-18 Cisco 5500 Series Controller Interface Configuration Example
Configuring VLAN Select

This section contains the following topics:

- Information About VLAN Select, page 4-39
- Guidelines and Limitations, page 4-39

Information About VLAN Select

Whenever a wireless client connects to a wireless network (WLAN), the client is placed in a VLAN that is associated with the WLAN. In a large venue such as an auditorium, a stadium, or a conference where there may be numerous wireless clients, having only a single WLAN to accommodate many clients might be a challenge.

The VLAN select feature enables you to use a single WLAN that can support multiple VLANs. Clients can get assigned to one of the configured VLANs. This feature enables you to map a WLAN to a single or multiple interface VLANs using interface groups. Wireless clients that associate to the WLAN get an IP address from a pool of subnets identified by the interfaces. The IP address is derived by an algorithm based on the MAC address of the wireless client. This feature also extends the current AP group architecture where AP groups can override an interface or interface group to which the WLAN is mapped to, with multiple interfaces using the interface groups. This feature also provides the solution to auto anchor restrictions where a wireless guest user on a foreign location can get an IP address from multiple subnets based on their foreign locations or foreign controllers from the same anchor controller.

When a client roams from one controller to another, the foreign controller sends the VLAN information as part of the mobility announce message. Based on the VLAN information received, the anchor decides whether the tunnel should be created between the anchor controller and the foreign controller. If the same VLAN is available on the foreign controller, the client context is completely deleted from the anchor and the foreign controller becomes the new anchor controller for the client.

If an interface (int-1) in a subnet is untagged in one controller (Vlan ID 0) and the interface (int-2) in the same subnet is tagged to another controller (Vlan ID 1), then with the VLAN select feature, client joining the first controller over this interface may not undergo an L2 roam while it moves to the second controller. Hence, for L2 roaming to happen between two controllers with VLAN select, all the interfaces in the same subnet should be either tagged or untagged.

As part of the VLAN select feature, the mobility announce message carries an additional vendor payload that contains the list of VLAN interfaces in an interface group mapped to a foreign controller’s WLAN. This VLAN list enables the anchor to differentiate from a local to local or local to foreign handoff.

**Note**

VLAN pooling applies to wireless clients and centrally switched WLANs.

Guidelines and Limitations

- Release 7.0.116.0 and prior releases of the controller software enabled you to associate one VLAN with a WLAN. Each VLAN required a single IP subnet. As a result, a WLAN required a large subnet to accommodate more clients. The VLAN select feature enables you to use a single WLAN that can support multiple VLANs.
- The following lightweight access points are supported: Cisco Aironet 1130, 1040, 1140, 1240, 1250, 1260, 3500, 3600, 1522/1524 Access Points, and 800 Series access points.
The following controllers are supported: Cisco Flex 7500, Cisco 5508, WiSM-2, 2500 Series Controllers.

Configuring Interface Groups

This section contains the following topics:

- Information About Interface Groups, page 4-40
- Guidelines and Limitations, page 4-40
- Configuring Interface Groups, page 4-41

Information About Interface Groups

Interface groups are logical groups of interfaces. Interface groups facilitate user configuration where the same interface group can be configured on multiple WLANs or while overriding a WLAN interface per AP group. An interface group can exclusively contain either quarantine or nonquarantine interfaces. An interface can be part of multiple interface groups.

A WLAN can be associated with an interface or interface group. The interface group name and the interface name cannot be the same.

This feature also enables you to associate a client to specific subnets based on the foreign controller that they are connected to. The anchor controller WLAN can be configured to maintain a mapping between foreign controller MAC and a specific interface or interface group (Foreign maps) as needed. If this mapping is not configured, clients on that foreign controller gets VLANs associated from interface group configured on WLAN.

You can also configure AAA override for interface groups. This feature extends the current access point group and AAA override architecture where access point groups and AAA override can be configured to override the interface group WLAN that the interface is mapped to. This is done with multiple interfaces using interface groups.

This feature enables network administrators to configure guest anchor restrictions where a wireless guest user at a foreign location can obtain an IP address from multiple subnets on the foreign location and controllers from within the same anchor controller.

Guidelines and Limitations

Table 4-1 lists the platform support for interface and interface groups:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Interface Groups</th>
<th>Interfaces per Interface Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>WiSM2, Cisco 5508 Series Controller, Cisco Flex 7500 Series Controller, Cisco 2500 Series Controller.</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>NM6 series</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>
Configuring Interface Groups

This section contains the following topics:

- Creating Interface Groups (GUI), page 4-41
- Creating Interface Groups (CLI), page 4-41
- Adding Interfaces to Interface Groups (GUI), page 4-41
- Adding Interfaces to Interface Groups (CLI), page 4-42
- Adding an Interface Group to a WLAN (GUI), page 4-42
- Adding an Interface Group to a WLAN (CLI), page 4-42
- Viewing VLANs in Interface Groups (CLI), page 4-42

Creating Interface Groups (GUI)

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Controller &gt; Interface Groups from the left navigation pane. The Interface Groups page appears with the list of interface groups already created.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>To remove an interface group, hover your mouse pointer over the blue drop-down icon and choose Remove.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Click Add Group to add a new group. The Add New Interface Group page appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Enter the details of the interface group:</td>
</tr>
<tr>
<td></td>
<td>• Interface Group Name—Specify the name of the interface group.</td>
</tr>
<tr>
<td></td>
<td>• Description—Add a brief description of the interface group.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Add.</td>
</tr>
</tbody>
</table>

Creating Interface Groups (CLI)

- `config interface group {create| delete} interface_group_name`—Creates or deletes an interface group
- `config interface group description interface_group_name "description"`—Adds a description to the interface group

Adding Interfaces to Interface Groups (GUI)

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Controller &gt; Interface Groups. The Interface Groups page appears with a list of all interface groups.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the name of the interface group to which you want to add interfaces. The Interface Groups &gt; Edit page appears.</td>
</tr>
</tbody>
</table>
Multicast Optimization

Step 3 Choose the interface name that you want to add to this interface group from the Interface Name drop-down list.

Step 4 Click Add Interface to add the interface to the Interface group.

Step 5 Repeat Steps 2 and 3 if you want to add multiple interfaces to this interface group.

Note To remove an interface from the interface group, hover your mouse pointer over the blue drop-down arrow and choose Remove.

Adding Interfaces to Interface Groups (CLI)

To add interfaces to interface groups, use the config interface group interface add interface_group interface_name command.

Viewing VLANs in Interface Groups (CLI)

To view a list of VLANs in the interface groups, use the show interface group detailed interface-group-name command.

Adding an Interface Group to a WLAN (GUI)

Step 1 Choose the WLAN tab.

The WLANs page appears listing the available WLANs.

Step 2 Click the WLAN ID of the WLAN to which you want to add the interface group.

Step 3 In the General tab, choose the interface group from the Interface/Interface Group (G) drop-down list.

Step 4 Click Apply.

Adding an Interface Group to a WLAN (CLI)

To add an interface group to a WLAN, use the command config wlan interface wlan_id interface_group_name.

Multicast Optimization

This section contains the following topics:

- Information About Multicast Optimization, page 4-43
- Configuring Multicast VLAN, page 4-43
Information About Multicast Optimization

Prior to the 7.0.116.0 release, multicast was based on the grouping of the multicast address and the VLAN as one entity, MGID. With VLAN select and VLAN pooling, there is a possibility that you might increase duplicate packets. With the VLAN select feature, every client listens to the multicast stream on a different VLAN. As a result, the controller creates different MGIDs for each multicast address and VLAN. Therefore, the upstream router sends one copy for each VLAN, which results, in the worst case, in as many copies as there are VLANs in the pool. Since the WLAN is still the same for all clients, multiple copies of the multicast packet are sent over the air. To suppress the duplication of a multicast stream on the wireless medium and between the controller and access points, you can use the multicast optimization feature.

Multicast optimization enables you to create a multicast VLAN which you can use for multicast traffic. You can configure one of the VLANs of the WLAN as a multicast VLAN where multicast groups are registered. Clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using multicast VLAN and multicast IP addresses. If multiple clients on the VLAN pool of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The controller makes sure that all multicast streams from the clients on this VLAN pool always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN pool. Only one multicast stream hits the VLAN pool even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the air is just one stream.

Configuring Multicast VLAN

This section contains the following topics:

- Configuring Multicast VLAN (GUI), page 4-43
- Configuring Multicast VLAN (CLI), page 4-43

Configuring Multicast VLAN (GUI)

Step 1 Choose the WLANs tab.
The WLANs tab appears.

Step 2 Click on the WLAN ID of the WLAN that you want to choose for a multicast VLAN.
The WLANs > Edit page appears.

Step 3 Enable the multicast VLAN feature by selecting the Multicast VLAN feature check box.
The Multicast Interface drop-down list appears.

Step 4 Choose the VLAN from the Multicast Interface drop-down list.

Step 5 Click Apply.

Configuring Multicast VLAN (CLI)

Use the config wlan multicast interface wlan_id enable interface_name command to configure the multicast VLAN feature.
Chapter 4  Configuring Ports and Interfaces

Multicast Optimization
Configuring Controller Settings

This chapter contains these sections:

- Installing and Configuring Licenses, page 4-2
- Configuring 802.11 Bands, page 4-25
- Configuring 802.11n Parameters, page 4-29
- Configuring 802.11h Parameters, page 4-34
- Configuring DHCP Proxy, page 4-36
- Configuring Administrator Usernames and Passwords, page 4-38
- Configuring SNMP, page 4-39
- SNMP Community Strings, page 4-40
- Changing the Default Values for SNMP v3 Users, page 4-42
- Configuring Aggressive Load Balancing, page 4-44
- Configuring Band Selection, page 4-48
- Configuring Fast SSID Changing, page 4-50
- Enabling 802.3X Flow Control, page 4-51
- Configuring 802.3 Bridging, page 4-51
- Configuring Multicast Mode, page 4-54
- Configuring Client Roaming, page 4-59
- Configuring IP-MAC Address Binding, page 4-64
- Configuring Quality of Service, page 4-66
- Configuring Voice and Video Parameters, page 4-73
- Configuring SIP Based CAC, page 4-88
- Configuring Voice Prioritization Using Preferred Call Numbers, page 4-88
- Configuring EDCA Parameters, page 4-90
- Configuring the Cisco Discovery Protocol, page 4-93
- Configuring Authentication for the Controller and NTP Server, page 4-101
- Configuring RFID Tag Tracking, page 4-102
- Configuring and Viewing Location Settings, page 4-110
- Using the Wireless LAN Controller Network Module, page 4-116
Installing and Configuring Licenses

This section contains the following topics:

- Information About Installing and Configuring Licenses, page 4-2
- Guidelines and Limitations, page 4-2
- Obtaining an Upgrade or Capacity Adder License, page 4-4
- Installing a License, page 4-7
- Viewing Licenses, page 4-9
- Activating an AP-Count Evaluation License, page 4-13
- Rehosting Licenses, page 4-16
- Configuring the License Agent, page 4-22

Information About Installing and Configuring Licenses

You can order Cisco 5500 Series Controllers with support for 12, 25, 50, 100, 250, or 500 access points as the controller’s base capacity. You can add additional access point capacity through capacity adder licenses available at 25, 50, 100, and 250 access point capacities. You can add the capacity adder licenses to any base license in any combination to arrive at the maximum capacity of 500 access points. The base and adder licenses are supported through both rehosting and RMAs.

Guidelines and Limitations

- These controller platforms do not require licenses: Cisco 2100 and Cisco 4400 Series Controllers, Cisco WiSMs, Controller Network Modules, and Catalyst 3750G Integrated Wireless LAN Controller Switches.
- All features included in a Wireless LAN Controller Wplus license are now included in the base license; this change is introduced in release 6.0.196.0. There are no changes to WCS BASE and PLUS licensing.
- The base license supports the standard base software set and, for releases 6.0.196.0 and later, the premium software set is included as part of the base feature set, which includes this functionality:
  - Datagram Transport Layer Security (DTLS) data encryption for added security across remote WAN and LAN links. For more information about data encryption, see the “Configuring Data Encryption” section on page 9-3.
- The Availability of data DTLS for the 7.0.116.0 release is as follows:
  - Cisco 5500 Series Controller—The Cisco 5500 Series Controller will be available with two licensing options: One with data DTLS capabilities and another image without data DTLS.
  - 2500, WiSM2, WLC2—These platforms by default will not contain DTLS. To turn on data DTLS, you must install a license. These platforms will have a single image with data DTLS turned off. To use data DTLS you will need to have a license.
- Support for OfficeExtend access points, which are used for secure mobile teleworking. For more information about the OfficeExtend access points, see the “Configuring OfficeExtend Access Points” section on page 9-62.

- Support for the 1130AG and 1240AG series indoor mesh access points, which dynamically establish wireless connections in locations where it might be difficult to connect to the wired network. For more information about mesh access points, see Chapter 10, “Controlling Mesh Access Points.”

- All features included in a Wireless LAN Controller WPLUS license are now included in the base license; this change is introduced in release 6.0.196.0. There are no changes to WCS BASE and PLUS licensing. These WPlus license features are included in the base license:
  - OfficeExtend AP
  - Enterprise Mesh
  - CAPWAP Data Encryption

- The licensing change can affect features on your wireless LAN when you upgrade or downgrade software releases, so you should be aware of these guidelines:
  - If you have a WPlus license and you upgrade from 6.0 or later to 7.0.98.0, your license file contains both Basic and WPlus license features. You will not see any disruption in feature availability and operation.
  - If you have a WPlus license and you downgrade from 7.0.98.0 to 6.0.196.0 or 6.0.188 or 6.0.182, your license file contains only base license, and you will lose all WPlus features.
  - If you have a base license and you downgrade from 6.0.196.0 to 6.0.188 or 6.0.182, when you downgrade, you lose all WPlus features.

- In the controller software 7.0.116.0 and later releases, the AP association trap is ciscoLwappApAssociated. In prior releases, the trap was bsnAPAssociated.

- To view the controller trap log, choose Monitor and click View All under “Most Recent Traps” on the controller GUI.

Note: You can also view traps by using SNMP-based management tools.

Figure 4-1 Trap Logs Page

- The ap-count licenses and their corresponding image-based licenses are installed together. The controller keeps track of the licensed access point count and does not allow more than the number of access points to associate to it.

- The Cisco 5500 Series Controller is shipped with both permanent and evaluation base and base-ap-count licenses. If desired, you can activate the evaluation licenses, which are designed for temporary use and set to expire after 60 days.
Obtaining an Upgrade or Capacity Adder License

This section contains the following topics:

- Information About Obtaining an Upgrade or Capacity Adder License, page 4-4
- Obtaining and Registering a PAK Certificate, page 4-6

Information About Obtaining an Upgrade or Capacity Adder License

A certificate with a product authorization key (PAK) is required before you can obtain an upgrade license.

You can use the capacity adder licenses to increase the number of access points supported by the controller up to a maximum of 500 access points. The capacity adder licenses are available in access point capacities of 10, 25, 50, 100 and 250 access points. You can add these licenses to any of the base capacity licenses of 12, 25, 50, 100 and 250 access points.

For example, if your controller was initially ordered with support for 100 access points (base license AIR-CT5508-100-K9), you could increase the capacity to 500 access points by purchasing a 250 access point, 100 access point, and a 50 access point additive capacity license (LIC-CT5508-250A, LIC-CT5508-100A, and LIC-CT5508-50A).

You can find more information on ordering capacity adder licenses at this URL: http://www.cisco.com/en/US/products/ps10315/products_data_sheets_list.html

If you skip any tiers when upgrading (for example, if you do not install the -25U and -50U licenses along with the -100U), the license registration for the upgraded capacity fails.

For a single controller, you can order different upgrade licenses in one transaction (for example, -25U, -50U, -100U, and -250U), for which you receive one PAK with one license. Then you have only one license (instead of four) to install on your controller.

If you have multiple controllers and want to upgrade all of them, you can order multiple quantities of each upgrade license in one transaction (for example, you can order 10 each of the -25U, -50U, -100U, and -250 upgrade licenses), for which you receive one PAK with one license. You can continue to register the PAK for multiple controllers until it is exhausted.

Base license SKUs for the Cisco 5500 Series Controllers are as follows:

- AIR-CT5508-12-K9
- AIR-CT5508-25-K9
- AIR-CT5508-50-K9
• AIR-CT5508-100-K9
• AIR-CT5508-250-K9
• AIR-CT5508-500-K9

Base license SKUs for the Cisco 2500 Series Controllers are as follows:
• AIR-CT2504-5-K9
• AIR-CT2504-15-K9
• AIR-CT2504-25-K9
• AIR-CT2504-50-K9

Base license SKUs for the Cisco WiSM2 Controllers are as follows:
• WS-SVC-WISM2-1-K9—WiSM2 with 100 AP support.
• WS-SVC-WISM2-3-K9—WiSM2 with 300 AP support
• WS-SVC-WISM2-5-K9—WiSM2 with 500 AP support

Table 4-1 lists the available adder licenses for the 5500 and 2500 Series Controllers.

<table>
<thead>
<tr>
<th>Type</th>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>e-mail</td>
<td>L-LIC-CT5508-UPG</td>
<td>Primary upgrade SKU: Pick any number or combination of the following options under this SKU to upgrade one or many controllers under one product authorization key</td>
</tr>
<tr>
<td></td>
<td>L-LIC-CT5508-25A</td>
<td>25 AP Adder License for the 5508 Controller (eDelivery)</td>
</tr>
<tr>
<td></td>
<td>L-LIC-CT5508-50A</td>
<td>50 AP Adder License for the 5508 Controller (eDelivery)</td>
</tr>
<tr>
<td></td>
<td>L-LIC-CT5508-100A</td>
<td>100 AP Adder License for the 5508 Controller (eDelivery)</td>
</tr>
<tr>
<td></td>
<td>L-LIC-CT5508-250A</td>
<td>250 AP Adder License for the 5508 Controller (eDelivery)</td>
</tr>
<tr>
<td></td>
<td>L-LIC-CT2504-UPG</td>
<td>Primary upgrade SKU: Pick any number or combination of the following options under this SKU to upgrade one or many controllers under one product authorization key</td>
</tr>
<tr>
<td></td>
<td>L-LIC-CT2504-5A</td>
<td>5 AP Adder License for Cisco 2504 Wireless Controller (e-Delivery)</td>
</tr>
<tr>
<td></td>
<td>L-LIC-CT2504-25A</td>
<td>25 AP Adder License for Cisco 2504 Wireless Controller (e-Delivery)</td>
</tr>
</tbody>
</table>
Installing and Configuring Licenses

Obtaining and Registering a PAK Certificate

Step 1
Order the PAK certificate for an upgrade license through your Cisco channel partner or your Cisco sales representative, or order it online at this URL:

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

Step 2
If you are ordering online, begin by choosing the primary upgrade SKU LIC-CT5508-UPG or LIC-CT2504-UPG. Then, choose any number of the following options to upgrade one or more controllers under one PAK. Table 4-1 lists the capacity adder licenses available through e-mail or on paper: After you receive the certificate, use one of two methods to register the PAK:

- **Cisco License Manager (CLM)**—This method automates the process of obtaining licenses and deploying them on Cisco devices. For deployments with more than five controllers, we recommend using CLM to register PAKs and install licenses. You can also use CLM to rehost or RMA a license.

  You cannot use CLM to change the licensed feature set or activate an ap-count evaluation license. To perform these operations, you must follow the instructions in the “Activating an AP-Count Evaluation License” section on page 4-13. Because you can use CLM to perform all other license operations, you can disregard the remaining licensing information in this chapter except these two sections and the “Configuring the License Agent” section on page 4-22 if you want your controller to use HTTP to communicate with CLM.

  You can download the CLM software and access user documentation at this URL:

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

Table 4-1  Available Capacity Adder Licenses (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>paper</td>
<td>LIC-CT5508-UPG</td>
<td>Primary upgrade SKU: Pick any number or combination of the following options under this SKU, to upgrade one or many controllers under one product authorization key</td>
</tr>
<tr>
<td></td>
<td>LIC-CT5508-25A</td>
<td>25 AP Adder License for the 5508 Controller</td>
</tr>
<tr>
<td></td>
<td>LIC-CT5508-50A</td>
<td>50 AP Adder License for the 5508 Controller</td>
</tr>
<tr>
<td></td>
<td>LIC-CT5508-100A</td>
<td>100 AP Adder License for the 5508 Controller</td>
</tr>
<tr>
<td></td>
<td>LIC-CT5508-250A</td>
<td>250 AP Adder License for the 5508 Controller</td>
</tr>
<tr>
<td></td>
<td>LIC-CT2504-UPG</td>
<td>Primary upgrade SKU: Pick any number or combination of the following options under this SKU, to upgrade one or many controllers under one product authorization key</td>
</tr>
<tr>
<td></td>
<td>LIC-CT2504-5A</td>
<td>5 AP Adder License for Cisco 2504 Controller (Paper Certificate - US Mail)</td>
</tr>
<tr>
<td></td>
<td>LIC-CT2504-25A</td>
<td>25 AP Adder License for Cisco 2504 Controller (Paper Certificate - US Mail)</td>
</tr>
</tbody>
</table>
Installing and Configuring Licenses

**Licensing portal**—This alternative method enables you to manually obtain and install licenses on your controller. If you want to use the licensing portal to register the PAK, follow the instructions in Step 3.

**Step 3**

Use the licensing portal to register the PAK as follows:

- Go to [http://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet](http://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet)
- On the main Product License Registration page, enter the PAK mailed with the certificate in the Product Authorization Key (PAK) text box and click **Submit**.
- On the Validate Features page, enter the number of licenses that you want to register in the Qty text box and click **Update**.
- To determine the controller’s product ID and serial number, choose **Controller > Inventory** on the controller GUI or enter the `show license udi` command on the controller CLI.
  
  Information similar to the following appears on the controller CLI:
  
<table>
<thead>
<tr>
<th>Device#</th>
<th>PID</th>
<th>SN</th>
<th>UDI</th>
</tr>
</thead>
<tbody>
<tr>
<td>*0</td>
<td>AIR-CT5508-K9</td>
<td>FCW1308L030</td>
<td>AIR-CT5508-K9:FCW1308L030</td>
</tr>
</tbody>
</table>

- On the Designate Licensee page, enter the product ID and serial number of the controller on which you plan to install the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click **Submit**.
- On the Finish and Submit page, verify that all information is correct and click **Submit**.
- When a message appears indicating that the registration is complete, click **Download License**. The license is e-mailed within 1 hour to the address that you specified.
- When the e-mail arrives, follow the instructions provided.
- Copy the license file to your TFTP server.

---

**Installing a License**

This section contains the following topics:

- Installing a License (GUI), page 4-7
- Installing a License (CLI), page 4-8
- Additional References, page 4-9

**Installing a License (GUI)**

- Choose **Management > Software Activation > Commands** to open the License Commands page.
Installing and Configuring Licenses

Figure 4-2 License Commands Page

Step 2  From the Action drop-down list, choose Install License. The Install License from a File section appears.

Step 3  In the File Name to Install text box, enter the path to the license (*.lic) on the TFTP server.

Step 4  Click Install License. A message appears to show whether the license was installed successfully. If the installation fails, the message provides the reason for the failure, such as the license is an existing license, the path was not found, the license does not belong to this device, you do not have correct permissions for the license, and so on.

Step 5  If the end-user license agreement (EULA) acceptance dialog box appears, read the agreement and click Accept to accept the terms of the agreement.

Note  Typically, you are prompted to accept the EULA for evaluation, extension, and rehost licenses. The EULA is also required for permanent licenses, but it is accepted during license generation.

Step 6  Save a backup copy of all installed licenses as follows:

a.  From the Action drop-down list, choose Save License.

b.  In the File Name to Save text box, enter the path on the TFTP server where you want the licenses to be saved.

Note  You cannot save evaluation licenses.

c.  Click Save Licenses.

Step 7  Reboot the controller.

Installing a License (CLI)

Step 1  Install a license on the controller by entering this command:

```
license install url
```

where url is tftp://server_ip/path/filename.
Note To remove a license from the controller, enter the `license clear license_name` command. For example, you might want to delete an expired evaluation license or any unused license. You cannot delete unexpired evaluation licenses, the permanent base image license, or licenses that are in use by the controller.

**Step 2** If you are prompted to accept the end-user license agreement (EULA), read and accept the terms of the agreement.

**Note** Typically, you are prompted to accept the EULA for evaluation, extension, and rehost licenses. The EULA is also required for permanent licenses, but it is accepted during license generation.

**Step 3** Add comments to a license or delete comments from a license by entering this command:

```
license comment {add | delete} license_name comment_string
```

**Step 4** Save a backup copy of all installed licenses by entering this command:

```
license save url
```

where `url` is `tftp://server_ip/path/filename`.

**Step 5** Reboot the controller by entering this command:

```
reset system
```

---

**Additional References**

- To see the status of the license that is installed, see “Viewing Licenses” section on page 4-9.
- To modify the license that is used by the controller, see the “Activating an AP-Count Evaluation License” section on page 4-13.

**Viewing Licenses**

This section contains the following topics:

- Viewing Licenses (GUI), page 4-9
- Viewing Licenses (CLI), page 4-11

**Viewing Licenses (GUI)**

**Step 1** Choose Management > Software Activation > Licenses to open the Licenses page.
Figure 4-3  Licenses Page

This page lists all of the licenses installed on the controller. For each license, it shows the license type, expiration, count (the maximum number of access points allowed for this license), priority (low, medium, or high), and status (in use, not in use, inactive, or EULA not accepted).

**Note**  Controller platforms do not support the status of “grace period” or “extension” as a license type. The license status will always show “evaluation” even if a grace period or an extension evaluation license is installed.

**Note**  If you ever want to remove a license from the controller, hover your cursor over the blue drop-down arrow for the license and click **Remove**. For example, you might want to delete an expired evaluation license or any unused license. You cannot delete unexpired evaluation licenses, the permanent base image license, or licenses that are in use by the controller.

**Step 2**  Click the link for the desired license to view more details for a particular license. The License Detail page appears.

This page shows the following additional information for the license:

- The license type (permanent, evaluation, or extension)
- The license version
- The status of the license (in use, not in use, inactive, or EULA not accepted)
- The length of time before the license expires

**Note**  Permanent licenses never expire.

- Whether the license is a built-in license
- The maximum number of access points allowed for this license
- The number of access points currently using this license

**Step 3**  If you want to enter a comment for this license, type it in the Comment text box and click **Apply**.
Step 4 Click **Save Configuration** to save your changes.

### Viewing Licenses (CLI)

- See the license level, license type, and number of access points licensed on the controller by entering this command:
  
  ```
  show sysinfo
  ```

  Information similar to the following appears:

  ```
  Manufacturer’s Name......................... Cisco Systems Inc.
  Product Name.................................. Cisco Controller
  Product Version.............................. 7.0
  RTOS Version.................................. 7.0
  Bootloader Version........................... 5.2
  Emergency Image Version...................... N/A
  Build Type..................................... DATA + WPS
  System Name................................... Cisco 69
  System Location.............................. na
  System Contact................................ abc@cisco.com
  System ObjectID............................... 1.3.6.1.4.1.14179.1.1.4.3
  IP Address.................................... 10.10.10.10
  System Up Time............................... 3 days 1 hrs 12 mins 42 secs
  System Timezone Location.....................
  CurrentBoot License Level.................... base
  CurrentBoot License Type..................... Permanent
  NextBoot License Level....................... base
  NextBoot License Type......................... Permanent
  Operating Environment....................... Commercial (0 to 40 C)
  Internal Temp Alarm Limits................... 0 to 65 C
  Internal Temperature........................ +40 C
  State of 802.11b Network..................... Enabled
  State of 802.11a Network..................... Enabled
  Number of WLANs.............................. 4
  Number of Active Clients..................... 0
  Burned-in MAC Address....................... 00:1A:6D:DD:1E:40
  Crypto Accelerator 1.......................... Absent
  Crypto Accelerator 2.......................... Absent
  Power Supply 1................................ Absent
  Power Supply 2................................ Present, OK
  Maximum number of APs supported............. 12
  ```

  **Note** The Operating Environment and Internal Temp Alarm Limits data are not displayed for Cisco Flex 7500 Series Controllers.

- See a brief summary of all active licenses installed on the controller by entering this command:
  
  ```
  show license summary
  ```

  Information similar to the following appears:

  ```
  Index 1 Feature: wplus
  Period left: 0 minute 0 second
  Index 2 Feature: wplus-ap-count
  Period left: 0 minute 0 second
  Index3 Feature: base
  Period left: Life time
  License Type: Permanent
  ```
License State: Active, In Use  
License Count: Non-Counted  
License Priority: Medium  

Index 4 Feature: base-ap-count  
  Period left: 6 weeks, 4 days  
  License Type: Evaluation  
  License State: Active, In Use  
  License Count: 250/250/0  
  License Priority: High

- See all of the licenses installed on the controller by entering this command:

  **show license all**

  Information similar to the following appears:

  License Store: Primary License Storage  
  StoreIndex:  1  Feature: base  Version: 1.0  
  License Type: Permanent  
  License State: Active, Not in Use  
  License Count: Non-Counted  
  License Priority: Medium

  StoreIndex:  3  Feature: base-ap-count  Version: 1.0  
  License Type: Evaluation  
  License State: Active, In Use  
  Evaluation period left: 8 weeks 4 days

- See the details for a particular license by entering this command:

  **show license detail license_name**

  Information similar to the following appears:

  Index:  1  Feature: base-ap-count  Version: 1.0  
  License Type: Permanent  
  License State: Active, Not in Use  
  License Count: 12/0/0  
  License Priority: Medium  
  Store Index: 0  
  Store Name: Primary License Storage

  Index:  2  Feature: base-ap-count  Version: 1.0  
  License Type: Evaluation  
  License State: Inactive  
  Evaluation period left: 8 weeks 4 days

- See all expiring, evaluation, permanent, or in-use licenses by entering this command:

  **show license { expiring | evaluation | permanent | in-use }**

  Information similar to the following appears for the **show license in-use** command:

  StoreIndex:  2  Feature: base-ap-count  Version: 1.0  
  License Type: Permanent  
  License State: Active, In Use  
  License Count: 12/12/0  
  License Priority: Medium
StoreIndex: 3 Feature: base Version: 1.0
License Type: Permanent
License State: Active, In Use
License Count: Non-Counted License Priority: Medium

Note Controller platforms do not support the status of “grace period” or “extension” as a license type. The license status will always show “evaluation” even if a grace period or an extension evaluation license is installed.

- See the maximum number of access points allowed for this license on the controller, the number of access points currently joined to the controller, and the number of access points that can still join the controller by entering this command:

  **show license capacity**

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Licensed Feature</th>
<th>Max Count</th>
<th>Current Count</th>
<th>Remaining Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Count</td>
<td>250</td>
<td>4</td>
<td>246</td>
</tr>
</tbody>
</table>

- See statistics for all licenses on the controller by entering this command:

  **show license statistics**

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Administrative statistics</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Install success count:</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install failure count:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install duplicate count:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment add count:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment delete count:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear count:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Save count:</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Save cred count:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Client status</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Request success count</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request failure count</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Release count</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global Notify count</td>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- See a summary of license-enabled features by entering this command:

  **show license feature**

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Feature name</th>
<th>Enforcement</th>
<th>Evaluation</th>
<th>Clear Allowed</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>base</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>base-ap-count</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

**Activating an AP-Count Evaluation License**

This section contains the following topics:

- Information About Activating an AP-Count Evaluation License, page 4-14
- Activating an AP-Count Evaluation License, page 4-14
Information About Activating an AP-Count Evaluation License

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license with a 50-access-point count and want to try an evaluation license with a 100-access-point count, you can try out the evaluation license for 60 days.

AP-count evaluation licenses are set to low priority by default so that the controller uses the ap-count permanent license. If you want to try an evaluation license with an increased access point count, you must change its priority to high. If you no longer want to have this higher capacity, you can lower the priority of the ap-count evaluation license, which forces the controller to use the permanent license.

Note

To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

Activating an AP-Count Evaluation License

This section contains the following topics:

- Activating an AP-Count Evaluation License (GUI), page 4-14
- Activating an AP-Count Evaluation License (CLI), page 4-15

Activating an AP-Count Evaluation License (GUI)

Step 1  Choose Management > Software Activation > Licenses to open the Licenses page.

Figure 4-4  Licenses Page

The Status column shows which licenses are currently in use, and the Priority column shows the current priority of each license.
Step 2  Activate an ap-count evaluation license as follows:

a. Click the link for the ap-count evaluation license that you want to activate. The License Detail page appears.

b. Choose **High** from the Priority drop-down list and click **Set Priority**.

| Note   | You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured. |

c. Click **OK** when prompted to confirm your decision about changing the priority of the license.

d. When the EULA appears, read the terms of the agreement and then click **Accept**.

e. When prompted to reboot the controller, click **OK**.

f. Reboot the controller in order for the priority change to take effect.

g. Click **Licenses** to open the Licenses page and verify that the ap-count evaluation license now has a high priority and is in use. You can use the evaluation license until it expires.

Step 3  If you decide to stop using the ap-count evaluation license and want to revert to using an ap-count permanent license, follow these steps:

a. On the Licenses page, click the link for the ap-count evaluation license that is in use.

b. Choose **Low** from the Priority drop-down list and click **Set Priority**.

| Note   | You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured. |

c. Click **OK** when prompted to confirm your decision about changing the priority of the license.

d. When the EULA appears, read the terms of the agreement and then click **Accept**.

e. When prompted to reboot the controller, click **OK**.

f. Reboot the controller in order for the priority change to take effect.

g. Click **Licenses** to open the Licenses page and verify that the ap-count evaluation license now has a low priority and is not in use. Instead, the ap-count permanent license should be in use.

Activating an AP-Count Evaluation License (CLI)

**Step 1**  See the current status of all the licenses on your controller by entering this command:

```
show license all
```

Information similar to the following appears:

```
License Store: Primary License Storage
StoreIndex: 0  Feature: base-ap-count  Version: 1.0
  License Type: Permanent
  License State: Active, In Use
  License Count: 12/0/0
  License Priority: Medium
StoreIndex: 1  Feature: base  Version: 1.0
  License Type: Permanent
  License State: Active, In Use
```
License Count: Non-Counted
License Priority: Medium
StoreIndex:  2  Feature: base   Version: 1.0
License Type: Evaluation
License State: Inactive
  Evaluation total period:  8 weeks  4 days
  Evaluation period left:  8 weeks  4 days
License Count: Non-Counted
License Priority: Low
StoreIndex:  3  Feature: base-ap-count   Version: 1.0
License Type: Evaluation
License State: Inactive
  Evaluation total period:  8 weeks  4 days
  Evaluation period left:  8 weeks  4 days
License Count: 250/0/0
License Priority: Low

The License State text box shows the licenses that are in use, and the License Priority text box shows the current priority of each license.

**Step 2**
Activate an ap-count evaluation license as follows:

a. To raise the priority of the base-ap-count evaluation license, enter this command:
   ```
   license modify priority license_name high
   ```
   
   **Note**
   You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.

b. To reboot the controller in order for the priority change to take effect, enter this command:
   ```reset system```

c. To verify that the ap-count evaluation license now has a high priority and is in use, enter this command:
   ```show license all```
   You can use the evaluation license until it expires.

**Step 3**
If you decide to stop using the ap-count evaluation license and want to revert to using an ap-count permanent license, follow these steps:

a. To lower the priority of the ap-count evaluation license, enter this command:
   ```
   license modify priority license_name low
   ```

b. To reboot the controller in order for the priority change to take effect, enter this command:
   ```reset system```

c. To verify that the ap-count evaluation license now has a low priority and is not in use, enter this command:
   ```show license all```
   Instead, the ap-count permanent license should be in use.

---

**Rehosting Licenses**

This section contains the following topics:
Information About Rehosting Licenses

Revoking a license from one controller and installing it on another is called rehosting. You might want to rehost a license in order to change the purpose of a controller. For example, if you want to move your OfficeExtend or indoor mesh access points to a different controller, you could transfer the adder license from one controller to another controller of the same model, say from one 5500 series controller to another 5500 series controller (intramodel transfer). This can be done in the case of RMA or a network rearchitecture that requires you to transfer licenses from one appliance to another. It is not possible to rehost base licenses in normal scenarios of network rearchitecture. The only exception where the transfer of base licenses is allowed is for RMA when you get a replacement hardware when your existing appliance has a failure.

Evaluation licenses cannot be rehosted.

In order to rehost a license, you must generate credential information from the controller and use it to obtain a permission ticket to revoke the license from the Cisco licensing site. Next, you must obtain a rehost ticket and use it to obtain a license installation file for the controller on which you want to install the license.

Note
A revoked license cannot be reinstalled on the same controller

Rehosting a License

This section contains the following topics:

- Rehosting a License (GUI), page 4-17
- Rehosting a License (CLI), page 4-19

Rehosting a License (GUI)

Step 1
Choose Management > Software Activation > Commands to open the License Commands page.

Step 2
From the Action drop-down list, choose Rehost. The Revoke a License from the Device and Generate Rehost Ticket area appears.
Step 3  In the File Name to Save Credentials text box, enter the path on the TFTP server where you want the device credentials to be saved and click **Save Credentials**.

Step 4  To obtain a permission ticket to revoke the license, follow these steps:

- a. Click **Cisco Licensing** ([https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet](https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet)).
- b. On the Product License Registration page, click **Look Up a License** under Manage Licenses.
- c. Enter the product ID and serial number for your controller.

  **Note**  To find the controller’s product ID and serial number, choose **Controller > Inventory** on the controller GUI.

- d. Open the device credential information file that you saved in Step 3 and copy and paste the contents of the file into the Device Credentials text box.
- e. Enter the security code in the blank box and click **Continue**.
- f. Choose the licenses that you want to revoke from this controller and click **Start License Transfer**.
- g. On the Rehost Quantities page, enter the number of licenses that you want to revoke in the To Rehost text box and click **Continue**.
- h. On the Designate Licensee page, enter the product ID and serial number of the controller for which you plan to revoke the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click **Continue**.
- i. On the Review and Submit page, verify that all information is correct and click **Submit**.
- j. When a message appears indicating that the registration is complete, click **Download Permission Ticket**. The rehost permission ticket is e-mailed within 1 hour to the address that you specified.
- k. After the e-mail arrives, copy the rehost permission ticket to your TFTP server.
Step 5  Use the rehost permission ticket to revoke the license from this controller and generate a rehost ticket as follows:
  a. In the Enter Saved Permission Ticket File Name text box, enter the TFTP path and filename (*.lic) for the rehost permission ticket that you generated in Step 4.
  b. In the Rehost Ticket File Name text box, enter the TFTP path and filename (*.lic) for the ticket that will be used to rehost this license on another controller.
  c. Click Generate Rehost Ticket.
  d. When the end-user license agreement (EULA) acceptance dialog box appears, read the agreement and click Accept to accept the terms of the agreement.

Step 6  Use the rehost ticket generated in Step 5 to obtain a license installation file, which can then be installed on another controller as follows:
  a. Click Cisco Licensing.
  b. On the Product License Registration page, click Upload Rehost Ticket under Manage Licenses.
  c. On the Upload Ticket page, enter the rehost ticket that you generated in Step 5 in the Enter Rehost Ticket text box and click Continue.
  d. On the Validate Features page, verify that the license information for your controller is correct, enter the rehost quantity, and click Continue.
  e. On the Designate Licensee page, enter the product ID and serial number of the controller on which you plan to use the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click Continue.
  f. On the Review and Submit page, verify that all information is correct and click Submit.
  g. When a message appears indicating that the registration is complete, click Download License. The rehost license key is e-mailed within 1 hour to the address that you specified.
  h. After the e-mail arrives, copy the rehost license key to your TFTP server.
  i. Follow the instructions in the “Installing a License (GUI)” section on page 4-7 to install this license on another controller.

Rehosting a License (CLI)

Step 1  Save device credential information to a file by entering this command:

```
license save credential url
```

where `url` is `tftp://server_ip/path/filename`.

Step 2  Obtain a permission ticket to revoke the license as follows:
  b. Under Manage Licenses, click Look Up a License.
  c. Enter the product ID and serial number for your controller.

Note: To find the controller’s product ID and serial number, enter the `show license udi` command on the controller CLI.
d. Open the device credential information file that you saved in Step 1 and copy and paste the contents of the file into the Device Credentials text box.

e. Enter the security code in the blank box and click Continue.

f. Choose the licenses that you want to revoke from this controller and click Start License Transfer.

g. On the Rehost Quantities page, enter the number of licenses that you want to revoke in the To Rehost text box and click Continue.

h. On the Designate Licensee page, enter the product ID and serial number of the controller for which you plan to revoke the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click Continue.

i. On the Review and Submit page, verify that all information is correct and click Submit.

j. When a message appears indicating that the registration is complete, click Download Permission Ticket. The rehost permission ticket is e-mailed within 1 hour to the address that you specified.

k. After the e-mail arrives, copy the rehost permission ticket to your TFTP server.

**Step 3**

Use the rehost permission ticket to revoke the license from this controller and generate a rehost ticket as follows:

a. To revoke the license from the controller, enter this command:

   ```
   license revoke permission_ticket_url
   ```

   where `permission_ticket_url` is `tftp://server_ip/path/filename`.

b. To generate the rehost ticket, enter this command:

   ```
   license revoke rehost rehost_ticket_url
   ```

   where `rehost_ticket_url` is `tftp://server_ip/path/filename`.

c. If prompted, read and accept the terms of the end-user license agreement (EULA).

**Step 4**

Use the rehost ticket generated in Step 3 to obtain a license installation file, which can then be installed on another controller as follows:


b. On the Product License Registration page, click Upload Rehost Ticket under Manage Licenses.

c. On the Upload Ticket page, enter the rehost ticket that you generated in Step 3 in the Enter Rehost Ticket text box and click Continue.

d. On the Validate Features page, verify that the license information for your controller is correct, enter the rehost quantity, and click Continue.

e. On the Designate Licensee page, enter the product ID and serial number of the controller on which you plan to use the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click Continue.

f. On the Review and Submit page, verify that all information is correct and click Submit.

g. When a message appears indicating that the registration is complete, click Download License. The rehost license key is e-mailed within 1 hour to the address that you specified.

h. After the e-mail arrives, copy the rehost license key to your TFTP server.

i. Follow the instructions in the “Installing a License (GUI)” section on page 4-7 to install this license on another controller.
Transferring Licenses to a Replacement Controller after an RMA

This section contains the following topics:
- Information About Transferring Licenses to a Replacement Controller after an RMA, page 4-21
- Transferring a License to a Replacement Controller after an RMA, page 4-21

Information About Transferring Licenses to a Replacement Controller after an RMA

If you return a Cisco 5500 Series Controller to Cisco as part of the Return Material Authorization (RMA) process, you must transfer that controller’s licenses within 60 days to a replacement controller that you receive from Cisco.

Replacement controllers come preinstalled with the following licenses: permanent base and evaluation base, base-ap-count. No other permanent licenses are installed. The SKU for replacement controllers is AIR-CT5508-CA-K9.

Because licenses are registered to the serial number of a controller, you can use the licensing portal on Cisco.com to request that the license from your returned controller be revoked and authorized for use on the replacement controller. After your request is approved, you can install the old license on the replacement controller. Before you begin, you need the product ID and serial number of both the returned controller and the replacement controller. This information is included in your purchase records.

Note

The evaluation licenses on the replacement controller are designed for temporary use and expire after 60 days. To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. If the evaluation licenses expire before you transfer the permanent licenses from your defective controller to your replacement controller, the replacement controller remains up and running using the permanent base license, but access points are no longer able to join the controller.

Transferring a License to a Replacement Controller after an RMA

Step 1 Go to https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet.
Step 2 On the main Product License Registration page, click Register for an RMA License under RMA License Transfer.
Step 3 In the Select a Product drop-down list, choose Cisco 5500 Series Wireless Controllers.
Step 4 Enter the security code in the blank box and click Go to RMA Portal.
Step 5 On the RMA License Transfer page, enter the product ID and serial number of the controller that you returned and your RMA service contract number, and click Continue.
Step 6 On the Validate Features page, verify that the license information for your controller is correct, and click Continue.
Step 7 On the Designate Licensee page, enter the product ID and serial number of the replacement controller.
Step 8 Read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click Submit.
Step 9 On the Review and Submit page, verify that all information is correct and click Submit. A message appears indicating that your registration request has been submitted, and you will receive an e-mail that contains your RMA request ID.
Step 10  Select the status of your RMA registration request by following the instructions in the e-mail.

Step 11  After you receive another e-mail notifying you that your RMA registration request is approved (usually within 1 hour), follow the instructions in the “Installing a License (GUI)” section on page 4-7 to install the license on the replacement controller.

### Configuring the License Agent

This section contains the following topics:

- Information About Configuring the License Agent, page 4-22
- Configuring the License Agent, page 4-22

#### Information About Configuring the License Agent

If your network contains various Cisco-licensed devices, you might want to consider using the Cisco License Manager (CLM) to manage all of the licenses using a single application. CLM is a secure client/server application that manages Cisco software licenses network wide.

The license agent is an interface module that runs on the controller and mediates between CLM and the controller’s licensing infrastructure. CLM can communicate with the controller using various channels, such as HTTP, Telnet, and so on. If you want to use HTTP as the communication method, you must enable the license agent on the controller.

The license agent receives requests from CLM and translates them into license commands. It also sends notifications to CLM. It uses XML messages over HTTP or HTTPS to receive the requests and send the notifications. For example, CLM sends a license install command, and the agent notifies CLM after the license expires.

Note  You can download the CLM software and access user documentation at http://www.cisco.com/go/clm.

#### Configuring the License Agent

This section contains the following topics:

- Configuring the License Agent (GUI), page 4-22
- Configuring the License Agent (CLI), page 4-24

### Configuring the License Agent (GUI)

**Step 1**  Choose Management > Software Activation > License Agent to open the License Agent Configuration page.
Figure 4-6     License Agent Configuration Page

Step 2 Select the Enable Default Authentication check box to enable the license agent, or leave it unselected to disable this feature. The default value is unselected.

Step 3 In the Maximum Number of Sessions text box, enter the maximum number of sessions for the license agent. The valid range is 1 to 25 sessions (inclusive).

Step 4 Configure the license agent to listen for requests from the CLM as follows:
   a. Select the Enable Listener check box to enable the license agent to receive license requests from the CLM, or unselect this check box to disable this feature. The default value is unselected.
   b. In the Listener Message Processing URL text box, enter the URL where the license agent receives license requests (for example, http://209.165.201.30/licenseAgent/custom). The Protocol parameter indicates whether the URL requires HTTP or HTTPS.
      
      Note You can specify the protocol to use on the HTTP Configuration page. For more information, see the “Enabling Web and Secure Web Modes” section on page 3-18.
   c. Select the Enable Authentication for Listener check box to enable authentication for the license agent when it is receiving license requests, or unselect this check box to disable this feature. The default value is unselected.
   d. In the Max HTTP Message Size text box, enter the maximum size for license requests. The valid range is 0 to 9999 bytes, and the default value is 0.

Step 5 Configure the license agent to send license notifications to the CLM as follows:
   a. Select the Enable Notification check box to enable the license agent to send license notifications to the CLM, or unselect this check box to disable this feature. The default value is unselected.
   b. In the URL to Send the Notifications text box, enter the URL where the license agent sends the notifications (for example, http://www.cisco.com/license/notify).
   c. In the User Name text box, enter the username required in order to view the notification messages at this URL.
d. In the Password and Confirm Password text boxes, enter the password required in order to view the notification messages at this URL.

**Step 6** Click **Apply** to commit your changes.

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

### Configuring the License Agent (CLI)

**Step 1** Enable the license agent by entering one of these commands:

- `config license agent default authenticate`—Enables the license agent default listener with authentication.
- `config license agent default authenticate none`—Enables the license agent default listener without authentication.

**Note** To disable the license agent default listener, enter the `config license agent default disable` command. The default value is disabled.

**Step 2** Specify the maximum number of sessions for the license agent by entering this command:

`config license agent max-sessions sessions`

The valid range for the `sessions` parameter is 1 to 25 (inclusive), and the default value is 9.

**Step 3** Enable the license agent to receive license requests from the CLM and to specify the URL where the license agent receives the requests by entering this command:

`config license agent listener http {plaintext | encrypt} url authenticate [none] [max-message size] [acl acl]`

The valid range for the `size` parameter is 0 to 65535 bytes, and the default value is 0.

**Note** To prevent the license agent from receiving license requests from the CLM, enter the `config license agent listener http disable` command. The default value is disabled.

**Step 4** Configure the license agent to send license notifications to the CLM and to specify the URL where the license agent sends the notifications by entering this command:

`config license agent notify url username password`

**Note** To prevent the license agent from sending license notifications to the CLM, enter the `config license agent notify disable username password` command. The default value is disabled.

**Step 5** Save your changes by entering this command:

`save config`

**Step 6** See statistics for the license agent’s counters or sessions by entering this command:

`show license agent {counters | sessions}`

Information similar to the following appears for the `show license agent counters` command:

License Agent Counters
Request Messages Received: 10: Messages with Errors: 1
Request Operations Received: 9: Operations with Errors: 0
Notification Messages Sent: 12: Transmission Errors: 0: Soap Errors: 0

Information similar to the following appears for the `show license agent sessions` command:
License Agent Sessions: 1 open, maximum is 9

**Note** To clear the license agent’s counter or session statistics, enter the `clear license agent { counters | sessions }` command.

### Configuring 802.11 Bands

This section contains the following topics:
- Information About Configuring 802.11 Bands, page 4-25
- Configuring 802.11 Bands, page 4-25

### Information About Configuring 802.11 Bands

You can configure the 802.11b/g/n (2.4-GHz) and 802.11a/n (5-GHz) bands for the controller to comply with the regulatory requirements in your country. By default, both 802.11b/g/n and 802.11a/n are enabled.

### Configuring 802.11 Bands

This section contains the following topics:
- Configuring 802.11 Bands (GUI), page 4-25
- Configuring 802.11 Bands (CLI), page 4-27

### Configuring 802.11 Bands (GUI)

**Step 1** Choose **Wireless > 802.11a/n or 802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.
**Figure 4-7 802.11a Global Parameters Page**

**Step 2**  
Select the **802.11a** (or **802.11b/g**) **Network Status** check box to enable the 802.11a or 802.11b/g band. To disable the band, unselect the check box. The default value is enabled. You can enable both the 802.11a and 802.11b/g bands.

**Step 3**  
If you enabled the 802.11b/g band in **Step 2**, select the **802.11g Support** check box if you want to enable 802.11g network support. The default value is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.

**Step 4**  
Specify the rate at which the SSID is broadcast by the access point by entering a value between 100 and 600 milliseconds (inclusive) in the **Beacon Period** text box. The default value is 100 milliseconds.

**Note**  
The beacon period in controllers is listed in terms of milliseconds. The beacon period can also be measured in time units, where one time unit equals 1024 microseconds or 0.1024 milliseconds. If a beacon interval is listed as 100 milliseconds in a controller, it is only a rounded off value for 102.4 milliseconds. Due to hardware limitation in certain radios, even though the beacon interval is, say 100 time units, it is adjusted to 102 time units, which roughly equals 104.448 milliseconds. When the beacon period is to be represented in terms of time units, the value is adjusted to the nearest multiple of 17.

**Step 5**  
Specify the size at which packets are fragmented by entering a value between 256 and 2346 bytes (inclusive) in the **Fragmentation Threshold** text box. Enter a low number for areas where communication is poor or where there is a great deal of radio interference.

**Step 6**  
Make access points advertise their channel and transmit power level in beacons and probe responses. Select the **DTPC Support** check box. Otherwise, unselect this check box. The default value is enabled. Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.
Chapter 4 Configuring Controller Settings

Configuring 802.11 Bands

**Note** On access points that run Cisco IOS software, this feature is called *world mode*.

**Note** DTPC and 802.11h power constraint cannot be enabled simultaneously.

**Step 7** Specify the maximum allowed clients by entering a value between 1 to 200 in the Maximum Allowed Client text box. The default value is 200.

**Step 8** Use the Data Rates options to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:

- **802.11a**—6, 9, 12, 18, 24, 36, 48, and 54 Mbps
- **802.11b/g**—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

For each data rate, choose one of these options:

- **Mandatory**—Clients must support this data rate in order to associate to an access point on the controller.
- **Supported**—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.
- **Disabled**—The clients specify the data rates used for communication.

**Step 9** Click **Apply** to commit your changes.

**Step 10** Click **Save Configuration** to save your changes.

---

Configuring 802.11 Bands (CLI)

**Step 1** Disable the 802.11a band by entering this command:

```
config 802.11a disable network
```

**Note** The 802.11a band must be disabled before you can configure the 802.11a network parameters in this section.

**Step 2** Disable the 802.11b/g band by entering this command:

```
config 802.11b disable network
```

**Note** The 802.11b band must be disabled before you can configure the 802.11b network parameters in this section.

**Step 3** Specify the rate at which the SSID is broadcast by the access point by entering this command:

```
config {802.11a | 802.11b} beaconperiod time_unit
```

where *time_unit* is the beacon interval in time units (TUs). One TU is 1024 microseconds. You can configure the access point to send a beacon every 20 to 1000 milliseconds.

**Step 4** Specify the size at which packets are fragmented by entering this command:
config {802.11a | 802.11b} fragmentation threshold

where threshold is a value between 256 and 2346 bytes (inclusive). Specify a low number for areas where communication is poor or where there is a great deal of radio interference.

**Step 5**

Make access points advertise their channel and transmit power level in beacons and probe responses by entering this command:

```
config {802.11a | 802.11b} dtpc {enable | disable}
```

The default value is enabled. Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

**Note**

On access points that run Cisco IOS software, this feature is called *world mode*.

**Step 6**

Specify the maximum allowed clients that can be configured using the command:

```
config {802.11a | 802.11b} max-clients max_allow_clients
```

**Step 7**

Specify the rates at which data can be transmitted between the controller and the client by entering this command:

```
config {802.11a | 802.11b} rate {disabled | mandatory | supported} rate
```

where

- **disabled**—Clients specify the data rates used for communication.
- **mandatory**—Clients support this data rate in order to associate to an access point on the controller.
- **supported**—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.
- **rate**—The rate at which data is transmitted:
  - 6, 9, 12, 18, 24, 36, 48, and 54 Mbps (802.11a)
  - 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps (802.11b/g)

**Step 8**

Enable the 802.11a band by entering this command:

```
config 802.11a enable network
```

The default value is enabled.

**Step 9**

Enable the 802.11b band by entering this command:

```
config 802.11b enable network
```

The default value is enabled.

**Step 10**

Enable or disable 802.11g network support by entering this command:

```
config 802.11b 11gSupport {enable | disable}
```

The default value is enabled. You can use this command only if the 802.11b band is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.

**Step 11**

Save your changes by entering this command:

```
save config
```

**Step 12**

View the configuration settings for the 802.11a or 802.11b/g band by entering this command:

```
show {802.11a | 802.11b}
```
Information similar to the following appears:

- **802.11a Network**............................... Enabled
- **11nSupport**.................................... Enabled
  - **802.11a Low Band**........................... Enabled
  - **802.11a Mid Band**........................... Enabled
  - **802.11a High Band**......................... Enabled
- **802.11a Operational Rates**
  - **802.11a 6M Rate**.............................. Mandatory
  - **802.11a 9M Rate**.............................. Supported
  - **802.11a 12M Rate**............................. Mandatory
  - **802.11a 18M Rate**............................. Supported
  - **802.11a 24M Rate**............................. Mandatory
  - **802.11a 36M Rate**............................. Supported
  - **802.11a 48M Rate**............................. Supported
  - **802.11a 54M Rate**............................. Supported
- **Beacon Interval**................................. 100
- **Default Channel**............................... 36
- **Default Tx Power Level**....................... 1
- **DTPC Status**................................... Enabled
- **Fragmentation Threshold**....................... 2346
- **Maximum Number of Clients per AP**............ 200

---

**Configuring 802.11n Parameters**

This section contains the following topics:

- Information About Configuring 802.11n Parameters, page 4-29
- Configuring 802.11n Parameters, page 4-29
- Additional References, page 4-34

**Information About Configuring 802.11n Parameters**

This section provides instructions for managing 802.11n devices such as the Cisco Aironet 1140 and 1250 Series Access Points on your network. The 802.11n devices support the 2.4- and 5-GHz bands and offer high-throughput data rates.

The 802.11n high-throughput rates are available on 1040, 1140, 1250, 1260, 3500, and 3600 series access points for WLANs using WMM with no Layer 2 encryption or with WPA2/AES encryption enabled.

**Configuring 802.11n Parameters**

This section contains the following topics:

- Configuring 802.11n Parameters (GUI), page 4-30
- Configuring 802.11n Parameters (CLI), page 4-31
Chapter 4 Configuring Controller Settings

Configuring 802.11n Parameters

Step 1 Choose Wireless > 802.11a/n or 802.11b/g/n > High Throughput (802.11n) to open the 802.11n (5 GHz or 2.4 GHz) High Throughput page.

Figure 4-8 802.11n (2.4 GHz) High Throughput Page

Step 2 Select the 11n Mode check box to enable 802.11n support on the network. The default value is enabled.

Step 3 Select the check boxes of the desired rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. These data rates, which are calculated for a 20-MHz channel width using a short guard interval, are available:

- 0 (7 Mbps)
- 1 (14 Mbps)
- 2 (21 Mbps)
- 3 (29 Mbps)
- 4 (43 Mbps)
- 5 (58 Mbps)
- 6 (65 Mbps)
- 7 (72 Mbps)
- 8 (14 Mbps)
- 9 (29 Mbps)
Chapter 4  Configuring Controller Settings

Configuring 802.11n Parameters

Step 4  Click Apply to commit your changes.

Step 5  Use the 802.11n data rates that you configured by enabling WMM on the WLAN as follows:

a. Choose WLANs to open the WLANs page.

b. Click the ID number of the WLAN for which you want to configure WMM mode.

c. When the WLANs > Edit page appears, choose the QoS tab to open the WLANs > Edit (Qos) page.

d. From the WMM Policy drop-down list, choose Required or Allowed to require or allow client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

e. Click Apply to commit your changes.

Step 6  Click Save Configuration to save your changes.

Note  To determine if an access point supports 802.11n, look at the 11n Supported text box on either the 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page or the 802.11a/n (or 802.11b/g/n) AP Interfaces > Details page.

Configuring 802.11n Parameters (CLI)

Step 1  Enable 802.11n support on the network by entering this command:

```
config {802.11a | 802.11b} 11nsupport {enable | disable}
```

Step 2  Specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client by entering this command:

```
config {802.11a | 802.11b} 11nsupport mcs tx {0-15} {enable | disable}
```

See the descriptions of the 0 through 15 MCS data rates in the “Configuring 802.11n Parameters (GUI)” section on page 4-30.

Step 3  Use the 802.11n data rates that you configured by enabling WMM on the WLAN as follows:

```
config wlan wmm required wlan_id
```

The required parameter requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 4  Specify the aggregation method used for 802.11n packets as follows:

a. Disable the network by entering this command:
config {802.11a | 802.11b} disable network

b. Specify the aggregation method entering this command:

    config {802.11a | 802.11b} 11nsupport a-mpdu tx priority {0-7 | all} {enable | disable}

Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). Both A-MPDU and A-MSDU are performed in the software.

You can specify the aggregation method for various types of traffic from the access point to the clients. Table 4-2 defines the priority levels (0-7) assigned per traffic type.

<table>
<thead>
<tr>
<th>User Priority</th>
<th>Traffic Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Best effort</td>
</tr>
<tr>
<td>1</td>
<td>Background</td>
</tr>
<tr>
<td>2</td>
<td>Spare</td>
</tr>
<tr>
<td>3</td>
<td>Excellent effort</td>
</tr>
<tr>
<td>4</td>
<td>Controlled load</td>
</tr>
<tr>
<td>5</td>
<td>Video, less than 100-ms latency and jitter</td>
</tr>
<tr>
<td>6</td>
<td>Voice, less than 10-ms latency and jitter</td>
</tr>
<tr>
<td>7</td>
<td>Network control</td>
</tr>
</tbody>
</table>

You can configure each priority level independently, or you can use the all parameter to configure all of the priority levels at once. When you use the enable command, the traffic associated with that priority level uses A-MPDU transmission. When you use the disable command, the traffic associated with that priority level uses A-MSDU transmission. Configure the priority levels to match the aggregation method used by the clients. By default, A-MPDU is enabled for priority level 0, 4 and 5 and the rest are disabled. By default, A-MPDU is enabled for all priorities except 6 and 7.

c. Reenable the network by entering this command:

    config {802.11a | 802.11b} enable network

Step 5 Configure the 802.11n-5 GHz A-MPDU transmit aggregation scheduler by entering this command:

    config 802.11{a | b} 11nsupport a-mpdu tx scheduler {enable | disable | timeout rt timeout-value}

The timeout value is in milliseconds. The valid range is between 1 millisecond to 1000 milliseconds.

Step 6 Configure the guard interval for the network by entering this command:

    config 802.11{a | b} 11nsupport guard-interval {any | long}

Step 7 Configure the Reduced Interframe Space (RIFS) for the network by entering this command:

    config 802.11{a | b} 11nsupport rifs rx {enable | disable}

Step 8 Enter the save config command to save your configuration.

Step 9 View the configuration settings for the 802.11a/n or 802.11b/g/n band by entering this command:

    show {802.11a | 802.11b}

Information similar to the following appears:

    802.11a Network........................................ Enabled
11nSupport................................. Enabled
802.11a Low Band.......................... Enabled
802.11a Mid Band.......................... Enabled
802.11a High Band.......................... Enabled

802.11a Operational Rates
802.11a 6M Rate.............................. Mandatory
802.11a 9M Rate.............................. Supported
802.11a 12M Rate............................. Mandatory
802.11a 18M Rate............................. Supported
802.11a 24M Rate............................. Mandatory
802.11a 36M Rate............................. Supported
802.11a 48M Rate............................. Supported
802.11a 54M Rate............................. Supported

802.11n MCS Settings:
MCS 0........................................ Supported
MCS 1........................................ Supported
MCS 2........................................ Supported
MCS 3........................................ Supported
MCS 4........................................ Supported
MCS 5........................................ Supported
MCS 6........................................ Supported
MCS 7........................................ Supported
MCS 8........................................ Supported
MCS 9........................................ Supported
MCS 10....................................... Supported
MCS 11....................................... Supported
MCS 12....................................... Supported
MCS 13....................................... Supported
MCS 14....................................... Supported
MCS 15....................................... Supported

802.11n Status:
A-MPDU Tx.................................. Enabled
Priority 0.................................... Enabled
Priority 1.................................... Enabled
Priority 2.................................... Enabled
Priority 3.................................... Enabled
Priority 4.................................... Enabled
Priority 5.................................... Disabled
Priority 6.................................... Disabled
Priority 7.................................... Enabled
A-MSDU Tx.................................. Enabled
Rifs Tx....................................... Enabled
Guard Interval............................... Short
Beacon Interval............................... 100
CF Pollable mandatory....................... Disabled
CF Poll Request mandatory.................... Disabled
CFP Period.................................... 4
CFP Maximum Duration....................... 60
Default Channel............................. 36
Default Tx Power Level....................... 1
DTPC Status.................................. Enabled
Fragmentation Threshold..................... 2346
Long Retry Limit............................ 4
Maximum Rx Life Time....................... 512
Max Tx MSDU Life Time...................... 512
Medium Occupancy Limit.................... 100
RTS Threshold............................... 2347
Short Retry Limit........................... 7
TI Threshold................................. -50
Traffic Stream Metrics Status................ Enabled
Expedited BW Request Status................ Disabled
EDCA profile type.......................... default-wmm
Voice MAC optimization status............... Disabled
Call Admission Control (CAC) configuration
Configuring 802.11h Parameters

This section contains the following topics:

- Information About Configuring 802.11h Parameters, page 4-34
- Configuring 802.11h Parameters, page 4-34

Information About Configuring 802.11h Parameters

802.11h informs client devices about channel changes and can limit the transmit power of those client devices.

Configuring 802.11h Parameters

This section contains the following topics:

- Configuring 802.11h Parameters (GUI), page 4-34
- Configuring 802.11h Parameters (CLI), page 4-35

Configuring 802.11h Parameters (GUI)

Step 1  Disable the 802.11a band as follows:

a. Choose Wireless > 802.11a/n > Network to open the 802.11a Global Parameters page.

b. Unselect the 802.11a Network Status check box.

c. Click Apply to commit your change.

Step 2  Choose Wireless > 802.11a/n > DFS (802.11h) to open the 802.11h Global Parameters page.
Figure 4-9  802.11h Global Parameters Page

Step 3  Select the **Channel Announcement** check box if you want the access point to announce when it is switching to a new channel and the new channel number, or unselect this check box to disable the channel announcement. The default value is disabled.

Step 4  If you enabled the channel announcement in **Step 3**, the **Channel Quiet Mode** check box appears. Select this check box if you want the access point to stop transmitting on the current channel, or unselect this check box to disable quiet mode. The default value is disabled.

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

Step 6  Reenable the 802.11a band as follows:
   a.  Choose **Wireless > 802.11a/n > Network** to open the 802.11a Global Parameters page.
   b.  Select the **802.11a Network Status** check box.
   c.  Click **Apply** to commit your change.

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

**Configuring 802.11h Parameters (CLI)**

Step 1  Disable the 802.11a network by entering this command:
   \[ \texttt{config 802.11a disable network} \]

Step 2  Enable or disable the access point to announce when it is switching to a new channel and the new channel number by entering this command:
   \[ \texttt{config 802.11h channelswitch \{ enable | disable \} switch\_mode} \]
   You can enter a 0 or 1 for the switch\_mode parameter to specify whether transmissions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled.

Step 3  Configure a new channel using the 802.11h channel announcement by entering this command:
   \[ \texttt{config 802.11h setchannel channel channel} \]

Step 4  Configure the 802.11h power constraint value by entering this command:
   \[ \texttt{config 802.11h powerconstraint value} \]
The default value for the value parameter is 3 dB.

Step 5
Reenable the 802.11a network by entering this command:
```
config 802.11a enable network
```

Step 6
See the status of 802.11h parameters by entering this command:
```
show 802.11h
```

Information similar to the following appears:
```
Power Constraint......................... 0
Channel Switch.......................... Disabled
Channel Switch Mode.................... 0
```

## Configuring DHCP Proxy

This section contains the following topics:
- Information About Configuring DHCP Proxy, page 4-36
- Guidelines and Limitations, page 4-36
- Configuring DHCP Proxy, page 4-37

### Information About Configuring DHCP Proxy

When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself.

When DHCP proxy is disabled on the controller, those DHCP packets transmitted to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are removed from the CAPWAP tunnel and transmitted on the upstream VLAN. DHCP packets directed to the client are received on the upstream VLAN, converted to 802.11, and transmitted through a CAPWAP tunnel toward the client. As a result, the internal DHCP server cannot be used when DHCP proxy is disabled. The ability to disable DHCP proxy allows organizations to use DHCP servers that do not support Cisco’s native proxy mode of operation. It should be disabled only when required by the existing infrastructure.

### Guidelines and Limitations

- DHCP proxy is enabled by default.
- DHCP proxy must be enabled in order for DHCP option 82 to operate correctly.
- All controllers that will communicate must have the same DHCP proxy setting.

**Note**

For information about configuring DHCP servers, see Chapter 8, “Working with WLANs.”
Configuring DHCP Proxy

This section contains the following topics:

- Configuring DHCP Proxy (GUI), page 4-37
- Configuring DHCP Proxy (CLI), page 4-37
- Configuring DHCP Timeout (GUI), page 4-37
- Configuring DHCP Timeout (CLI), page 4-38

Configuring DHCP Proxy (GUI)

**Step 1** Choose Controller > Advanced > DHCP to open the DHCP Parameters page.

**Figure 4-10 DHCP Parameters Page**

**Step 2** Select the Enable DHCP Proxy check box to enable DHCP proxy on a global basis. Otherwise, unselect the check box. The default value is selected.

**Step 3** Click Apply to commit your changes.

**Step 4** Click Save Configuration to save your changes.

Configuring DHCP Proxy (CLI)

**Step 1** Enable or disable DHCP proxy by entering this command:

```
config dhcp proxy {enable | disable}
```

**Step 2** View the DHCP proxy configuration by entering this command:

```
show dhcp proxy
```

Information similar to the following appears:

```
DHCP Proxy Behavior: enabled
```

Configuring DHCP Timeout (GUI)

**Step 1** Choose Controller > Advanced > DHCP to open the DHCP Parameters page.

**Step 2** Select the DHCP Timeout (5 - 120 seconds) check box to enable a DHCP timeout on a global basis. Otherwise, unselect the check box. The valid range is 5 through 120 seconds.

**Step 3** Click Apply to commit your changes.
**Step 4**  
Click **Save Configuration** to save your changes.

---

### Configuring DHCP Timeout (CLI)

To configure a DHCP timeout using the controller CLI, use the following command:

```
config dhcp timeout seconds
```

### Configuring Administrator Usernames and Passwords

This section contains the following topics:

- Information About Configuring Administrator Usernames and Passwords, page 4-38
- Configuring Usernames and Passwords, page 4-38

### Information About Configuring Administrator Usernames and Passwords

You can configure administrator usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information. This section provides instructions for initial configuration and for password recovery.

### Configuring Usernames and Passwords

This section contains the following topics:

- Configuring Usernames and Passwords (CLI), page 4-38
- Restoring Passwords (CLI), page 4-39

### Configuring Usernames and Passwords (CLI)

**Step 1**  
Configure a username and password by entering one of these commands:

- `config mgmtuser add username password read-write`—Creates a username-password pair with read-write privileges.
- `config mgmtuser add username password read-only`—Creates a username-password pair with read-only privileges.

Usernames and passwords are case-sensitive and can contain up to 24 ASCII characters. Usernames and passwords cannot contain spaces.

**Note**  
If you ever need to change the password for an existing username, enter the `config mgmtuser password username new_password` command.

**Step 2**  
List the configured users by entering this command:
show mgmtuser

Restoring Passwords (CLI)

Step 1  After the controller boots up, enter **Restore-Password** at the User prompt.

*Note*  For security reasons, the text that you enter does not appear on the controller console.

Step 2  At the Enter User Name prompt, enter a new username.

Step 3  At the Enter Password prompt, enter a new password.

Step 4  At the Re-enter Password prompt, reenter the new password. The controller validates and stores your entries in the database.

Step 5  When the User prompt reappears, enter your new username.

Step 6  When the Password prompt appears, enter your new password. The controller logs you in with your new username and password.

Configuring SNMP

This section contains the following topic:

- Configuring SNMP (CLI), page 4-39

Configuring SNMP (CLI)

Step 1  Enter the `config snmp community create name` command to create an SNMP community name.

Step 2  Enter the `config snmp community delete name` command to delete an SNMP community name.

Step 3  Enter the `config snmp community accessmode ro name` command to configure an SNMP community name with read-only privileges. Enter `config snmp community accessmode rw name` to configure an SNMP community name with read-write privileges.

Step 4  Enter the `config snmp community ipaddr ip-address ip-mask name` command to configure an IP address and subnet mask for an SNMP community.

*Note*  This command behaves like an SNMP access list. It specifies the IP address from which the device accepts SNMP packets with the associated community. An AND operation is performed between the requesting entity’s IP address and the subnet mask before being compared to the IP address. If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches to all IP addresses. The default value is 0.0.0.0.
SNMP Community Strings

This section contains the following topics:

- Information About SNMP Community Strings, page 4-40
- Changing the SNMP Community String Default Values, page 4-41

Information About SNMP Community Strings

The controller has commonly known default values of “public” and “private” for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. If you use the default community names, and since these are known, the community names could be used to communicate to the controller using the SNMP protocol. Therefore, we strongly advise that you change these values.
Changing the SNMP Community String Default Values

This section contains the following topics:

- Changing the SNMP Community String Default Values (GUI), page 4-41
- Changing the SNMP Community String Default Values (CLI), page 4-41

Changing the SNMP Community String Default Values (GUI)

**Step 1** Choose **Management** and then **Communities** under SNMP. The SNMP v1 / v2c Community page appears.

**Figure 4-11  **SNMP v1 / v2c Community Page

<table>
<thead>
<tr>
<th>Community Name</th>
<th>IP Address</th>
<th>IP Mask</th>
<th>Access Mode</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>public</td>
<td>192.168.200.225</td>
<td>255.255.255.224</td>
<td>Read-Only</td>
<td>Enable</td>
</tr>
<tr>
<td>private</td>
<td>192.168.200.225</td>
<td>255.255.255.224</td>
<td>Read-Write</td>
<td>Enable</td>
</tr>
</tbody>
</table>

**Step 2** If “public” or “private” appears in the Community Name column, hover your cursor over the blue drop-down arrow for the desired community and choose **Remove** to delete this community.

**Step 3** Click **New** to create a new community. The SNMP v1 / v2c Community > New page appears.

**Step 4** In the Community Name text box, enter a unique name containing up to 16 alphanumeric characters. Do not enter “public” or “private.”

**Step 5** In the next two text boxes, enter the IP address from which this device accepts SNMP packets with the associated community and the IP mask.

**Step 6** Choose **Read Only** or **Read/Write** from the Access Mode drop-down list to specify the access level for this community.

**Step 7** Choose **Enable** or **Disable** from the Status drop-down list to specify the status of this community.

**Step 8** Click **Apply** to commit your changes.

**Step 9** Click **Save Configuration** to save your settings.

**Step 10** Repeat this procedure if a “public” or “private” community still appears on the SNMP v1 / v2c Community page.

Changing the SNMP Community String Default Values (CLI)

**Step 1** See the current list of SNMP communities for this controller by entering this command:

```
show snmp community
```

**Step 2** If “public” or “private” appears in the SNMP Community Name column, enter this command to delete this community:
**Changing the Default Values for SNMP v3 Users**

This section contains the following topics:

- Information About Changing the Default Values for SNMP v3 Users, page 4-42
- Changing the SNMP v3 User Default Values, page 4-42

**Information About Changing the Default Values for SNMP v3 Users**

The controller uses a default value of “default” for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values.

**Note**

SNMP v3 is time sensitive. Ensure that you configure the correct time and time zone on your controller.

**Changing the SNMP v3 User Default Values**

This section contains the following topics:

- Changing the SNMP v3 User Default Values (GUI), page 4-43
- Changing the SNMP v3 User Default Values (CLI), page 4-43

---

**Changing the Default Values for SNMP v3 Users**

The controller uses a default value of “default” for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values.

**Step 3**

Create a new community by entering this command:

```
config snmp community create name
```

Enter up to 16 alphanumeric characters for the `name` parameter. Do not enter “public” or “private.”

**Step 4**

Enter the IP address from which this device accepts SNMP packets with the associated community by entering this command:

```
config snmp community ipaddr ip_address ip_mask name
```

**Step 5**

Specify the access level for this community by entering this command, where `ro` is read-only mode and `rw` is read/write mode:

```
config snmp community accessmode {ro | rw} name
```

**Step 6**

Enable or disable this SNMP community by entering this command:

```
config snmp community mode {enable | disable} name
```

**Step 7**

Save your changes by entering `save config`.

**Step 8**

Repeat this procedure if you still need to change the default values for a “public” or “private” community string.
Changing the SNMP v3 User Default Values (GUI)

**Step 1** Choose **Management > SNMP > SNMP V3 Users** to open the SNMP V3 Users page.

**Figure 4-12 SNMP V3 Users Page**

<table>
<thead>
<tr>
<th>User Name</th>
<th>Access Level</th>
<th>Auth Protocol</th>
<th>Privacy Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>ReadWrite</td>
<td>HMAC-Sha</td>
<td>AES</td>
</tr>
</tbody>
</table>

**Step 2** If “default” appears in the User Name column, hover your cursor over the blue drop-down arrow for the desired user and choose **Remove** to delete this SNMP v3 user.

**Step 3** Click **New** to add a new SNMP v3 user. The SNMP V3 Users > New page appears.

**Step 4** In the User Profile Name text box, enter a unique name. Do not enter “default.”

**Step 5** Choose **Read Only** or **Read Write** from the Access Mode drop-down list to specify the access level for this user. The default value is Read Only.

**Step 6** From the Authentication Protocol drop-down list, choose the desired authentication method: **None**, **HMAC-MD5** (Hashed Message Authentication Coding-Message Digest 5), or **HMAC-SHA** (Hashed Message Authentication Coding-Secure Hashing Algorithm). The default value is HMAC-SHA.

**Step 7** In the Auth Password and Confirm Auth Password text boxes, enter the shared secret key to be used for authentication. You must enter at least 12 characters.

**Step 8** From the Privacy Protocol drop-down list, choose the desired encryption method: **None**, **CBC-DES** (Cipher Block Chaining-Digital Encryption Standard), or **CFB-AES-128** (Cipher Feedback Mode-Advanced Encryption Standard-128). The default value is CFB-AES-128.

**Note** In order to configure CBC-DES or CFB-AES-128 encryption, you must have selected either HMAC-MD5 or HMAC-SHA as the authentication protocol in **Step 6**.

**Step 9** In the Priv Password and Confirm Priv Password text boxes, enter the shared secret key to be used for encryption. You must enter at least 12 characters.

**Step 10** Click **Apply** to commit your changes.

**Step 11** Click **Save Configuration** to save your settings.

**Step 12** Reboot the controller so that the SNMP v3 user that you added takes effect.

Changing the SNMP v3 User Default Values (CLI)

**Step 1** See the current list of SNMP v3 users for this controller by entering this command:

```
show snmpv3user
```
Configuring Aggressive Load Balancing

This section contains the following topics:
- Information About Configuring Aggressive Load Balancing, page 4-44
- Guidelines and Limitations, page 4-45
- Configuring Aggressive Load Balancing, page 4-46

Information About Configuring Aggressive Load Balancing

Enabling aggressive load balancing on the controller allows lightweight access points to load balance wireless clients across access points. You can enable aggressive load balancing using the controller.

Note

Clients are load balanced between access points on the same controller. Load balancing does not occur between access points on different controllers.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. This code indicates whether the access point can accept any more associations. If the access point is too busy, the client attempts to associate to a different access point in the area. The system determines if an access point is relatively more busy than its neighbor access points that are also accessible to the client.
For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it would be allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

Note: Cisco Aironet 600 OfficeExtend Access Points and FlexConnect access points do not support client load balancing.

Guidelines and Limitations

- **Client Association Limits**—The maximum number of client associations that the access points can support is dependent upon the following factors:
  - The maximum number of client associations differs for lightweight and autonomous Cisco IOS access points.
  - There may be a limit per radio and an overall limit per AP.
  - AP hardware (the 16-MB APs have a lower limit than the 32-MB and higher APs)

- **Client Association Limits for Lightweight Access Points**—The Per-AP limits are as follows:
  - For 16-MB APs, the limit is 128 clients per AP. This limit is applicable to 1100 and 1200 series APs.
  - For 32-MB and higher APs, there is no per-AP limit.

  The per-radio limits are as follows:
  - For all Cisco IOS APs, the limit is 200 associations per radio.
  - For all 1000 and 1500 series APs, which are not supported beyond release 4.2, the limit is 250 associations per radio.

  Note: With 32-MB and higher lightweight Cisco IOS APs, with two radios, up to 200 + 200 = 400 associations are supported.

- **Client Association Limits for Autonomous Cisco IOS Access Points**—The limit is around 80 to 127 clients per AP. This number varies depending on the following factors:
  - AP model (whether it is 16 MB or 32 MB or higher)
  - Cisco IOS version
  - Hardware configuration (two radios use more memory than one)
  - Enabled features (WDS functionality in particular)

  The per-radio limit is about 200 associations. One association will likely hit the per-AP limit first.
Note
Unlike Cisco Unified Wireless Network, autonomous Cisco IOS supports per-SSID/per-AP association limits. This limit is configured using the max-associations CLI, under dot11 SSID. The maximum number is 255 associations (which is also the default number).

Configuring Aggressive Load Balancing

This section contains the following topics:

- Configuring Aggressive Load Balancing (GUI), page 4-46
- Configuring Aggressive Load Balancing (CLI), page 4-47

Configuring Aggressive Load Balancing (GUI)

Step 1
Choose Wireless > Advanced > Load Balancing to open the Load Balancing page.

Figure 4-13 Wireless > Advanced > Load Balancing Page

Step 2
In the Client Window Size text box, enter a value between 1 and 20. The window size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

\[
\text{load-balancing window} + \text{client associations on AP with highest load} = \text{load-balancing threshold}
\]

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client window size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.
Step 3  In the Maximum Denial Count text box, enter a value between 0 and 10. The denial count sets the maximum number of association denials during load balancing.

Step 4  Click **Apply** to commit your changes.

Step 5  Click **Save Configuration** to save your changes.

Step 6  To enable or disable aggressive load balancing on specific WLANs, choose WLANs > WLAN ID. The WLANs > Edit page appears.

Step 7  Click the **Advanced** tab.

Step 8  Click **Apply** to commit your changes.

Step 9  Click **Save Configuration** to save your settings

---

## Configuring Aggressive Load Balancing (CLI)

Step 1  Set the client window for aggressive load balancing by entering this command:

```
config load-balancing window client_count
```

You can enter a value between 0 and 20 for the `client_count` parameter.

Step 2  Set the denial count for load balancing by entering this command:

```
config load-balancing denial denial_count
```

You can enter a value between 1 and 10 for the `denial_count` parameter.

Step 3  Save your changes by entering this command:

```
save config
```

Step 4  Enable or disable aggressive load balancing on specific WLANs by entering this command:

```
config wlan load-balance allow {enable | disable} wlan_ID
```

You can enter a value between 1 and 512 for `wlan_ID` parameter.

Step 5  Verify your settings by entering this command:

```
show load-balancing
```

Information similar to the following appears:

```
Aggressive Load Balancing......................... Enabled
Aggressive Load Balancing Window...............  1 clients
Aggressive Load Balancing Denial Count........  3

Statistics
Total Denied Count...............................  5 clients
Total Denial Sent...............................  10 messages
Exceeded Denial Max Limit Count.................  0 times
None 5G Candidate Count.......................  0 times
None 2.4G Candidate Count.....................  0 times
```

Step 6  Save your changes by entering this command:

```
save config
```
Configuring Band Selection

This section contains the following topics:

- Information About Configuring Band Selection, page 4-48
- Guidelines and Limitations, page 4-48
- Configuring Band Selection, page 4-48

Information About Configuring Band Selection

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three nonoverlapping channels. To combat these sources of interference and improve overall network performance, you can configure band selection on the controller.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

Guidelines and Limitations

- Band selection is enabled globally by default.
- Band-selection enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.
- Band selection can be used only with Cisco Aironet 1040, 1140, 1250, 1260, 3500, and the 3600 series access points.
- Band selection operates only on access points that are connected to a controller. A flexconnect access point without a controller connection does not perform band selection after a reboot.

Note

OEAP 600 Series access points do not support band select.

- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.
- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.

Configuring Band Selection

This section contains the following topics:

- Configuring Band Selection (GUI), page 4-49
- Configuring Band Selection (CLI), page 4-50
Configuring Band Selection (GUI)

**Step 1** Choose **Wireless > Advanced > Band Select** to open the Band Select page.

**Figure 4-14 Wireless > Advanced > Band Select Page**

**Step 2** In the Probe Cycle Count text box, enter a value between 1 and 10. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

**Step 3** In the Scan Cycle Period Threshold (milliseconds) text box, enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.

**Step 4** In the Age Out Suppression (seconds) text box, enter a value between 10 and 200 seconds. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

**Step 5** In the Age Out Dual Band (seconds) text box, enter a value between 10 and 300 seconds. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

**Step 6** In the Acceptable Client RSSI (dBm) text box, enter a value between –20 and –90 dBm. This parameter sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

**Step 7** Click **Apply** to commit your changes.

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

**Step 9** To enable or disable aggressive load balancing on specific WLANs, choose **WLANs > WLAN ID**. The WLANs > Edit page appears.

**Step 10** Click the **Advanced** tab.

**Step 11** Click **Save Configuration** to save your changes.
Configuring Band Selection (CLI)

Step 1  Set the probe cycle count for band select by entering this command:

```plaintext
config band-select cycle-count cycle_count
```
You can enter a value between 1 and 10 for the `cycle_count` parameter.

Step 2  Set the time threshold for a new scanning cycle period by entering this command:

```plaintext
config band-select cycle-threshold milliseconds
```
You can enter a value for threshold between 1 and 1000 for the `milliseconds` parameter.

Step 3  Set the suppression expire to the band select by entering this command:

```plaintext
config band-select expire suppression seconds
```
You can enter a value for suppression between 10 to 200 for the `seconds` parameter.

Step 4  Set the dual band expire by entering this command:

```plaintext
config band-select expire dual-band seconds
```
You can enter a value for dual band between 10 and 300 for the `seconds` parameter.

Step 5  Set the client RSSI threshold by entering this command:

```plaintext
config band-select client-rssi client_rssi
```
You can enter a value for minimum dBm of a client RSSI to respond to a probe between 20 and 90 for the `client_rssi` parameter.

Step 6  Enter the `save config` command to save your changes.

Step 7  Enable or disable band selection on specific WLANs by entering this command:

```plaintext
config wlan band-select allow {enable | disable} wlan_ID
```
You can enter a value between 1 and 512 for `wlan_ID` parameter.

Step 8  Verify your settings by entering this command:

```plaintext
show band-select
```
Information similar to the following appears:

```
Band Select Probe Response....................... Enabled
Cycle Count................................... 3 cycles
Cycle Threshold............................... 300 milliseconds
Age Out Suppression........................... 20 seconds
Age Out Dual Band............................. 20 seconds
Client RSSI................................... -30 dBm
```

Step 9  Save your changes by entering this command:

```plaintext
save config
```

Configuring Fast SSID Changing

This section contains the following topics:

- Information About Configuring Fast SSID Changing, page 4-51
- Configuring Fast SSID, page 4-51
Information About Configuring Fast SSID Changing

When fast SSID changing is enabled, the controller allows clients to move between SSIDs. When the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID. When fast SSID changing is disabled, the controller enforces a delay before clients are allowed to move to a new SSID.

Configuring Fast SSID

This section contains the following topics:

- Configuring Fast SSID Changing (GUI), page 4-51
- Configuring Fast SSID Changing (CLI), page 4-51

Configuring Fast SSID Changing (GUI)

Step 1. Choose Controller to open the General page.

Step 2. From the Fast SSID Change drop-down list, choose Enabled to enable this feature or Disabled to disable it. The default value is disabled.

Step 3. Click Apply to commit your changes.

Step 4. Click Save Configuration to save your changes.

Configuring Fast SSID Changing (CLI)

Step 1. Enable or disable fast SSID changing by entering this command:

```bash
config network fast-ssid-change {enable | disable}
```

Step 2. Enter the save config command to save your settings.

Enabling 802.3X Flow Control

802.3X Flow Control is disabled by default. To enable it, enter the `config switchconfig flowcontrol enable` command.

Configuring 802.3 Bridging

This section contains the following topics:

- Information About Configuring 802.3 Bridging, page 4-52
- Guidelines and Limitations, page 4-52
- Configuring 802.3 Bridging, page 4-52
Information About Configuring 802.3 Bridging

The controller supports 802.3 frames and the applications that use them, such as those typically used for cash registers and cash register servers. However, to make these applications work with the controller, the 802.3 frames must be bridged on the controller.

Guidelines and Limitations

- Support for raw 802.3 frames allows the controller to bridge non-IP frames for applications not running over IP. Only this raw 802.3 frame format is currently supported:

  +-------------------+---------------------+-----------------+------------------------+
  | Destination     | Source              | Total packet | Payload ..... |
  | MAC address   | MAC address    | length           |            |
  +-------------------+---------------------+-----------------+------------------------+

- You can configure 802.3 bridging through the controller GUI in software release 4.1 or later releases and through the controller CLI in software release 4.0 or later releases.

- In controller software release 5.2 or later releases, the software-based forwarding architecture for 2100-series-based controllers is being replaced with a new forwarding plane architecture. As a result, Cisco 2100 Series Controller and the Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers (as well as Cisco 5500 Series Controllers) bridge 802.3 packets by default. Therefore, 802.3 bridging can now be disabled only on 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch.

- By default, Cisco 2100 Series Controllers that run software release 5.2 or later releases and Cisco 5500 Series Controllers bridge all non-IPv4 packets (such as AppleTalk, and so on). If desired, you can use ACLs to block the bridging of these protocols.

- You can also configure 802.3 bridging using the Cisco Wireless Control System (WCS). See the Cisco Wireless Control System Configuration Guide for instructions.

Configuring 802.3 Bridging

This section contains the following topics:

- Configuring 802.3 Bridging (GUI), page 4-52
- Configuring 802.3 Bridging (CLI), page 4-53

Configuring 802.3 Bridging (GUI)

Step 1  Choose Controller > General to open the General page.
Step 2  From the 802.3 Bridging drop-down list, choose Enabled to enable 802.3 bridging on your controller or Disabled to disable this feature. The default value is Disabled.

Note In controller software release 5.2 or later releases, you can disable 802.3 bridging only for 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch.

Step 3  Click Apply to commit your changes.

Step 4  Click Save Configuration to save your changes.

Configuring 802.3 Bridging (CLI)

Step 1  See the current status of 802.3 bridging for all WLANs by entering this command:

```
show network
```

Step 2  Enable or disable 802.3 bridging globally on all WLANs by entering this command:

```
config network 802.3-bridging {enable | disable}
```

The default value is disabled.

Note In controller software release 5.2 or later releases, you can disable 802.3 bridging only for 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch.

Step 3  Enter the save config command to save your settings.
Chapter 4 Configuring Controller Settings

Configuring Multicast Mode

This section contains the following topics:

- Information About Configuring Multicast Mode, page 4-54
- Guidelines and Limitations, page 4-55
- Configuring Multicast Mode, page 4-56

Information About Configuring 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.

The controller supports Multicast Listener Discovery (MLD) v1 snooping for IPv6 multicast. This feature keeps track of and delivers IPv6 multicast flows to the clients that request them. To support IPv6 multicast, you must enable Global Multicast Mode.

In controller software release 4.2 or later releases, Internet Group Management Protocol (IGMP) snooping is introduced to better direct multicast packets. When this feature is enabled, the controller gathers IGMP reports from the clients, processes them, creates unique multicast group IDs (MGIDs) from the IGMP reports after selecting the Layer 3 multicast address and the VLAN number, and sends the IGMP reports to the infrastructure switch. The controller sends these reports with the source address as the interface address on which it received the reports from the clients. The controller then updates the access point MGID table on the access point with the client MAC address. When the controller receives multicast traffic for a particular multicast group, it forwards it to all the access points, but only those access points that have active clients listening or subscribed to that multicast group send multicast traffic on that particular WLAN. IP packets are forwarded with an MGID that is unique for an ingress VLAN and the destination multicast group. Layer 2 multicast packets are forwarded with an MGID that is unique for the ingress interface.

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 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.

If Layer 2 multicast is enabled, a single MGID is assigned to all the multicast addresses coming from an interface.

**Guidelines and Limitations**

- The Cisco Unified Wireless Network solution uses some IP address ranges for specific purposes, and you should keep these ranges in mind when configuring a multicast group:
  - 224.0.0.0 through 224.0.0.255—Reserved link local addresses
  - 224.0.1.0 through 238.255.255.255—Globally scoped addresses
  - 239.0.0.0 through 239.255.x.y /16—Limited scope addresses
- When you enable multicast mode on the controller, you also must configure a CAPWAP multicast group address. Access points subscribe to the CAPWAP multicast group using IGMP.
- Cisco 1100, 1130, 1200, 1230, and 1240 access points use IGMP versions 1, 2, and 3.
- Access points in monitor mode, sniffer mode, or rogue detector mode do not join the CAPWAP multicast group address.
- The CAPWAP multicast group configured on the controllers should be different for different controllers.
- Multicast mode does not operate across intersubnet mobility events such as guest tunneling. It does, however, operate with interface overrides using RADIUS (but only when IGMP snooping is enabled) and with site-specific VLANs (access point group VLANs).
- For LWAPP, the controller drops multicast packets sent to UDP control port 12223. For CAPWAP, the controller drops multicast packets sent to UDP control and data ports 5246 and 5247, respectively. Therefore, you may want to consider not using these port numbers with the multicast applications on your network.
• We recommend that any multicast applications on your network not use the multicast address configured as the CAPWAP multicast group address on the controller.

• Cisco 2100 Series Controllers do not support multicast-unicast mode. They do, however, support multicast-multicast mode, except when access points are connected directly to the local port of a 2100 series controller.

• For multicast to work on 2500 series controller, you have to configure the multicast IP address.

• Multicast mode is not supported on Cisco Flex 7500 Series Controllers.

Configuring Multicast Mode

This section contains the following topics:
• Enabling Multicast Mode (GUI), page 4-56
• Enabling Multicast Mode (CLI), page 4-57
• Viewing Multicast Groups (GUI), page 4-58
• Viewing Multicast Groups (CLI), page 4-58
• Viewing an Access Point’s Multicast Client Table (CLI), page 4-59

Enabling Multicast Mode (GUI)

Step 1 Choose Controller > Multicast to open the Multicast page.

Figure 4-16 Multicast Page

Step 2 Select 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, select the Enable IGMP Snooping check box. If you want to disable IGMP snooping, leave the check box unselected. 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 \( \text{timeout} / 3 \) 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).

Step 6  Select 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 7  In the MLD Timeout text box, enter a value between 30 and 7200 seconds to set the MLD timeout.

Step 8  Enter the MLD Query Interval (seconds). The range is from 15 to 2400 seconds.

Step 9  Click Apply to commit your changes.

Step 10  Click Save Configuration to save your changes.

Enabling Multicast Mode (CLI)

Step 1  Enable or disable multicasting on the controller by entering this command:

```
config network multicast global {enable | disable}
```

The default value is disabled.

Note  The config network broadcast {enable | disable} command allows you to enable or disable broadcasting without enabling or disabling multicasting as well. This command uses the multicast mode currently on the controller to operate.

Step 2  Perform either of the following:

a. Configure the controller to use the unicast method to send multicast packets by entering this command:

```
config network multicast mode unicast
```

b. Configure the controller to use the multicast method to send multicast packets to a CAPWAP multicast group by entering this command:

```
config network multicast mode multicast multicast_group_ip_address
```

Step 3  Enable or disable IGMP snooping by entering this command:

```
config network multicast igmp snooping {enable | disable}
```

The default value is disabled.

Step 4  Set the IGMP timeout value by entering this command:

```
config network multicast igmp timeout timeout
```

You can enter a timeout value between 30 and 7200 seconds. 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  Enable or disable MLD Snooping by entering this command:
config network multicast mld snooping {enable | disable}
The default value is disabled.

**Note** To enable MLD Snooping, you must enable Global Multicast Mode of the controller.

**Step 6** Set the MLD timeout value by entering this command:
```plaintext
config network multicast mld timeout timeout
```
You can enter a `timeout` value between 30 and 7200 seconds.

**Step 7** Configure the Layer 2 multicast on an interface or all interfaces by entering this command:
```plaintext
config network multicast l2mcast {enable | disable} {all | interface-name}
```

**Step 8** Enter the `save config` command to save your settings.

---

**Viewing Multicast Groups (GUI)**

**Step 1** Choose Monitor > Multicast. The Multicast Groups page appears.

**Figure 4-17 Multicast Groups Page**

This page shows all the multicast groups and their corresponding MGIDs.

**Step 2** Click the link for a specific MGID (such as MGID 550) to see a list of all the clients joined to the multicast group in that particular MGID.

---

**Viewing Multicast Groups (CLI)**

- See all the multicast groups and their corresponding MGIDs by entering this command:
  ```plaintext
  show network multicast mgid summary
  ```
  Information similar to the following appears:
  ```plaintext
  Layer2 MGID Mapping:
  ----------------------
  InterfaceName        vlanId  MGID
  mgmt                  0       0
  test                  0       9
  wired                 20      8
  ```
### Configuring Client Roaming

This section contains the following topics:

- Information About Client Roaming, page 4-60
- Guidelines and Limitations, page 4-62
- Configuring CCX Client Roaming Parameters, page 4-62
Information About Client Roaming

The Cisco UWN Solution supports seamless client roaming across lightweight access points managed by the same controller, between controllers in the same mobility group on the same subnet, and across controllers in the same mobility group on different subnets. Also, in controller software release 4.1 or later releases, client roaming with multicast packets is supported.

You can adjust the default RF settings (RSSI, hysteresis, scan threshold, and transition time) to fine-tune the operation of client roaming using the controller GUI or CLI.

This section contains the following topics:

- Intra-Controller Roaming, page 4-60
- Inter-Controller Roaming, page 4-60
- Inter-Subnet Roaming, page 4-60
- Voice-over-IP Telephone Roaming, page 4-60
- CCX Layer 2 Client Roaming, page 4-61

Intra-Controller Roaming

Each controller supports same-controller client roaming across access points managed by the same controller. This roaming is transparent to the client as the session is sustained, and the client continues using the same DHCP-assigned or client-assigned IP address. The controller provides DHCP functionality with a relay function. Same-controller roaming is supported in single-controller deployments and in multiple-controller deployments.

Inter-Controller Roaming

Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group and on the same subnet. This roaming is also transparent to the client because the session is sustained and a tunnel between controllers allows the client to continue using the same DHCP- or client-assigned IP address as long as the session remains active. The tunnel is torn down, and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 169.254.*.* client auto-IP address or when the operator-set session timeout is exceeded.

Inter-Subnet Roaming

Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group on different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the controllers allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active. The tunnel is torn down, and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 169.254.*.* client auto-IP address or when the operator-set user timeout is exceeded.

Voice-over-IP Telephone Roaming

802.11 voice-over-IP (VoIP) telephones actively seek out associations with the strongest RF signal to ensure the best quality of service (QoS) and the maximum throughput. The minimum VoIP telephone requirement of 20-millisecond or shorter latency time for the roaming handover is easily met by the
Cisco UWN Solution, which has an average handover latency of 5 or fewer milliseconds when open authentication is used. This short latency period is controlled by controllers rather than allowing independent access points to negotiate roaming handovers.

The Cisco UWN Solution supports 802.11 VoIP telephone roaming across lightweight access points managed by controllers on different subnets, as long as the controllers are in the same mobility group. This roaming is transparent to the VoIP telephone because the session is sustained and a tunnel between controllers allows the VoIP telephone to continue using the same DHCP-assigned IP address as long as the session remains active. The tunnel is torn down, and the VoIP client must reauthenticate when the VoIP telephone sends a DHCP Discover with a 0.0.0.0 VoIP telephone IP address or a 169.254.*.* VoIP telephone auto-IP address or when the operator-set user timeout is exceeded.

**CCX Layer 2 Client Roaming**

The controller supports five CCX Layer 2 client roaming enhancements:

- **Access point assisted roaming**—This feature helps clients save scanning time. When a CCXv2 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client’s current SSID(s), and time elapsed since disassociation.

- **Enhanced neighbor list**—This feature focuses on improving a CCXv4 client’s roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.

- **Enhanced neighbor list request (E2E)**—The End-2-End specification is a Cisco and Intel joint program that defines new protocols and interfaces to improve the overall voice and roaming experience. It applies only to Intel clients in a CCX environment. Specifically, it enables Intel clients to request a neighbor list at will. When this occurs, the access point forwards the request to the controller. The controller receives the request and replies with the current CCX roaming sublist of neighbors for the access point to which the client is associated.

- **Roam reason report**—This feature enables CCXv4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.

- **Directed roam request**—This feature enables the controller to send directed roam requests to the client in situations when the controller can better service the client on an access point different from the one to which it is associated. In this case, the controller sends the client a list of the best access points that it can join. The client can either honor or ignore the directed roam request. Non-CCX clients and clients running CCXv3 or below must not take any action. No configuration is required for this feature.

---

**Note**

To see whether a particular client supports E2E, choose Wireless > Clients on the controller GUI, click the Detail link for the desired client, and look at the E2E Version text box under Client Properties.
Guidelines and Limitations

- Controller software release 4.2 or later releases support CCX versions 1 through 5. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to generate and respond to CCX frames appropriately. Clients must support CCXv4 or v5 (or CCXv2 for access point assisted roaming) in order to utilize these roaming enhancements. See the “Configuring Cisco Client Extensions” section on page 7-57 for more information on CCX.

The roaming enhancements mentioned above are enabled automatically, with the appropriate CCX support.

- FlexConnect access points in standalone mode do not support CCX Layer 2 roaming.

- Client roaming between 600 Series Access points is not supported.

Configuring CCX Client Roaming Parameters

This section contains the following topics:

- Configuring CCX Client Roaming Parameters (GUI), page 4-62
- Configuring CCX Client Roaming Parameters (CLI), page 4-63
- Obtaining CCX Client Roaming Information (CLI), page 4-64
- Debugging CCX Client Roaming Issues (CLI), page 4-64

Configuring CCX Client Roaming Parameters (GUI)

**Step 1** Choose **Wireless** > **802.11a/n** (or **802.11b/g/n**) > **Client Roaming.** The 802.11a (or 802.11b) > Client Roaming page appears.

**Figure 4-18 802.11a > Client Roaming Page**

- **Wireless:**
  - Access Points
  - Mesh
  - HREAP Groups
  - **802.11a/n**
    - Network
    - RAY
    - AP Cell
    - Client Roaming
    - Video

- **RF Parameters:**
  - **Mode**
  - Minimum RSSI
  - Hysteresis
  - Scan Threshold
  - Transition Time

**Step 2** If you want to fine-tune the RF parameters that affect client roaming, choose **Custom** from the Mode drop-down list and go to **Step 3**. If you want to leave the RF parameters at their default values, choose **Default** and go to **Step 8**.
Step 3  In the Minimum RSSI text box, enter a value for the minimum received signal strength indicator (RSSI) required for the client to associate to an access point. If the client’s average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

The range is –80 to –90 dBm.

The default is –85 dBm.

Step 4  In the Hysteresis text box, enter a value to indicate how much greater the signal strength of a neighboring access point must be in order for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points.

The range is 3 to 20 dB.

The default is 3 dB.

Step 5  In the Scan Threshold text box, enter the minimum RSSI that is allowed before the client should roam to a better access point. When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold.

The range is –70 to –77 dBm.

The default is –72 dBm.

Step 6  In the Transition Time text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client’s associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

The range is 1 to 10 seconds.

The default is 5 seconds.

Step 7  Click Apply to commit your changes.

Step 8  Click Save Configuration to save your changes.

Step 9  Repeat this procedure if you want to configure client roaming for another radio band (802.11a or 802.11b/g).

---

**Configuring CCX Client Roaming Parameters (CLI)**

Configure CCX Layer 2 client roaming parameters by entering this command:

```
config {802.11a | 802.11b} l2roam rf-params {default | custom min_rssi roam_hyst scan_thresh trans_time}
```

**Note**  See the description, range, and default value of each RF parameter in the “Configuring CCX Client Roaming Parameters” section on page 4-62.
Obtaining CCX Client Roaming Information (CLI)

**Step 1** View the current RF parameters configured for client roaming for the 802.11a or 802.11b/g network by entering this command:

```
show {802.11a | 802.11b} l2roam rf-param
```

**Step 2** View the CCX Layer 2 client roaming statistics for a particular access point by entering this command:

```
show {802.11a | 802.11b} l2roam statistics ap_mac
```

This command provides the following information:

- The number of roam reason reports received
- The number of neighbor list requests received
- The number of neighbor list reports sent
- The number of broadcast neighbor updates sent

**Step 3** View the roaming history for a particular client by entering this command:

```
show client roam-history client_mac
```

This command provides the following information:

- The time when the report was received
- The MAC address of the access point to which the client is currently associated
- The MAC address of the access point to which the client was previously associated
- The channel of the access point to which the client was previously associated
- The SSID of the access point to which the client was previously associated
- The time when the client disassociated from the previous access point
- The reason for the client roam

Debugging CCX Client Roaming Issues (CLI)

If you experience any problems with CCX Layer 2 client roaming, enter this command:

```
debg l2roam [detail | error | packet | all] {enable | disable}
```

Configuring IP-MAC Address Binding

This section contains the following topics:

- Information About Configuring IP-MAC Address Binding, page 4-65
- Configuring IP-MAC Address Binding (CLI), page 4-65
Information About Configuring IP-MAC Address Binding

In the controller software Release 5.2 or later releases, the controller enforces strict IP address-to-MAC address binding in client packets. The controller checks the IP address and MAC address in a packet, compares them to the addresses that are registered with the controller, and forwards the packet only if they both match. In previous releases, the controller checks only the MAC address of the client and ignores the IP address.

**Note**
If the IP address or MAC address of the packet has been spoofed, the check does not pass, and the controller discards the packet. Spoofed packets can pass through the controller only if both the IP and MAC addresses are spoofed together and changed to that of another valid client on the same controller.

Configuring IP-MAC Address Binding (CLI)

**Step 1**
Enable or disable IP-MAC address binding by entering this command:
```
config network ip-mac-binding {enable | disable}
```
The default value is enabled.

**Note**
You might want to disable this binding check if you have a routed network behind a workgroup bridge (WGB).

**Note**
You must disable this binding check in order to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller, a Cisco 2100 Series Controller, or a controller network module that runs software release 6.0 or later releases.

**Step 2**
Save your changes by entering this command:
```
save config
```

**Step 3**
View the status of IP-MAC address binding by entering this command:
```
show network summary
```
Information similar to the following appears:

```
RF-Network Name............................. ctrl4404
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High....... Disable
Secure Web Mode Cipher-Option SSLv2...... Enable
...
IP/MAC Addr Binding Check ............... Enabled
...
```
Configuring Quality of Service

This section contains the following topics:

- Information About Configuring Quality of Service Profiles, page 4-66
- Configuring Quality of Service Profiles, page 4-66

Information About Configuring Quality of Service Profiles

Quality of service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics.

The controller supports four QoS profiles:

- Platinum/Voice—Ensures a high quality of service for voice over wireless.
- Gold/Video—Supports high-quality video applications.
- Silver/Best Effort—Supports normal bandwidth for clients. This is the default setting.
- Bronze/Background—Provides the lowest bandwidth for guest services.

Note

VoIP clients should be set to Platinum.

You can configure the bandwidth of each QoS level using QoS profiles and then apply the profiles to WLANs. The profile settings are pushed to the clients associated to that WLAN. In addition, you can create QoS roles to specify different bandwidth levels for regular and guest users. Follow the instructions in this section to configure QoS profiles and QoS roles. You can also define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN.

Configuring Quality of Service Profiles

This section contains the following topics:

- Configuring QoS Profiles (GUI), page 4-66
- Configuring QoS Profiles (CLI), page 4-68

Configuring QoS Profiles (GUI)

Step 1
Disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles.

To disable the radio networks, choose Wireless > 802.11a/n or 802.11b/g/n > Network, unselect the 802.11a (or 802.11b/g) Network Status check box, and click Apply.

Step 2
Choose Wireless > QoS > Profiles to open the QoS Profiles page.

Step 3
Click the name of the profile that you want to configure to open the Edit QoS Profile page.
Step 4 Change the description of the profile by modifying the contents of the Description text box.

Step 5 Define the average data rate for TCP traffic per user by entering the rate in Kbps in the Average Data Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the profile.

Step 6 Define the peak data rate for TCP traffic per user by entering the rate in Kbps in the Burst Data Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the profile.

Note The Burst Data Rate should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 7 Define the average real-time rate for UDP traffic on a per-user basis by entering the rate in Kbps in the Average Real-Time Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the profile.

Note Average Data Rate is used to measure TCP traffic while Average Real-time rate is used for UDP traffic. They are measured in kbps for all the entries. The values for Average Data Rate and Average Real-time rate can be different because they are applied to different upper layer protocols such as TCP and UDP. These different values for the rates do not impact the bandwidth.

Step 8 Define the peak real-time rate for UDP traffic on a per-user basis by entering the rate in Kbps in the Burst Real-Time Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the profile.

Note The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.
Chapter 4  Configuring Controller Settings

Configuring Quality of Service

Step 9  Define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN as follows:

a. From the Maximum Priority drop-down list, choose the maximum QoS priority for any data frames transmitted by the AP to any station in the WLAN.
   
   For example, a QoS profile named ‘gold’ targeted for video applications has the maximum priority set to video by default.

b. From the Unicast Default Priority drop-down list, choose the QoS priority for unicast data frames transmitted by the AP to non-WMM stations in the WLAN.

c. From the Multicast Default Priority drop-down list, choose the QoS priority for multicast data frames transmitted by the AP to stations in the WLAN.

Note  You cannot use the default unicast priority for non-WMM clients in a mixed WLAN.

Step 10  Choose 802.1p from the Protocol Type drop-down list and enter the maximum priority value in the 802.1p Tag text box to define the maximum value (0–7) for the priority tag associated with packets that fall within the profile.

The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network.

Note  If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.

Step 11  Click Apply to commit your changes.

Step 12  Click Save Configuration to save your changes.

Step 13  Reenable the 802.11a and 802.11b/g networks.

To enable the radio networks, choose Wireless > 802.11a/n or 802.11b/g/n > Network, select the 802.11a (or 802.11b/g) Network Status check box, and click Apply.

Step 14  Follow the instructions in the “Assigning a QoS Profile to a WLAN” section on page 8-38 to assign a QoS profile to a WLAN.

Configuring QoS Profiles (CLI)

Step 1  Disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles by entering these commands:

  config 802.11a disable network
  config 802.11b disable network

Step 2  Change the profile description by entering this command:

  config qos description \{bronze | silver | gold | platinum\} description

Step 3  Define the average data rate in Kbps for TCP traffic per user by entering this command:

  config qos average-data-rate \{bronze | silver | gold | platinum\} rate
Chapter 4      Configuring Controller Settings

Configuring Quality of Service

Note
For the rate parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Step 4
Define the peak data rate in Kbps for TCP traffic per user by entering this command:

```
config qos burst-data-rate {bronze | silver | gold | platinum} rate
```

Step 5
Define the average real-time rate in Kbps for UDP traffic per user by entering this command:

```
config qos average-realtime-rate {bronze | silver | gold | platinum} rate
```

Step 6
Define the peak real-time rate in Kbps for UDP traffic per user by entering this command:

```
config qos burst-realtime-rate {bronze | silver | gold | platinum} rate
```

Step 7
Define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN by entering this command:

```
config qos priority {bronze | gold | platinum | silver} {maximum priority} {default unicast priority} {default multicast priority}
```

You choose from the following options for the maximum priority, default unicast priority, and default multicast priority parameters:

- besteffort
- background
- video
- voice

Step 8
Define the maximum value (0–7) for the priority tag associated with packets that fall within the profile, by entering these commands:

```
config qos protocol-type {bronze | silver | gold | platinum} dot1p
config qos dot1p-tag {bronze | silver | gold | platinum} tag
```

The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network.

Note
The 802.1p tagging has impact only on wired packets. Wireless packets are impacted only by the maximum priority level set for a QoS profile.

Note
If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.

Step 9
Reenable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles by entering these commands:

```
config 802.11a enable network
config 802.11b enable network
```

Step 10
Follow the instructions in the “Assigning a QoS Profile to a WLAN” section on page 8-38 to assign a QoS profile to a WLAN.
Configuring Quality of Service Roles

This section contains the following topics:

- Information About Configuring Quality of Service Roles, page 4-70
- Configuring QoS Roles, page 4-70

Information About Configuring Quality of Service Roles

After you configure a QoS profile and apply it to a WLAN, it limits the bandwidth level of clients associated to that WLAN. Multiple WLANs can be mapped to the same QoS profile, which can result in bandwidth contention between regular users (such as employees) and guest users. In order to prevent guest users from using the same level of bandwidth as regular users, you can create QoS roles with different (and presumably lower) bandwidth contracts and assign them to guest users.

You can configure up to ten QoS roles for guest users.

Note

If you choose to create an entry on the RADIUS server for a guest user and enable RADIUS authentication for the WLAN on which web authentication is performed rather than adding a guest user to the local user database from the controller, you need to assign the QoS role on the RADIUS server itself. To do so, a “guest-role” Airespace attribute needs to be added on the RADIUS server with a datatype of “string” and a return value of “11.” This attribute is sent to the controller when authentication occurs. If a role with the name returned from the RADIUS server is found configured on the controller, the bandwidth associated to that role is enforced for the guest user after authentication completes successfully.

Configuring QoS Roles

This section contains the following topics:

- Configuring QoS Roles (GUI), page 4-70
- Configuring QoS Roles (CLI), page 4-72

Configuring QoS Roles (GUI)

Note

Guest User role is not supported on Cisco 2106 Controller.

Step 1 Choose **Wireless > QoS > Roles** to open the QoS Roles for Guest Users page.
Step 2 Click **New** to create a new QoS role. The QoS Role Name > New page appears.

Step 3 In the Role Name text box, enter a name for the new QoS role. The name should uniquely identify the role of the QoS user (such as Contractor, Vendor, and so on).

Step 4 Click **Apply** to commit your changes.

Step 5 Click the name of the QoS role to edit the bandwidth of a QoS role. The Edit QoS Role Data Rates page appears.

**Note** The values that you configure for the per-user bandwidth contracts affect only the amount of bandwidth going downstream (from the access point to the wireless client). They do not affect the bandwidth for upstream traffic (from the client to the access point).

Step 6 Define the average data rate for TCP traffic on a per-user basis by entering the rate in Kbps in the Average Data Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Step 7 Define the peak data rate for TCP traffic on a per-user basis by entering the rate in Kbps in the Burst Data Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

**Note** The Burst Data Rate should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 8 Define the average real-time rate for UDP traffic on a per-user basis by entering the rate in Kbps in the Average Real-Time Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Step 9 Define the peak real-time rate for UDP traffic on a per-user basis by entering the rate in Kbps in the Burst Real-Time Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.
Note: The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 10 Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Step 12 Apply a QoS role to a guest user, by following the steps in the “Configuring Local Network Users on the Controller” section on page 7-27.

### Configuring QoS Roles (CLI)

Step 1 Create a QoS role for a guest user by entering this command:

```
config netuser guest-role create role_name
```

Note: If you want to delete a QoS role, enter the `config netuser guest-role delete role_name` command.

Step 2 Configure the bandwidth contracts for a QoS role by entering these commands:

- `config netuser guest-role qos data-rate average-data-rate role_name rate`—Configures the average data rate for TCP traffic on a per-user basis.
- `config netuser guest-role qos data-rate burst-data-rate role_name rate`—Configures the peak data rate for TCP traffic on a per-user basis.

Note: The Burst Data Rate should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

- `config netuser guest-role qos data-rate average-realtime-rate role_name rate`—Configures the average real-time rate for UDP traffic on a per-user basis.
- `config netuser guest-role qos data-rate burst-realtime-rate role_name rate`—Configures the peak real-time rate for UDP traffic on a per-user basis.

Note: The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Note: For the `role_name` parameter in each of these commands, enter a name for the new QoS role. The name should uniquely identify the role of the QoS user (such as Contractor, Vendor, and so on). For the `rate` parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Step 3 Apply a QoS role to a guest user by entering this command:

```
config netuser guest-role apply username role_name
```
For example, the role of *Contractor* could be applied to guest user *jsmith*.

---

**Note**

If you do not assign a QoS role to a guest user, the Role text box in the User Details shows the role as “default.” The bandwidth contracts for this user are defined in the QoS profile for the WLAN.

---

**Note**

If you want to unassign a QoS role from a guest user, enter the `config netuser guest-role apply username default` command. This user now uses the bandwidth contracts defined in the QoS profile for the WLAN.

---

**Step 4**

Save your changes by entering this command:

```
save config
```

**Step 5**

See a list of the current QoS roles and their bandwidth parameters by entering this command:

```
show netuser guest-roles
```

Information similar to the following appears:

```
Role Name............................... Contractor
  Average Data Rate..................... 10
  Burst Data Rate....................... 10
  Average Realtime Rate............... 100
  Burst Realtime Rate.................. 100

Role Name............................... Vendor
  Average Data Rate..................... unconfigured
  Burst Data Rate....................... unconfigured
  Average Realtime Rate............... unconfigured
  Burst Realtime Rate.................. unconfigured
```

---

## Configuring Voice and Video Parameters

This section contains the following topics:

- Information About Configuring Voice and Video Parameters, page 4-73
- Configuring Voice Parameters, page 4-77
- Configuring Video Parameters, page 4-80
- Viewing Voice and Video Settings, page 4-82
- Configuring Media Parameters (GUI), page 4-87

---

## Information About Configuring Voice and Video Parameters

Three parameters on the controller affect voice and/or video quality:

- Call admission control
- Expedited bandwidth requests
- Unscheduled automatic power save delivery
Each of these parameters is supported in Cisco Compatible Extensions (CCX) v4 and v5. See the “Configuring AP Groups” section on page 8-58 for more information on CCX.

Note

CCX is not supported on the AP1030.

Traffic stream metrics (TSM) can be used to monitor and report issues with voice quality.

This section contains the following topics:

- Call Admission Control, page 4-74
- Expedited Bandwidth Requests, page 4-75
- U-APSD, page 4-76
- Traffic Stream Metrics, page 4-76

Call Admission Control

Call admission control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi Multimedia (WMM) protocol deployed in CCXv3 ensures sufficient QoS as long as the wireless LAN is not congested. However, in order to maintain QoS under differing network loads, CAC in CCXv4 is required. Two types of CAC are available: bandwidth-based CAC and load-based CAC.

Bandwidth-Based CAC

Bandwidth-based, or static, CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new call and in turn enables the access point to determine whether it is capable of accommodating this particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

The QoS setting for a WLAN determines the level of bandwidth-based CAC support. To use bandwidth-based CAC with voice applications, the WLAN must be configured for Platinum QoS. To use bandwidth-based CAC with video applications, the WLAN must be configured for Gold QoS. Also, make sure that WMM is enabled for the WLAN. See the “Configuring 802.3 Bridging” section on page 4-51 for QoS and WMM configuration instructions.

Note

You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, bandwidth-based CAC does not operate properly.

Load-Based CAC

Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types (including that from clients), co-channel access point loads, and collocated channel interference, for voice applications. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

In load-based CAC, the access point continuously measures and updates the utilization of the RF channel (that is, the percentage of bandwidth that has been exhausted), channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents oversubscription of the channel and maintains QoS under all conditions of WLAN loading and interference.
Load-based CAC is supported only on lightweight access points. If you disable load-based CAC, the access points start using bandwidth-based CAC.

**Expedited Bandwidth Requests**

The expedited bandwidth request feature enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. When the controller receives this request, it attempts to facilitate the urgency of the call in any way possible without potentially altering the quality of other TSPEC calls that are in progress.

You can apply expedited bandwidth requests to both bandwidth-based and load-based CAC. Expedited bandwidth requests are disabled by default. When this feature is disabled, the controller ignores all expedited requests and processes TSPEC requests as normal TSPEC requests.

See Table 4-3 for examples of TSPEC request handling for normal TSPEC requests and expedited bandwidth requests.

<table>
<thead>
<tr>
<th>CAC Mode</th>
<th>Reserved bandwidth for voice calls¹</th>
<th>Usage²</th>
<th>Normal TSPEC Request</th>
<th>TSPEC with Expedited Bandwidth Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth-based CAC</td>
<td>75% (default setting)</td>
<td>Less than 75%</td>
<td>Admitted</td>
<td>Admitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Between 75% and 90% (reserved bandwidth for voice calls exhausted)</td>
<td>Rejected</td>
<td>Admitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>More than 90%</td>
<td>Rejected</td>
<td>Rejected</td>
</tr>
<tr>
<td>Load-based CAC</td>
<td></td>
<td>Less than 75%</td>
<td>Admitted</td>
<td>Admitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Between 75% and 85% (reserved bandwidth for voice calls exhausted)</td>
<td>Rejected</td>
<td>Admitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>More than 85%</td>
<td>Rejected</td>
<td>Rejected</td>
</tr>
</tbody>
</table>

1. For bandwidth-based CAC, the voice call bandwidth usage is per access point and does not take into account co-channel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.
2. Bandwidth-based CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

**Note**
Controller software release 6.0 or later releases support admission control for TSPEC g711-40ms codec type.

**Note**
When video ACM is enabled, the controller rejects a video TSPEC if the non-MSDU size in the TSPEC is greater than 149 or the mean data rate is greater than 1 Kbps.
U-APSD

Unscheduled automatic power save delivery (U-APSD) is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. U-APSD is enabled automatically when WMM is enabled.

Traffic Stream Metrics

In a voice-over-wireless LAN (VoWLAN) deployment, traffic stream metrics (TSM) can be used to monitor voice-related metrics on the client-access point air interface. It reports both packet latency and packet loss. You can isolate poor voice quality issues by studying these reports.

The metrics consist of a collection of uplink (client side) and downlink (access point side) statistics between an access point and a client device that supports CCX v4 or later releases. If the client is not CCX v4 or CCXv5 compliant, only downlink statistics are captured. The client and access point measure these metrics. The access point also collects the measurements every 5 seconds, prepares 90-second reports, and then sends the reports to the controller. The controller organizes the uplink measurements on a client basis and the downlink measurements on an access point basis and maintains an hour’s worth of historical data. To store this data, the controller requires 32 MB of additional memory for uplink metrics and 4.8 MB for downlink metrics.

TSM can be configured through either the GUI or the CLI on a per radio-band basis (for example, all 802.11a radios). The controller saves the configuration in flash memory so that it persists across reboots. After an access point receives the configuration from the controller, it enables TSM on the specified radio band.

Note
Access points support TSM entries in both local and FlexConnect modes.

Table 4-4 shows the upper limit for TSM entries in different controller series.

<table>
<thead>
<tr>
<th>TSM Entries</th>
<th>5500 Series Controller</th>
<th>7500 Series Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAX AP TSM entries</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>MAX Client TSM entries</td>
<td>250</td>
<td>250</td>
</tr>
<tr>
<td>MAX TSM entries</td>
<td>100*250=25000</td>
<td>100*250=25000</td>
</tr>
</tbody>
</table>

Note
Once the upper limit is reached, additional TSM entries cannot be stored and sent to WCS or NCS. If client TSM entries are full and AP TSM entries are available, only the AP entries are stored, and vice versa. This situation leads to partial output.

A TSM cleanup occurs every hour. Entries are removed only for those APs and clients that are not in the system.
Configuring Voice Parameters

This section contains the following topics:

- Configuring Voice Parameters (GUI), page 4-77
- Configuring Voice Parameters (CLI), page 4-79

Configuring Voice Parameters (GUI)

Step 1  Ensure that the WLAN is configured for WMM and the Platinum QoS level.

Step 2  Disable all WLANs with WMM enabled and click Apply.

Step 3  Choose Wireless and then Network under 802.11a/n or 802.11b/g/n, unselect the 802.11a (or 802.11b/g) Network Status check box, and click Apply to disable the radio network.

Step 4  Choose Wireless > 802.11a/n or 802.11b/g/n > Media. The 802.11a (or 802.11b) > Media page appears. The Voice tab is displayed by default.

Step 5  Select the Admission Control (ACM) check box to enable bandwidth-based CAC for this radio band. The default value is disabled.

Step 6  Select the Admission Control (ACM) you want to use by choosing from the following choices:

- Load-based—To enable channel-based CAC. This is the default option.
- Static—To enable radio-based CAC.

Step 7  In the Max RF Bandwidth text box, enter the percentage of the maximum bandwidth allocated to clients for voice applications on this radio band. Once the client reaches the value specified, the access point rejects new calls on this radio band.
The range is 5 to 85%. The sum of max bandwidth% of voice and video should not exceed 85%.
The default is 75%.

**Step 8** In the Reserved Roaming Bandwidth text box, enter the percentage of maximum allocated bandwidth that is reserved for roaming voice clients. The controller reserves this bandwidth from the maximum allocated bandwidth for roaming voice clients.
The range is 0 to 25%.
The default is 6%.

**Step 9** To enable expedited bandwidth requests, select the **Expedited Bandwidth** check box. By default, this text box is disabled.

**Step 10** To enable SIP CAC support, select the **SIP CAC Support** check box. By default, SIP CAC this check box is disabled.

**Step 11** From the SIP Codec drop-down list, choose one of the following options to set the codec name. The default value is G.711. The options are as follows:

- User Defined
- G.711
- G.729

**Step 12** In the SIP Bandwidth (kbps) text box, enter the bandwidth in kilo bits per second.
The possible range is 8 to 64.
The default value is 64.

**Note** The SIP Bandwidth (kbps) text box is highlighted only when you select the SIP codec as User-Defined. If you choose the SIP codec as G.711, the SIP Bandwidth (kbps) text box is set to 64. If you choose the SIP codec as G.729, the SIP Bandwidth (kbps) text box is set to 8.

**Step 13** In the SIP Voice Sample Interval (msecs) text box, enter the value for the sample interval.

**Step 14** In the Maximum Calls text box, enter the maximum number of calls that can be made to this radio. The maximum call limit includes both direct and roaming-in calls. If the maximum call limit is reached, new or roaming-in calls will fail.
The possible range is 0 to 25.
The default value is 0, which indicates that there is no check for maximum call limit.

**Note** If SIP CAC is supported and the CAC method is static, the Maximum Possible Voice Calls and Maximum Possible Roaming Reserved Calls fields appear.

**Step 15** Select the **Metrics Collection** check box to collect Traffic Stream Metrics. By default, this box is unselected. That is, the traffic stream metrics is not collected by default.

**Step 16** Click **Apply** to commit your changes.

**Step 17** Reenable all WMM WLANs and click **Apply**.

**Step 18** Choose **Network** under 802.11a/n or 802.11b/g/n, select the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to reenable the radio network.

**Step 19** Click **Save Configuration** to save your changes.
Step 20 Repeat this procedure if you want to configure voice parameters for another radio band (802.11a or 802.11b/g).

### Configuring Voice Parameters (CLI)

Ensure that you have configured SIP-based CAC. For instructions, see the “Configuring SIP-Based CAC (CLI)” section on page 4-88.

**Step 1** See all of the WLANs configured on the controller by entering this command:

```
show wlan summary
```

**Step 2** Make sure that the WLAN that you are planning to modify is configured for WMM and the QoS level is set to Platinum by entering this command:

```
show wlan wlan_id
```

**Step 3** Disable all WLANs with WMM enabled prior to changing the voice parameters by entering the command:

```
config wlan disable wlan_id
```

**Step 4** Enable or Disable bandwidth-based voice CAC for the 802.11a or 802.11b/g network by entering this command:

```
config {802.11a | 802.11b} {enable | disable} network
```

**Step 5** Save your settings by entering this command:

```
save config
```

**Step 6** Enable or disable bandwidth-based voice CAC for the 802.11a/n or 802.11b/g/n network by entering this command:

```
config {802.11a | 802.11b} cac voice acm {enable | disable}
```

**Step 7** Set the percentage of maximum bandwidth allocated to clients for voice applications on the 802.11a/n or 802.11b/g/n network by entering this command:

```
config {802.11a | 802.11b} cac voice max-bandwidth bandwidth
```

The `bandwidth` range is 5 to 85%, and the default value is 75%. Once the client reaches the value specified, the access point rejects new calls on this network.

**Step 8** Set the percentage of maximum allocated bandwidth reserved for roaming voice clients by entering this command:

```
config {802.11a | 802.11b} cac voice roam-bandwidth bandwidth
```

The `bandwidth` range is 0 to 25%, and the default value is 6%. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients.

**Step 9** Configure the codec name and sample interval as parameters and to calculate the required bandwidth per call by entering this command:

```
config {802.11a | 802.11b} cac voice sip codec {g711 | g729} sample-interval number_msecs
```

**Step 10** Configure the bandwidth that is required per call by entering this command:

```
config {802.11a | 802.11b} cac voice sip bandwidth bandwidth_kbps sample-interval number_msecs
```

**Step 11** Reenable all WLANs with WMM enabled by entering this command:

```
config wlan enable wlan_id
```
Step 12  Reenable the radio network by entering this command:

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

Step 13  To view the TSM voice metrics, by entering this command:

```
show {802.11a | 802.11b} cu-metrics AP_Name
```

The command also displays the channel utilization metrics.

Step 14  Save your changes by entering this command:
```
save config
```

---

### Configuring Video Parameters

This section contains the following topics:

- Configuring Video Parameters (GUI), page 4-80
- Configuring Video Parameters (CLI), page 4-81

#### Configuring Video Parameters (GUI)

Step 1  Ensure that the WLAN is configured for WMM and the Gold QoS level.

Step 2  Disable all WLANs with WMM enabled and click Apply.

Step 3  Choose Wireless and then Network under 802.11a/n or 802.11b/g/n, unselect the 802.11a (or 802.11b/g) Network Status check box, and click Apply to disable the radio network.

Step 4  Choose Wireless > 802.11a/n or 802.11b/g/n > Media. The 802.11a (or 802.11b) > Media page appears.

**Figure 4-22 802.11a > Video Parameters Page**

Step 5  Choose the Video tab to configure the CAC for Video parameters.

Step 6  Select the Admission Control (ACM) check box to enable video CAC for this radio band. The default value is disabled.
Configuring Voice and Video Parameters

Step 7 In the Max RF Bandwidth text box, enter the percentage of the maximum bandwidth allocated to clients for video applications on this radio band. Once the client reaches the value specified, the access point rejects new requests on this radio band.

The range is 5 to 85%. The sum of maximum bandwidth% of voice and video should not exceed 85%. The default is 0%.

Step 8 Click Apply to commit your changes.

Step 9 Reenable all WMM WLANs and click Apply.

Step 10 Choose Network under 802.11a/n or 802.11b/g/n, select the 802.11a (or 802.11b/g) Network Status check box, and click Apply to reenable the radio network.

Step 11 Click Save Configuration to save your changes.

Step 12 Repeat this procedure if you want to configure video parameters for another radio band (802.11a or 802.11b/g).

Configuring Video Parameters (CLI)

Prerequisites

Ensure that you have configured SIP-based CAC. For instructions, see the “Configuring SIP-Based CAC (CLI)” section on page 4-88.

Step 1 See all of the WLANs configured on the controller by entering this command:

```
show wlan summary
```

Step 2 Make sure that the WLAN that you are planning to modify is configured for WMM and the QoS level is set to Gold by entering this command:

```
show wlan wlan_id
```

Step 3 Disable all WLANs with WMM enabled prior to changing the video parameters by entering this command:

```
config wlan disable wlan_id
```

Step 4 Disable the radio network by entering this command:

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

Step 5 Save your settings by entering this command:

```
save config
```

Step 6 Enable or disable video CAC for the 802.11a or 802.11b/g network by entering this command:

```
config {802.11a | 802.11b} cac video acm {enable | disable}
```

Step 7 Set the percentage of maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network by entering this command:

```
config {802.11a | 802.11b} cac video max-bandwidth bandwidth
```

The bandwidth range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network.
Step 8 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command:
```
config {802.11a | 802.11b} cac video tspec-inactivity-timeout {enable | ignore}
```

Step 9 Reenable all WLANs with WMM enabled by entering this command:
```
config wlan enable wlan_id
```

Step 10 Reenable the radio network by entering this command:
```
config {802.11a | 802.11b} enable network
```

Step 11 Enter the `save config` command to save your settings.

---

### Viewing Voice and Video Settings

This section contains the following topics:

- Viewing Voice and Video Settings (GUI), page 4-82
- Viewing Voice and Video Settings (CLI), page 4-83

#### Viewing Voice and Video Settings (GUI)

**Step 1** Choose **Monitor > Clients** to open the Clients page.

**Figure 4-23 Clients Page**

- Click the MAC address of the desired client to open the Clients > Detail page.
- This page shows the U-APSD status (if enabled) for this client under Quality of Service Properties.
- Click **Back** to return to the Clients page.
Step 4  See the TSM statistics for a particular client and the access point to which this client is associated as follows:
   a. Hover your cursor over the blue drop-down arrow for the desired client and choose 802.11aTSM or 802.11b/g TSM. The Clients > AP page appears.
   b. Click the Detail link for the desired access point to open the Clients > AP > Traffic Stream Metrics page.

This page shows the TSM statistics for this client and the access point to which it is associated. The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Step 5  See the TSM statistics for a particular access point and a particular client associated to this access point, as follows:
   a. Choose Wireless > Access Points > Radios > 802.11a/n or 802.11b/g/n. The 802.11a/n Radios or 802.11b/g/n Radios page appears.
   b. Hover your cursor over the blue drop-down arrow for the desired access point and choose 802.11aTSM or 802.11b/g TSM. The AP > Clients page appears.
   c. Click the Detail link for the desired client to open the AP > Clients > Traffic Stream Metrics page.

This page shows the TSM statistics for this access point and a client associated to it. The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Viewing Voice and Video Settings (CLI)

Step 1  See the CAC configuration for the 802.11a or 802.11b/g network by entering this command:

```
show ap stats {802.11a | 802.11b}
```

Step 2  See the CAC statistics for a particular access point by entering this command:

```
show ap stats {802.11a | 802.11b} ap_name
```

Information similar to the following appears:

```
Call Admission Control (CAC) Stats
 Voice Bandwidth in use(% of config bw) .......... 0
 Total channel MT free .. 0
 Total voice MT free .. 0
 Na Direct .. 0
 Na Roam .. 0
 Video Bandwidth in use(% of config bw) .......... 0
 Total num of voice calls in progress .. 0
 Num of roaming voice calls in progress .. 0
 Total Num of voice calls since AP joined .. 0
 Total Num of roaming calls since AP joined .. 0
 Total Num of exp bw requests received .. 5
 Total Num of exp bw requests admitted .. 2
 Num of voice calls rejected since AP joined .. 0
 Num of roam calls rejected since AP joined .. 0
 Num of calls rejected due to insufficient bw .. 0
 Num of calls rejected due to invalid params .. 0
 Num of calls rejected due to PHY rate .. 0
 Num of calls rejected due to QoS policy .. 0
```
In the example above, “MT” is medium time, “Na” is the number of additional calls, and “exp bw” is expedited bandwidth.

**Note**
Suppose an AP has to be rebooted when a voice client associated with the AP is on an active call. After the AP is rebooted, the client continues to maintain the call, and during the time the AP is down, the database is not refreshed by the controller. Therefore, we recommend that all active calls are ended before the AP is taken down.

**Step 3**
See the U-APSD status for a particular client by entering this command:

```
show client detail client_mac
```

**Step 4**
See the TSM statistics for a particular client and the access point to which this client is associated by entering this command:

```
show client tsm {802.11a | 802.11b} client_mac {ap_mac | all}
```

The optional all command shows all access points to which this client has associated. Information similar to the following appears:

| Client Interface Mac:               | 00:01:02:03:04:05 |
| Measurement Duration:               | 90 seconds        |
| Timestamp                           | 1st Jan 2006, 06:35:80 |

**UpLink Stats**

```
Average Delay (5sec intervals)......................35
Delay less than 10 ms..............................20
Delay bet 10 - 20 ms...............................20
Delay bet 20 - 40 ms...............................20
Delay greater than 40 ms............................20
Total packet Count.................................80
Total packet lost count (5sec)......................10
Maximum Lost Packet count(5sec)......................5
Average Lost Packet count(5secs)....................2
```

**DownLink Stats**

```
Average Delay (5sec intervals)......................35
Delay less than 10 ms..............................20
Delay bet 10 - 20 ms...............................20
Delay bet 20 - 40 ms...............................20
Delay greater than 40 ms............................20
Total packet Count.................................80
Total packet lost count (5sec)......................10
Maximum Lost Packet count(5sec)......................5
Average Lost Packet count(5secs)....................2
```

**Note**
The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

**Note**
To clear the TSM statistics for a particular access point or all the access points to which this client is associated, enter the `clear client tsm {802.11a | 802.11b} client_mac {ap_mac | all}` command.

**Step 5**
See the TSM statistics for a particular access point and a particular client associated to this access point by entering this command:


show ap stats \{802.11a | 802.11b\} \{ap_name tsm \{client_mac | all\}\}  

The optional all command shows all clients associated to this access point. Information similar to the following appears:

AP Interface Mac: 00:0b:85:01:02:03  
Client Interface Mac: 00:01:02:03:04:05  
Measurement Duration: 90 seconds  
Timestamp 1st Jan 2006, 06:35:80  

Uplink Stats  
================ 
Average Delay (5sec intervals)............................35 
Delay less than 10 ms.....................................20 
Delay bet 10 - 20 ms......................................20 
Delay bet 20 - 40 ms......................................20 
Delay greater than 40 ms.................................20 
Total packet Count........................................80 
Total packet lost count (5sec)............................10 
Maximum Lost Packet count(5sec).........................5 
Average Lost Packet count(5sec).........................2 

Downlink Stats  
================ 
Average Delay (5sec intervals)............................35 
Delay less than 10 ms.....................................20 
Delay bet 10 - 20 ms......................................20 
Delay bet 20 - 40 ms......................................20 
Delay greater than 40 ms.................................20 
Total packet Count........................................80 
Total packet lost count (5sec)............................10 
Maximum Lost Packet count(5sec).........................5 
Average Lost Packet count(5sec).........................2 

Note  
The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Step 6  
Enable or disable debugging for call admission control (CAC) messages, events, or packets by entering this command:

debug cac \{all | event | packet\} \{enable | disable\}  

where all configures debugging for all CAC messages, event configures debugging for all CAC events, and packet configures debugging for all CAC packets.

Step 7  
Use the following command to perform voice diagnostics and to view the debug messages between a maximum of two 802.11 clients:

debug client voice-diag \{enable | disable\} mac-id mac-id2 \{verbose\}  

The verbose mode is an optional argument. When the verbose option is used, all debug messages are displayed in the console. You can use this command to monitor a maximum of two 802.11 clients. If one of the clients is a non-WiFi client, only the 802.11 client is monitored for debug messages.

Note  
It is implicitly assumed that the clients being monitored are on call.

Note  
The debug command automatically stops after 60 minutes.
Step 8  Use the following commands to view various voice-related parameters:

- `show client voice-diag status`
  Displays information about whether voice diagnostics is enabled or disabled. If enabled, will also display information about the clients in the watch list and the time remaining for the diagnostics of the voice call.

If voice diagnostics is disabled when the following commands are invoked, a message indicating that voice diagnostics is disabled appears.

- `show client voice-diag tspec`
  Displays the TSPEC information sent from the clients that are enabled for voice diagnostics.

- `show client voice-diag qos-map`
  Displays information about the QoS/DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.

- `show client voice-diag avrg_rssi`
  Display the client’s RSSI values in the last 5 seconds when voice diagnostics is enabled.

- `show client voice-diag roam-history`
  Displays information about the last three roaming calls. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, reason for roaming-failure.

- `show client calls {active | rejected} {802.11a | 802.11bg | all}`
  This command lists the details of active TSPEC and SIP calls on the controller.

Step 9  Use the following commands to troubleshoot video debug messages and statistics:

- `debug ap show stats {802.11b | 802.11a} ap-name multicast`
  Displays the access point’s supported multicast rates.

- `debug ap show stats {802.11b | 802.11a} ap-name load`
  Displays the access point’s QBSS and other statistics.

- `debug ap show stats {802.11b | 802.11a} ap-name tx-queue`
  Displays the access point’s transmit queue traffic statistics.

- `debug ap show stats {802.11b | 802.11a} ap-name client {all | video | <client-mac>}`
  Displays the access point’s client metrics.

- `debug ap show stats {802.11b | 802.11a} ap-name packet`
  Displays the access point’s packet statistics.

- `debug ap show stats {802.11b | 802.11a} ap-name video metrics`
  Displays the access point’s video metrics.

- `debug ap show stats video ap-name multicast mgid number`
  Displays an access point’s Layer 2 MGID database number.

- `debug ap show stats video ap-name admission`
  Displays an access point’s admission control statistics.

- `debug ap show stats video ap-name bandwidth`
  Displays an access point’s video bandwidth.
Configuring Media Parameters (GUI)

Step 1  Make sure that the WLAN is configured for WMM and the Gold QoS level.

Step 2  Disable all WLANs with WMM enabled and click Apply.

Step 3  Choose Wireless and then Network under 802.11a/n or 802.11b/g/n, unselect the 802.11a (or 802.11b/g) Network Status check box, and click Apply to disable the radio network.

Step 4  Choose Wireless > 802.11a/n or 802.11b/g/n > Media. The 802.11a (or 802.11b) > Media > Parameters page appears.

Figure 4-24  802.11a > Media Parameters Page

Step 5  Choose the Media tab to open the Media page.

Step 6  Select the Unicast Video Redirect check box to enable Unicast Video Redirect. The default value is disabled.

Step 7  In the Maximum Media Bandwidth (0-85%) text box, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches the specified value, the access point rejects new calls on this radio band.

The default value is 85%; valid values are from 0 to 85%.

Step 8  In the Client Phy Rate text box, enter the value for the rate in kilobits per second at which the client operates.

Step 9  In the Maximum Retry Percent (0-100%) text box, enter the percentage of the maximum retry. The default value is 80.

Step 10 Select the Multicast Direct Enable check box to enable the Multicast Direct Enable text box. The default value is enabled.

Step 11 From the Max Streams per Radio drop-down list, choose the maximum number of allowed multicast direct streams per radio. Choose a value between 1 to 20 or No Limit. The default value is set to No Limit.
Step 12  From the Max Streams per Client drop-down list, choose the maximum number of allowed clients per radio. Choose a value between 1 to 20 or No Limit. The default value is set to No Limit.

Step 13  If you want to enable the best radio queue for this radio, select the **Best Effort QoS Admission** check box. The default value is disabled.

---

### Configuring SIP Based CAC

This section contains the following topics:
- Guidelines and Limitations, page 4-88
- Configuring SIP-Based CAC (CLI), page 4-88

#### Guidelines and Limitations

- SIPs are available only on the Cisco 4400 Series and Cisco 5500 Series Controllers, and on the 1240, 1130, and 11n access points.
- SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
- SIP CAC will be supported only if SIP snooping is enabled.

#### Configuring SIP-Based CAC (CLI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Set the voice to the platinum QoS level by entering this command:  
      | `config wlan qos wlan-id Platinum` |
| 2    | Enable the call-snooping feature for a particular WLAN by entering this command:  
      | `config wlan call-snoop enable wlan-id` |
| 3    | Enable the ACM to this radio by entering this command:  
      | `config {802.11a | 802.11b} cac {voice | video} acm enable` |

---

### Configuring Voice Prioritization Using Preferred Call Numbers

This section contains the following topics:
- Information About Configuring Voice Prioritization Using Preferred Call Numbers, page 4-89
- Guidelines and Limitations, page 4-89
- Configuring a Preferred Call Number, page 4-89
Information About Configuring Voice Prioritization Using Preferred Call Numbers

You can configure a controller to support calls from clients that do not support TSPEC-based calls. This feature is known as voice prioritization. These calls are given priority over other clients utilizing the voice pool. Voice prioritization is available only for SIP-based calls and not for TSPEC-based calls. If the bandwidth is available, it takes the normal flow and allocates the bandwidth to those calls.

You can configure up to six preferred call numbers. When a call comes to one of the configured preferred numbers, the controller does not check on the maximum call limit. It invokes the CAC to allocate bandwidth for the preferred call. The bandwidth allocation is 85 percent of the entire bandwidth pool, not just from the maximum configured voice pool. The bandwidth allocation is the same even for roaming calls.

Guidelines and Limitations

- You must configure the following before configuring voice prioritization:
  - Set WLAN QoS to platinum.
  - Enable ACM for the radio.
  - Enable SIP call snooping on the WLAN.
- Cisco 5500 Series Controllers and all nonmesh access points do not support voice prioritization.

Configuring a Preferred Call Number

This section contains the following topics:

- Configuring a Preferred Call Number (GUI), page 4-89
- Configuring a Preferred Call Number (CLI), page 4-90

Configuring a Preferred Call Number (GUI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Set the WLAN QoS profile to Platinum. See the “Assigning a QoS Profile to a WLAN” section on page 8-38.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enable ACM for the WLAN radio. See the “Configuring Voice and Video Parameters” section on page 4-73.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enable SIP call snooping for the WLAN. See the “Configuring Media Session Snooping and Reporting” section on page 8-43.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose Wireless &gt; Advanced &gt; Preferred Call to open the Preferred Call page. All calls configured on the controller appear.</td>
</tr>
<tr>
<td>Note</td>
<td>To remove a preferred call, hover your cursor over the blue drop-down arrow and choose Remove.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Add Number to add a new preferred call.</td>
</tr>
</tbody>
</table>
Configuring Controller Settings

Chapter 4

Configuring Controller Settings

Configuring EDCA Parameters

This section contains the following topics:

- Information About EDCA Parameters, page 4-90
- Configuring EDCA Parameters, page 4-90

Information About EDCA Parameters

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic. Follow the instructions in this section to configure EDCA parameters using the controller GUI or CLI.

Configuring EDCA Parameters

This section contains the following topics:
Configuring EDCA Parameters (GUI)

**Step 1** Choose Wireless and then Network under 802.11a/n or 802.11b/g/n, unselect the 802.11a (or 802.11b/g) Network Status check box, and click Apply to disable the radio network.

**Step 2** Choose EDCA Parameters under 802.11a/n or 802.11b/g/n. The 802.11a (or 802.11b/g) > EDCA Parameters page appears.

**Figure 4-25 802.11a > EDCA Parameters Page**

![802.11a > EDCA Parameters Page](image)

**Step 3** Choose one of the following options from the EDCA Profile drop-down list:

- **WMM**—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.
- **Spectralink Voice Priority**—Enables SpectraLink voice priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.
- **Voice Optimized**—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are deployed on your network.
- **Voice & Video Optimized**—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
- **Custom Voice**—Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.

*Note* If you deploy video services, admission control (ACM) must be disabled.

**Step 4** If you want to enable MAC optimization for voice, select the Enable Low Latency MAC check box. Otherwise, leave this check box unselected, which is the default value. This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, which improves the number of voice calls serviced per access point.
Configuring EDCA Parameters (CLI)

Step 1  Disable the radio network by entering this command:
        `config {802.11a | 802.11b} disable network`

Step 2  Save your settings by entering this command:
        `save config`

Step 3  Enable a specific EDCA profile by entering this command:
        `config advanced {802.11a | 802.11b} edca-parameters {wmm-default | svp-voice| optimized-voice| optimized-video-voice| custom-voice}`

        • wmm-default—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.
        • svp-voice—Enables SpectraLink voice priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.
        • optimized-voice—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are deployed on your network.
        • optimized-video-voice—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
        • custom-voice—Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.

        Note  If you deploy video services, admission control (ACM) must be disabled.

Step 4  View the current status of MAC optimization for voice by entering this command:
        `show {802.11a | 802.11b}`

        Information similar to the following appears:
        `Voice-mac-optimization......................Disabled`

Step 5  Enable or disable MAC optimization for voice by entering this command:
        `config advanced {802.11a | 802.11b} voice-mac-optimization {enable | disable}`
Configuring the Cisco Discovery Protocol

This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, which improves the number of voice calls serviced per access point. The default value is disabled.

**Step 6** Reenable the radio network by entering this command:
```
config {802.11a | 802.11b} enable network
```

**Step 7** Save your settings by entering this command:
```
save config
```

---

**Configuring the Cisco Discovery Protocol**

This section contains the following topics:

- Information About Configuring the Cisco Discovery Protocol, page 4-93
- Guidelines and Limitations, page 4-93
- Configuring the Cisco Discovery Protocol, page 4-95
- Viewing Cisco Discovery Protocol Information, page 4-98

---

**Information About Configuring the Cisco Discovery Protocol**

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco-manufactured equipment. A device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighboring devices.

The default value for the frequency of periodic transmissions is 60 seconds, and the default advertised time-to-live value is 180 seconds. The second and latest version of the protocol, CDPv2, introduces new time-length-values (TLVs) and provides a reporting mechanism that allows for more rapid error tracking, which reduces downtime.

---

**Guidelines and Limitations**

- CDPv1 and CDPv2 are supported on the following devices:
  - Cisco 5500, 4400, 2500, and 2100 Series Controllers

  **Note** CDP is not supported on the controllers that are integrated into Cisco switches and routers, including those in the Catalyst 3750G Integrated Wireless LAN Controller Switch, the Cisco WiSM, and the Cisco 28/37/38xx Series Integrated Services Router. However, you can use the `show ap cdp neighbors detail {Cisco_AP | all}` command on these controllers in order to see the list of CDP neighbors for the access points that are connected to the controller.

  - CAPWAP-enabled access points
  - An access point connected directly to a Cisco 5500, 4400, or 2100 Series Controller
To use the Intelligent Power Management feature, ensure that CDPv2 is enabled on the Cisco 2100 and 2500 Series Controllers. CDP v2 is enabled by default.

- The OEAP 600 access points do not support CDP.
- The support of CDPv1 and CDPv2 enables network management applications to discover Cisco devices.
- The following TLVs are supported by both the controller and the access point:
  - Device-ID TLV: 0x0001—The host name of the controller, the access point, or the CDP neighbor.
  - Address TLV: 0x0002—The IP address of the controller, the access point, or the CDP neighbor.
  - Port-ID TLV: 0x0003—The name of the interface on which CDP packets are sent out.
  - Capabilities TLV: 0x0004—The capabilities of the device. The controller sends out this TLV with a value of Host: 0x10, and the access point sends out this TLV with a value of Transparent Bridge: 0x02.
  - Version TLV: 0x0005—The software version of the controller, the access point, or the CDP neighbor.
  - Platform TLV: 0x0006—The hardware platform of the controller, the access point, or the CDP neighbor.
  - Power Available TLV: 0x001a—The amount of power available to be transmitted by power sourcing equipment to permit a device to negotiate and select an appropriate power setting.
  - Full/Half Duplex TLV: 0x000b—The full- or half-duplex mode of the Ethernet link on which CDP packets are sent out.
- These TLVs are supported only by the access point:
  - Power Consumption TLV: 0x0010—The maximum amount of power consumed by the access point.
  - Power Request TLV: 0x0019—The amount of power to be transmitted by a powerable device in order to negotiate a suitable power level with the supplier of the network power.
- You can configure CDP and view CDP information using the GUI in controller software release 4.1 or later or the CLI in controller software release 4.0 or later releases. Figure 4-26 shows a sample network that you can use as a reference when performing the procedures in this section.
- Changing the CDP configuration on the controller does not change the CDP configuration on the access points that are connected to the controller. You must enable and disable CDP separately for each access point.
- You can enable or disable the CDP state on all or specific interfaces and radios. This configuration can be applied to all access points or a specific access point. For more information on how to configure CDP on the interfaces and radios, see the “Configuring the Cisco Discovery Protocol” section on page 4-95 and the “Configuring the Cisco Discovery Protocol (CLI)” section on page 4-97.
- The following is the behavior assumed for various interfaces and access points:
  - CDP is disabled on radio interfaces on indoor (nonindoor mesh) access points.
  - Nonmesh access points have CDPs disabled on radio interfaces when they join the controller. The persistent CDP configuration is used for the APs that had CDP support in its previous image.
- CDP is enabled on radio interfaces on indoor-mesh and mesh access points.
- Mesh access points will have CDP enabled on their radio interfaces when they join the controller. The persistent CDP configuration is used for the access points that had CDP support in a previous image. The CDP configuration for radio interfaces is applicable only for mesh APs.

Figure 4-26 Sample Network Illustrating CDP

Configuring the Cisco Discovery Protocol

This section contains the following topics:
- Configuring the Cisco Discovery Protocol (GUI), page 4-95
- Configuring the Cisco Discovery Protocol (CLI), page 4-97

Configuring the Cisco Discovery Protocol (GUI)

Step 1 Choose Controller > CDP > Global Configuration to open the CDP > Global Configuration page.
Step 2 Select the CDP Protocol Status check box to enable CDP on the controller or unselect it to disable this feature. The default value is selected.

**Note** Enabling or disabling this feature is applicable to all controller ports.

Step 3 From the CDP Advertisement Version drop-down list, choose v1 or v2 to specify the highest CDP version supported on the controller. The default value is v1.

Step 4 In the Refresh-time Interval text box, enter the interval at which CDP messages are to be generated. The range is 5 to 254 seconds, and the default value is 60 seconds.

Step 5 In the Holdtime text box, enter the amount of time to be advertised as the time-to-live value in generated CDP packets. The range is 10 to 255 seconds, and the default value is 180 seconds.

Step 6 Click Apply to commit your changes.

Step 7 Click Save Configuration to save your changes.

Step 8 Perform one of the following:

- To enable or disable CDP on a specific access point, follow these steps:
  a. Choose Wireless > Access Points > All APs to open the All APs page.
  b. Click the link for the desired access point.
  c. Choose the Advanced tab to open the All APs > Details for (Advanced) page.
  d. Select the Cisco Discovery Protocol check box to enable CDP on this access point or unselect it to disable this feature. The default value is enabled.

**Note** If CDP is disabled in Step 2, a message indicating that the Controller CDP is disabled appears.

- Enable CDP for a specific Ethernet interface, radio, or slot as follows:
  a. Choose Wireless > Access Points > All APs to open the All APs page.
  b. Click the link for the desired access point.
  c. Choose the Interfaces tab and select the corresponding check boxes for the radios or slots from the CDP Configuration section.
Chapter 4  Configuring Controller Settings

Configuring the Cisco Discovery Protocol

Note: Configuration for radios is only applicable for mesh access points.

d. Click Apply to commit your changes.

To enable or disable CDP on all access points currently associated to the controller, follow these steps:

a. Choose Wireless > Access Points > Global Configuration to open the Global Configuration page.

b. Select the CDP State check box to enable CDP on all access points associated to the controller or unselect it to disable CDP on all access points. The default value is selected. You can enable CDP on a specific Ethernet interface, radio, or slot by selecting the corresponding check box. This configuration will be applied to all access points associated with the controller.

c. Click Apply to commit your changes.

Step 9  Click Save Configuration to save your changes.

Configuring the Cisco Discovery Protocol (CLI)

Step 1  Enable or disable CDP on the controller by entering this command:

```
config cdp {enable | disable}
```

CDP is enabled by default.

Step 2  Specify the interval at which CDP messages are to be generated by entering this command:

```
config cdp timer seconds
```

The range is 5 to 254 seconds, and the default value is 60 seconds.

Step 3  Specify the amount of time to be advertised as the time-to-live value in generated CDP packets by entering this command:

```
config cdp holdtime seconds
```

The range is 10 to 255 seconds, and the default value is 180 seconds.

Step 4  Specify the highest CDP version supported on the controller by entering this command:

```
config cdp advertise {v1 | v2}
```

The default value is v1.

Step 5  Enable or disable CDP on all access points that are joined to the controller by entering the config ap cdp {enable | disable} all command.

The config ap cdp disable all command disables CDP on all access points that are joined to the controller and all access points that join in the future. CDP remains disabled on both current and future access points even after the controller or access point reboots. To enable CDP, enter the config ap cdp enable all command.

Note: After you enable CDP on all access points joined to the controller, you may disable and then reenable CDP on individual access points using the command in Step 6. After you disable CDP on all access points joined to the controller, you may not enable and then disable CDP on individual access points.
Step 6 Enable or disable CDP on a specific access point by entering this command:

```
config ap cdp {enable | disable} Cisco_AP
```

Step 7 Configure CDP on a specific or all access points for a specific interface by entering this command:

```
config ap cdp {ethernet | radio} interface_number slot_id {enable | disable} {all | Cisco_AP}
```

Note When you use the config ap cdp command to configure CDP on radio interfaces, a warning message appears indicating that the configuration is applicable only for mesh access points.

Step 8 Save your changes by entering this command:

```
save config
```

### Viewing Cisco Discovery Protocol Information

This section contains the following topics:

- Viewing Cisco Discovery Protocol Information (GUI), page 4-98
- Viewing Cisco Discovery Protocol Information (CLI), page 4-100
- Getting CDP Debug Information, page 4-101

### Viewing Cisco Discovery Protocol Information (GUI)

Step 1 Choose Monitor > CDP > Interface Neighbors to open the CDP > Interface Neighbors page appears.

![Figure 4-28 CDP > Interface Neighbors Page](image)

This page shows the following information:

- The controller port on which the CDP packets were received
- The name of each CDP neighbor
• The IP address of each CDP neighbor
• The port used by each CDP neighbor for transmitting CDP packets
• The time left (in seconds) before each CDP neighbor entry expires
• The functional capability of each CDP neighbor, defined as follows: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, or M - Remotely Managed Device
• The hardware platform of each CDP neighbor device

Step 2 Click the name of the desired interface neighbor to see more detailed information about each interface’s CDP neighbor. The CDP > Interface Neighbors > Detail page appears.

This page shows the following information:
• The controller port on which the CDP packets were received
• The name of the CDP neighbor
• The IP address of the CDP neighbor
• The port used by the CDP neighbor for transmitting CDP packets
• The CDP version being advertised (v1 or v2)
• The time left (in seconds) before the CDP neighbor entry expires
• The functional capability of the CDP neighbor, defined as follows: Router, Trans Bridge, Source Route Bridge, Switch, Host, IGMP, Repeater, or Remotely Managed Device
• The hardware platform of the CDP neighbor device
• The software running on the CDP neighbor

Step 3 Choose AP Neighbors to see a list of CDP neighbors for all access points connected to the controller. The CDP AP Neighbors page appears.

Step 4 Click the CDP Neighbors link for the desired access point to see a list of CDP neighbors for a specific access point. The CDP > AP Neighbors page appears.

This page shows the following information:
• The name of each access point
• The IP address of each access point
• The name of each CDP neighbor
• The IP address of each CDP neighbor
• The port used by each CDP neighbor
• The CDP version being advertised (v1 or v2)

Step 5 Click the name of the desired access point to see detailed information about an access point’s CDP neighbors. The CDP > AP Neighbors > Detail page appears.

This page shows the following information:
• The name of the access point
• The MAC address of the access point’s radio
• The IP address of the access point
• The interface on which the CDP packets were received
• The name of the CDP neighbor
• The IP address of the CDP neighbor
Configuring the Cisco Discovery Protocol

The port used by the CDP neighbor
The CDP version being advertised (v1 or v2)
The time left (in seconds) before the CDP neighbor entry expires
The functional capability of the CDP neighbor, defined as follows: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, or M - Remotely Managed Device
The hardware platform of the CDP neighbor device
The software running on the CDP neighbor

Step 6
Choose Traffic Metrics to see CDP traffic information. The CDP > Traffic Metrics page appears. This page shows the following information:
The number of CDP packets received by the controller
The number of CDP packets sent from the controller
The number of packets that experienced a checksum error
The number of packets dropped due to insufficient memory
The number of invalid packets

Viewing Cisco Discovery Protocol Information (CLI)

Step 1
See the status of CDP and to view CDP protocol information by entering this command:
```
show cdp
```

Step 2
See a list of all CDP neighbors on all interfaces by entering this command:
```
show cdp neighbors [detail]
```
The optional detail command provides detailed information for the controller’s CDP neighbors.

Note
This command shows only the CDP neighbors of the controller. It does not show the CDP neighbors of the controller’s associated access points. Additional commands are provided below to show the list of CDP neighbors per access point.

Step 3
See all CDP entries in the database by entering this command:
```
show cdp entry all
```

Step 4
See CDP traffic information on a given port (for example, packets sent and received, CRC errors, and so on) by entering this command:
```
show cdp traffic
```

Step 5
See the CDP status for a specific access point by entering this command:
```
show ap cdp ap-name Cisco_AP
```

Step 6
See the CDP status for all access points that are connected to the controller by entering this command:
```
show ap cdp all
```

Step 7
See a list of all CDP neighbors for a specific access point by entering these commands:
• show ap cdp neighbors ap-name Cisco_AP
• show ap cdp neighbors detail Cisco_AP

Note

The access point sends CDP neighbor information to the controller only when the information changes.

Step 8

See a list of all CDP neighbors for all access points connected to the controller by entering these commands:
• show ap cdp neighbors all
• show ap cdp neighbors detail all

Information similar to the following appears when you enter the show ap cdp neighbors all command:

<table>
<thead>
<tr>
<th>AP Name</th>
<th>AP IP</th>
<th>Neighbor Name</th>
<th>Neighbor IP</th>
<th>Neighbor Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP0013.601c.0a0</td>
<td>10.76.108.123</td>
<td>6500-1</td>
<td>10.76.108.207</td>
<td>GigabitEthernet1/26</td>
</tr>
<tr>
<td>AP0013.601c.0b0</td>
<td>10.76.108.111</td>
<td>6500-1</td>
<td>10.76.108.207</td>
<td>GigabitEthernet1/27</td>
</tr>
<tr>
<td>AP0013.601c.0c0</td>
<td>10.76.108.125</td>
<td>6500-1</td>
<td>10.76.108.207</td>
<td>GigabitEthernet1/28</td>
</tr>
</tbody>
</table>

Information similar to the following appears when you enter the show ap cdp neighbors detail all command:

AP Name: AP0013.601c.0a0
AP IP Address: 10.76.108.125
----------------------------------
Device ID: 6500-1
Entry address(es): 10.76.108.207
Platform: cisco WS-C6506-E, Capabilities: Router Switch IGMP
Interface: Port - 1, Port ID (outgoing port): GigabitEthernet1/26
Holdtime: 157 sec

Version:
Compiled Fri 13-Mar

Note

The access point sends CDP neighbor information to the controller only when the information changes.

Getting CDP Debug Information

• Get debug information related to CDP packets by entering by entering this command:
  debug cdp packets
• Get debug information related to CDP events by entering this command:
  debug cdp events

Configuring Authentication for the Controller and NTP Server

This section contains the following topics:

• Information About Configuring Authentication for the Controller and NTP Server, page 4-102
Configuring RFID Tag Tracking

• Configuring Authentication for the Controller and NTP Server, page 4-102

Information About Configuring Authentication for the Controller and NTP Server

Starting in release 7.0.116.0, the controller software is now compliant with RFC 1305. As per this requirement, controllers must synchronize time with an NTP server by authentication. By default, an MD5 checksum is used.

Configuring Authentication for the Controller and NTP Server

This section contains the following topics:
• Configuring the NTP Server for Authentication (GUI), page 4-102
• Configuring the NTP Server for Authentication (CLI), page 4-102

Configuring the NTP Server for Authentication (GUI)

Step 1 Choose Controller > NTP > Servers to open the NTP Servers page.
Step 2 Click New to add a new NTP Server.
Step 3 In the Server Index (Priority) text box, enter the NTP server index.
   The controller tries Index 1 first, then Index 2 through 3, in a descending order. Set this to 1 if your network is using only one NTP server.
Step 4 Enter the server IP address in the Server IP Address field.
Step 5 Select the Enable NTP Authentication check box to enable NTP Authentication.
Step 6 Enter the Key index.
Step 7 Click Apply.

Configuring the NTP Server for Authentication (CLI)

• config time ntp auth enable server-index key-index—Enables NTP authentication on a given NTP server.
• config time ntp key-auth add key-index md5 key-format key—Adds an authentication key. By default MD5 is used. The key format can be "ascii" or "hex".
• config time ntp key-auth delete key-index—Deletes authentication keys.
• config time ntp auth disable server-index—Disables NTP authentication.
• show ntp-keys—Displays the NTP authentication related parameter.

Configuring RFID Tag Tracking

This section contains the following topics:
Information About Configuring RFID Tag Tracking

The controller enables you to configure radio-frequency identification (RFID) tag tracking. RFID tags are small wireless devices that are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller, and the location appliance.

To know more about the tags supported by controller, see http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html. See Table 4-5 for details. The location appliance receives telemetry and chokepoint information from tags that are compliant with this CCX specification.

**Table 4-5  Cisco Compatible Extensions for RFID Tags Summary**

<table>
<thead>
<tr>
<th>Partners</th>
<th>AeroScout</th>
<th>WhereNet</th>
<th>Pango (InnerWireless)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Name</td>
<td>T2</td>
<td>T3</td>
<td>V4</td>
</tr>
</tbody>
</table>

**Telemetry**

<table>
<thead>
<tr>
<th></th>
<th>T2</th>
<th>T3</th>
<th>Wheretag IV</th>
<th>V3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>X</td>
<td>X</td>
<td>—</td>
<td>X</td>
</tr>
<tr>
<td>Pressure</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Humidity</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Status</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Fuel</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Quantity</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Distance</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Motion Detection</td>
<td>X</td>
<td>X</td>
<td>—</td>
<td>X</td>
</tr>
<tr>
<td>Number of Panic</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Buttons</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tampering</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Battery Information</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Multiple-Frequency</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

1. For chokepoint systems, note that the tag can work only with chokepoints coming from the same vendor.

**Note**

The Network Mobility Services Protocol (NMSP) runs on location appliance software release 3.0 or later releases. In order for NMSP to function properly, the TCP port (16113) over which the controller and location appliance communicate must be open (not blocked) on any firewall that exists between these two devices. See the *Cisco Location Appliance Configuration Guide* for additional information on NMSP and RFID tags.

The Cisco-approved tags support these capabilities:

- **Information notifications**—Enable you to view vendor-specific and emergency information.
Configuring RFID Tag Tracking

Information polling—Enables you to monitor battery status and telemetry data. Many telemetry data types provide support for sensory networks and a large range of applications for RFID tags.

Measurement notifications—Enable you to deploy chokepoints at strategic points within your buildings or campuses. Whenever an RFID tag moves to within a defined proximity of a chokepoint, the tag begins transmitting packets that advertise its location in relation to the chokepoint.

The number of tags supported varies depending on controller platform. Table 4-6 lists the number of tags supported per controller.

<table>
<thead>
<tr>
<th>Controller</th>
<th>Number of RFID Tags Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>5508</td>
<td>2500</td>
</tr>
<tr>
<td>Catalyst 3750G Integrated Wireless LAN Controller Switch</td>
<td>1250</td>
</tr>
<tr>
<td>Controller Network Module within the Cisco 28/37/38xx Series Integrated Services Routers</td>
<td>500</td>
</tr>
<tr>
<td>2500</td>
<td>500</td>
</tr>
</tbody>
</table>

You can configure and view RFID tag tracking information through the controller CLI.

## Configuring RFID Tag Tracking

This section contains the following topics:

- Configuring RFID Tag Tracking (CLI), page 4-104
- Viewing RFID Tag Tracking Information (CLI), page 4-105
- Debugging RFID Tag Tracking Issues (CLI), page 4-106
- Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues (CLI), page 4-107
- Viewing NMSP Settings (CLI), page 4-107
- Debugging NMSP Issues, page 4-110

### Configuring RFID Tag Tracking (CLI)

**Step 1** Enable or disable RFID tag tracking by entering this command:

```
config rfid status {enable | disable}
```

The default value is enabled.

**Step 2** Specify a static timeout value (between 60 and 7200 seconds) by entering this command:

```
config rfid timeout seconds
```

The static timeout value is the amount of time that the controller maintains tags before expiring them. For example, if a tag is configured to beacon every 30 seconds, we recommend that you set the timeout value to 90 seconds (approximately three times the beacon value). The default value is 1200 seconds.

**Step 3** Enable or disable RFID tag mobility for specific tags by entering these commands:
• `config rfid mobility vendor_name enable`—Enables client mobility for a specific vendor’s tags. When you enter this command, tags are unable to obtain a DHCP address for client mode when attempting to select and/or download a configuration.

• `config rfid mobility vendor_name disable`—Disables client mobility for a specific vendor’s tags. When you enter this command, tags can obtain a DHCP address. If a tag roams from one subnet to another, it obtains a new address rather than retaining the anchor state.

**Note**
These commands can be used only for Pango tags. Therefore, the only valid entry for `vendor_name` is “pango” in all lowercase letters.

### Viewing RFID Tag Tracking Information (CLI)

**Step 1**
See the current configuration for RFID tag tracking by entering this command:

```
show rfid config
```

Information similar to the following appears:

- **RFID Tag data Collection**: Enabled
- **RFID timeout**: 1200 seconds
- **RFID mobility**: Oui:00:14:7e : Vendor:pango
  - State: Disabled

**Step 2**
See detailed information for a specific RFID tag by entering this command:

```
show rfid detail mac_address
```

where `mac_address` is the tag’s MAC address.

Information similar to the following appears:

- **RFID address**: 00:12:b8:00:20:52
- **Vendor**: G2
- **Last Heard**: 51 seconds ago
- **Packets Received**: 2
- **Bytes Received**: 324
- **Cisco Type**: Content Header
  - **Version**: 1
  - **TX Power**: 12 dBm
  - **Channel**: 1
  - **Reg Class**: 12
  - **Burst Length**: 1

**CCX Payload**

- **Last Sequence Control**: 0
- **Payload length**: 127
- **Payload Data Hex Dump**
  - 01 09 00 00 00 00 0b 85 52 52 52 02 07 4b ff ff
  - 7e ff ff ff 03 14 00 12 7b 10 48 53 c1 f7 51 4b
  - 50 ba 97 27 80 00 67 00 01 03 05 01 42 34 00
  - 00 03 05 02 42 5c 00 00 03 05 03 42 82 00 00 03
  - 05 04 42 96 00 00 03 05 05 05 00 00 55 03 05 06
42 be 00 00 03 02 07 05 03 12 08 10 00 01 02 03
04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 03 0d 09 03
08 05 07 a8 02 00 10 00 23 b2 4e 03 02 0a 03

Nearby AP Statistics:
   lap1242-2(slot 0, chan 1) 50 seconds ago..... -76 dBm
   lap1242(slot 0, chan 1) 50 seconds ago..... -65 dBm

Step 3  See a list of all RFID tags currently connected to the controller by entering this command:
show rfid summary

Information similar to the following appears:

<table>
<thead>
<tr>
<th>RFID ID</th>
<th>VENDOR</th>
<th>Closest AP</th>
<th>RSSI</th>
<th>Time Since Last Heard</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:04:f1:00:00:03 Wherenet flexconnect</td>
<td>-70</td>
<td>151 seconds ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:04:f1:00:00:05 Wherenet flexconnect</td>
<td>-66</td>
<td>251 seconds ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:0c:cc:5b:f8:1e Aerosct  flexconnect</td>
<td>-40</td>
<td>5 seconds ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:0c:cc:5c:05:10 Aerosct  flexconnect</td>
<td>-68</td>
<td>25 seconds ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:0c:cc:5c:06:69 Aerosct  flexconnect</td>
<td>-54</td>
<td>7 seconds ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:0c:cc:5c:06:6b Aerosct  flexconnect</td>
<td>-68</td>
<td>245 seconds ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:0c:cc:5c:06:b5 Aerosct  cisco1242</td>
<td>-67</td>
<td>70 seconds ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:0c:cc:5c:5a:2b Aerosct  cisco1242</td>
<td>-68</td>
<td>31 seconds ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:0c:cc:5c:87:34 Aerosct  flexconnect</td>
<td>-40</td>
<td>5 seconds ago</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Step 4  See a list of RFID tags that are associated to the controller as clients by entering this command:
show rfid client

When the RFID tag is in client mode, information similar to the following appears:

<table>
<thead>
<tr>
<th>RFID Mac</th>
<th>VENDOR</th>
<th>Sec Ago</th>
<th>Associated AP</th>
<th>Chnl</th>
<th>Client State</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:14:7e:00:0b:b1 Pango</td>
<td>35</td>
<td>AP0019.e75c.fef4</td>
<td>1</td>
<td>Probing</td>
<td></td>
</tr>
</tbody>
</table>

When the RFID tag is not in client mode, the above text boxes are blank.

### Debugging RFID Tag Tracking Issues (CLI)

If you experience any problems with RFID tag tracking, use these debug commands.

- Configure MAC address debugging by entering this command:
  
  `debug mac addr mac_address`

  **Note**  We recommend that you perform the debugging on a per-tag basis. If you enable debugging for all of the tags, the console or Telnet screen is inundated with messages.

- Enable or disable debugging for the 802.11 RFID tag module by entering this command:
  
  `debug dot11 rfid {enable | disable}`

- Enable or disable RFID debug options by entering this command:
debug rfid {all | detail | error | nmsp | receive} {enable | disable}

where
- **all** configures debugging of all RFID messages.
- **detail** configures debugging of RFID detailed messages.
- **error** configures debugging of RFID error messages.
- **nmsp** configures debugging of RFID NMSP messages.
- **receive** configures debugging of incoming RFID tag messages.

### Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues (CLI)

The Network Mobility Services Protocol (NMSP) manages communication between the location appliance and the controller for incoming and outgoing traffic. If your application requires more frequent location updates, you can modify the NMSP notification interval (to a value between 1 and 180 seconds) for clients, active RFID tags, and rogue access points and clients.

**Note**
The TCP port (16113) that the controller and location appliance communicate over must be open (not blocked) on any firewall that exists between the controller and the location appliance for NMSP to function.

**Step 1**
Set the NMSP notification interval value for clients, RFID tags, and rogue clients and access points by entering these commands, where `interval` is a value between 1 and 180 seconds:

- `config nmsp notification interval rssi clients interval`
- `config nmsp notification interval rssi rfid interval`
- `config nmsp notification interval rssi rogues interval`

**Step 2**
See the NMSP notification intervals by entering this command:

```
show nmsp notification interval
```

Information similar to the following appears:

```
NMSP Notification Interval Summary

RSSI Interval:
Client.......................................... 2 sec
RFID............................................ 0 sec
Rogue AP........................................ 2 sec
Rogue Client................................... 2 sec
```

### Viewing NMSP Settings (CLI)

To view NMSP information, use these CLI commands:

- See the status of active NMSP connections by entering this command:

```
show nmsp status
```

Information similar to the following appears:
Configuring RFID Tag Tracking

MSE IP Address    Tx Echo Resp    Rx Echo Req    Tx Data    Rx Data
--------------    ------------    -----------    -------    -------
171.71.132.107      39046           39046        103742     1

- See the NMSP capabilities by entering this command:
  
  `show nmsp capability`

  Information similar to the following appears:

  Service                  Subservice
  -------                  ----------
  RSSI                     Mobile Station, Tags, Rogue,
  Info                     Mobile Station, Rogue,
  Statistics               Mobile Station, Tags,
  IDS Services       WIPS

- See the NMSP counters by entering this command:
  
  `show nmsp statistics {summary | connection}

  where

  - `summary` shows the common NMSP counters.
  - `connection` shows the connection-specific NMSP counters.

  Information similar to the following appears for the `show nmsp statistics summary` command:

  NMSP Global Counters
  
  Client Measure Send Fail................................. 0
  Send RSSI with no entry.................................. 0
  APP msg too big........................................... 0
  Failed Select on Accept Socket......................... 0
  Failed SSL write.......................................... 0
  Partial SSL write........................................ 0
  SSL write returned zero.................................. 0
  SSL write attempts to want read......................... 0
  SSL write attempts to want write....................... 0
  SSL write got default error............................. 0
  SSL write max data length sent........................ 0
  SSL write max attempts to write in loop............... 0
  SSL read returned zero................................. 0
  SSL read attempts to want read......................... 0
  SSL read attempts to want write....................... 0
  SSL read got default error............................. 0
  Failed SSL read - Con Rx buf freed..................... 0
  Failed SSL read - Con/SSL freed......................... 0
  Max records read before exiting SSL read.............. 0
  Normal Prio Tx Q full.................................. 0
  Highest Prio Tx Q count................................. 0
  Normal Prio Tx Q count................................ 0
  Messages sent by APPs to Highest Prio TxQ............ 0
  Max Measure Notify Msg.................................. 0
  Max Info Notify Msg.................................... 0
  Max Highest Prio Tx Q Size............................. 0
  Max Normal Prio Tx Q Size.............................. 0
  Max Rx Size............................................... 1
  Max Info Notify Q Size.................................. 0
  Max Client Info Notify Delay............................ 0
  Max Rogue AP Info Notify Delay......................... 0
  Max Rogue Client Info Notify Delay..................... 0
  Max Client Measure Notify Delay......................... 0
  Max Tag Measure Notify Delay............................ 0
  Max Rogue AP Measure Notify Delay...................... 0
Max Rogue Client Measure Notify Delay............ 0
Max Client Stats Notify Delay..................... 0
Max Client Stats Notify Delay..................... 0
RFID Measurement Periodic..................... 0
RFID Measurement Immediate................... 0
SSL Handshake failed............................ 0
NMSP Rx detected con failure................... 0
NMSP Tx detected con failure................... 0
NMSP Tx buf size exceeded....................... 0
Reconnect Before Conn Timeout................. 0

Information similar to the following appears for each active connection when you enter the show nmsp statistics connection command:

NMSP Connection Counters

MSE IP: 171.71.132.107
Connection status: UP
Tx message count Rx message count
----------------- -----------------
WLC Capability: 1 MSE Capability: 0
Service Subscr Rsp: 1 Service Subscr Req: 1
Measure Rsp: 0 Measure Req: 0
Measure Notify: 0
Info Rsp: 0 Info Req: 0
Info Notify: 0
Stats Rsp: 0 Stats Req: 0
Stats Notify: 0
Loc Req: 0 Loc Rsp: 0
Loc Subscr Req: 0 Loc Subscr Rsp: 0
Loc Notify: 0
Loc Unsubscr Req: 0 Loc Unsubscr Rsp: 0
AP Monitor Rsp: 0 AP Monitor Req: 0
AP Monitor Notify: 64677
IDS Get Rsp: 0 IDS Get Req: 0
IDS Notif: 0
IDS Set Rsp: 0 IDS Set Req: 0

See the mobility services that are active on the controller by entering this command:

show nmsp subscription [summary | detail | detail ip_addr]

where

- **summary** shows all of the mobility services to which the controller is subscribed.
- **detail** shows details for all of the mobility services to which the controller is subscribed.
- **detail ip_addr** shows details only for the mobility services subscribed to by a specific IP address.

Information similar to the following appears for the show nmsp subscription summary command:

Mobility Services Subscribed:

<table>
<thead>
<tr>
<th>Server IP</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.4.93.31</td>
<td>RSSI, Info, Statistics</td>
</tr>
</tbody>
</table>

Information similar to the following appears for the show nmsp subscription detail ip_addr command:

Mobility Services Subscribed by 1.4.93.31

<table>
<thead>
<tr>
<th>Services</th>
<th>Sub-services</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
RSSI                     Mobile Station, Tags, Info                     Mobile Station, Statistics       Mobile Station, Tags,

- Clear all NMSP statistics by entering this command:
  clear nmsp statistics

**Debugging NMSP Issues**

Use these CLI commands if you experience any problems with NMSP:

- Configure NMSP debug options by entering this command:
  ```
  debug nmsp ?
  ``
  where ? is one of the following:
  - all {enable | disable}—Enables or disables debugging for all NMSP messages.
  - connection {enable | disable}—Enables or disables debugging for NMSP connection events.
  - detail {enable | disable}—Enables or disables debugging for NMSP detailed events.
  - error {enable | disable}—Enables or disables debugging for NMSP error messages.
  - event {enable | disable}—Enables or disables debugging for NMSP events.
  - message {tx | rx} {enable | disable}—Enables or disables debugging for NMSP transmit or receive messages.
  - packet {enable | disable}—Enables or disables debugging for NMSP packet events.

- Enable or disable debugging for NMSP interface events by entering this command:
  ```
  debug dot11 nmsp {enable | disable}
  ```

- Enable or disable debugging for IAPP NMSP events by entering this command:
  ```
  debug iapp nmsp {enable | disable}
  ```

- Enable or disable debugging for RFID NMSP messages by entering this command:
  ```
  debug rfid nmsp {enable | disable}
  ```

- Enable or disable debugging for access point monitor NMSP events by entering this command:
  ```
  debug service ap-monitor nmsp {enable | disable}
  ```

- Enable or disable debugging for wIPS NMSP events by entering this command:
  ```
  debug wips nmsp {enable | disable}
  ```

**Configuring and Viewing Location Settings**

This section contains the following topics:

- Information About Configuring and Viewing Location Settings, page 4-111
- Installing the Location Appliance Certificate, page 4-111
- Synchronizing the Controller and Location Appliance, page 4-112
- Configuring Location Settings, page 4-112
Information About Configuring and Viewing Location Settings

This section provides instructions to configure and view location settings from the controller CLI.

**Note**
Access points in monitor mode should not be used for location purposes.

Installing the Location Appliance Certificate

A self-signed certificate (SSC) is required on the location appliance. This certificate, which is comprised of the location appliance MAC address and a 20-byte key hash, must be present on the controller. Otherwise, the controller cannot authenticate the location appliance, and they can never establish a connection. WCS usually pushes the certificate to the controller automatically, but you can install the certificate on the controller using the controller CLI if necessary (for example, if the controller is not connected to WCS or if an error or certificate mismatch occurs on WCS).

**Note**
If an error occurs on WCS and prevents the location appliance certificate from being pushed to the controller, make sure that the time zone has been synchronized on the controller and the location appliance before following this procedure. Follow the instructions in the “Viewing Location Settings (CLI)” section on page 4-114 to do so.

To install the location appliance certificate on the controller using the controller CLI, follow these steps:

**Step 1**
Obtain the key hash value of the location appliance certificate by entering this command:
```
debug pm pki enable
```
Information similar to the following appears:
```
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key Data
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Key Data 30820122 300d0609 2a864886 f70d0101
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Key Data 01050003 82010f00 3082010a 02820101
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Key Data 009a98b5 d2b7c77b 036cd8b7 5bd20e5a
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Key Data 894c66f4 df1bcbcf fe2fcf01 09b723aa
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Key Data 5c0917f1 ec1d5061 2d386351 573f2c5e
Thu Oct 11 08:52:30 2007: sshpmGetIssuerHandles: Key Data b9020301 0001
Thu Oct 11 08:52:30 2007: sshpmGetIssuerHandles: Key Data 5c0917f1 ec1d5061 2d386351 573f2c5e
Thu Oct 11 08:52:30 2007: sshpmGetIssuerHandles: Key Data 4869b32638c00ffca88abe9b1a8e0525b9344b8b
```

**Step 2**
Install the location appliance certificate on the controller by entering this command:
```
config auth-list add lbs-ssc lbs_mac lbs_key
```
where
- `lbs_mac` is the MAC address of the location appliance.
- `lbs_key` is the 20-byte key hash value of the certificate.

**Step 3**
Save your changes by entering this command:
```
save config
```
Step 4 Verify that the location appliance certificate is installed on the controller by entering this command:

```
show auth-list
```

Information similar to the following appears:

```
Authorize APs against AAA ....................... disabled
Allow APs with Self-Signed Certificate (SSC) .... disabled

<table>
<thead>
<tr>
<th>Mac Addr</th>
<th>Cert Type</th>
<th>Key Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:16:36:91:9a:27</td>
<td>LBS-SSC</td>
<td>593f34e7cb151997a28cc7da2a6cac040b329636</td>
</tr>
</tbody>
</table>
```

Synchronizing the Controller and Location Appliance

For controller software release 4.2 or later releases, if a location appliance (release 3.1 or later releases) is installed on your network, the time zone must be set on the controller to ensure proper synchronization between the two systems. Also, the times must be synchronized on the two devices. We recommend that you set the time even for networks that do not have location appliances. See the “Configuring 802.11 Bands” section on page 4-25 for instructions on setting the time and date on the controller.

**Note**
The time zone can be different for the controller and the location appliance, but the time zone delta must be configured accordingly, based on GMT.

Configuring Location Settings

This section contains the following topics:

- Configuring Location Settings (CLI), page 4-112
- Viewing Location Settings (CLI), page 4-114

Configuring Location Settings (CLI)

The controller determines the location of client devices by gathering received signal strength indication (RSSI) measurements from access points all around the client of interest. The controller can obtain location reports from up to 16 access points for clients, RFID tags, and rogue access points.

Improve location accuracy by configuring the path loss measurement (S60) request for normal clients or calibrating clients by entering this command:

```
config location plm
```

where ? is one of the following:

- **client {enable | disable} burst_interval**—Enables or disables the path loss measurement request for normal, noncalibrating clients. The valid range for the `burst_interval` parameter is 1 to 3600 seconds, and the default value is 60 seconds.

- **calibrating {enable | disable} {uniband | multiband}**—Enables or disables the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio or on the associated 802.11a/b/g radio.
If a client does not send probes often or sends them only on a few channels, its location cannot be updated or cannot be updated accurately. The **config location plm** command forces clients to send more packets on all channels. When a CCXv4 (or higher) client associates, the controller sends it a path loss measurement request, which instructs the client to transmit on the bands and channels that the access points are on (typically, channels 1, 6, and 11 for 2.4-GHz-only access points) at a configurable interval (such as 60 seconds) indefinitely.

These four additional location CLI commands are available; however, they are set to optimal default values, so we do not recommend that you use or modify them:

- Configure the RSSI timeout value for various devices by entering this command:
  
  ```plaintext
  config location expiry 
  ```

  where ? is one of the following:

  - **client timeout**—Configures the RSSI timeout value for clients. The valid range for the **timeout** parameter is 5 to 3600 seconds, and the default value is 5 seconds.
  - **calibrating-client timeout**—Configures the RSSI timeout value for calibrating clients. The valid range for the **timeout** parameter is 0 to 3600 seconds, and the default value is 5 seconds.
  - **tags timeout**—Configures the RSSI timeout value for RFID tags. The valid range for the **timeout** parameter is 5 to 300 seconds, and the default value is 5 seconds.
  - **rogue-aps timeout**—Configures the RSSI timeout value for rogue access points. The valid range for the **timeout** parameter is 5 to 3600 seconds, and the default value is 5 seconds.

  Ensuring that recent, strong RSSIs are retained by the CPU is critical to location accuracy. The **config location expiry** command enables you to specify the length of time after which old RSSI averages expire.

  **Note** We recommend that you do not use or modify the **config location expiry** command.

- Configure the RSSI half life for various devices by entering this command:

  ```plaintext
  config location rssi-half-life 
  ```

  where ? is one of the following:

  - **client half_life**—Configures the RSSI half life for clients. The valid range for the **half_life** parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.
  - **calibrating-client half_life**—Configures the RSSI half life for calibrating clients. The valid range for the **half_life** parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.
  - **tags half_life**—Configures the RSSI half life for RFID tags. The valid range for the **half_life** parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.
  - **rogue-aps half_life**—Configures the RSSI half life for rogue access points. The valid range for the **half_life** parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.

  Some client devices transmit at reduced power immediately after changing channels, and RF is variable, so RSSI values might vary considerably from packet to packet. The **config location rssi-half-life** command increases accuracy by averaging nonuniformly arriving data using a configurable forget period (or half life).
Configuring and Viewing Location Settings

Note
We recommend that you do not use or modify the `config location rssi-half-life` command.

- Configure the NMSP notification threshold for RSSI measurements by entering this command:
  
  `config location notify-threshold` ?

  where `?` is one of the following:

  - `client threshold`—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the `threshold` parameter is 0 to 10 dB, and the default value is 0 dB.
  
  - `tags threshold`—Configures the NMSP notification threshold (in dB) for RFID tags. The valid range for the `threshold` parameter is 0 to 10 dB, and the default value is 0 dB.
  
  - `rogue-aps threshold`—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the `threshold` parameter is 0 to 10 dB, and the default value is 0 dB.

Note
We recommend that you do not use or modify the `config location notify-threshold` command.

- Configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command:
  
  `config location algorithm` ?

  where `?` is one of the following:

  - `simple`—Specifies a faster algorithm that requires low CPU overhead but provides less accuracy.
  
  - `rssi-average`—Specifies a more accurate algorithm but requires more CPU overhead.

Note
We recommend that you do not use or modify the `config location algorithm` command.

Viewing Location Settings (CLI)

To view location information, use these CLI commands:

- View the current location configuration values by entering this command:
  
  `show location summary`

  Information similar to the following appears:

  Location Summary

  Algorithm used: Average
  Client
  RSSI expiry timeout: 5 sec
  Half life: 0 sec
  Notify Threshold: 0 db
  Calibrating Client
  RSSI expiry timeout: 5 sec
  Half life: 0 sec
  Calibrating Rogue AP
  RSSI expiry timeout: 5 sec
  Calibrating Rogue AP
  RSSI expiry timeout: 5 sec
Chapter 4  Configuring Controller Settings

Configuring and Viewing Location Settings

- See the RSSI table for a particular client by entering this command:

  `show location detail client_mac_addr`

  Information similar to the following appears:

  ```
  ...[11] AP 00:00:00:00:00:00 : Slot 0 inUse 0, expired 0, Timestamp (antenna-A 0) (antenna-B 0), band 0 rssi (antenna-A 0) (antenna-B 0), snr 0, acceptable 0
  [12] AP 00:00:00:00:00:00 : Slot 0 inUse 0, expired 0, Timestamp (antenna-A 0) (antenna-B 0), band 0 rssi (antenna-A 0) (antenna-B 0), snr 0, acceptable 0
  [13] AP 00:00:00:00:00:00 : Slot 0 inUse 0, expired 0, Timestamp (antenna-A 0) (antenna-B 0), band 0 rssi (antenna-A -1) (antenna-B 0), snr 0, acceptable 0
  [14] AP 00:00:00:00:00:00 : Slot 0 inUse 0, expired 0, Timestamp (antenna-A 0) (antenna-B 0), band 0 rssi (antenna-A 0) (antenna-B 0), snr 0, acceptable 0
  [15] AP 00:00:00:00:00:00 : Slot 0 inUse 0, expired 0, Timestamp (antenna-A 0) (antenna-B 0), band 0 rssi (antenna-A 0) (antenna-B 0), snr 0, acceptable 0
  ```

- See the location-based RFID statistics by entering this command:

  `show location statistics rfid`

  Information similar to the following appears:

  ```
  RFID Statistics
  Database Full : 0 Failed Delete: 0
  Null Bufhandle: 0 Bad Packet: 0
  Bad LWAPP Data: 0 Bad LWAPP Encap: 0
  Off Channel: 0 Bad CCX Version: 0
  Bad AP Info : 0
  Above Max RSSI: 0 Below Max RSSI: 0
  Invalid RSSI: 0 Add RSSI Failed: 0
  Oldest Expired RSSI: 0 Smallest Overwrite: 0
  ```

- Clear the location-based RFID statistics by entering this command:

  `clear location statistics rfid`

- Clear a specific RFID tag or all of the RFID tags in the entire database by entering this command:

  `clear location rfid {mac_address | all}`

- See whether location presence (S69) is supported on a client by entering this command:

  `show client detail client_mac`

  When location presence is supported by a client and enabled on a location appliance, the location appliance can provide the client with its location upon request. Location presence is enabled automatically on CCXv5 clients.

  Information similar to the following appears:

  ```
  Client MAC Address............................... 00:40:96:b2:a3:44
  Client Username ................................. N/A
  AP MAC Address................................ 00:18:74:c7:c0:90
  Client State..................................... Associated
  Wireless LAN Id................................. 1
  BSSID............................................ 00:18:74:c7:c0:9f
  Channel......................................... 56
  ```
Using the Wireless LAN Controller Network Module

Follow these guidelines when using a wireless LAN controller network module (CNM) installed in a Cisco Integrated Services Router:

- The CNM does not support IPsec. To use IPsec with the CNM, configure IPsec on the router in which the CNM is installed. Click this link to browse IPsec configuration instructions for routers:

- The CNM does not have a battery and cannot save a time setting. It must receive a time setting from an external NTP server when it powers up. When you install the module, the configuration wizard prompts you for NTP server information.

- To access the CNM bootloader, we recommend that you reset the CNM from the router. If you reset the CNM from a CNM user interface, the router might reset the CNM while you are using the bootloader.

  When you reset the CNM from a CNM interface, you have 17 minutes to use the bootloader before the router automatically resets the CNM. The CNM bootloader does not run the Router Blade Configuration Protocol (RBCP), so the RBCP heartbeat running on the router times out after 17 minutes, triggering a reset of the CNM.

  If you reset the CNM from the router, the router stops the RBCP heartbeat exchange and does not restart it until the CNM boots up. To reset the CNM from the router, enter one of these commands on the router CLI:

  - service-module wlan-controller 1/0 reset (for Fast Ethernet CNM versions)
  - service-module integrated-service-engine 1/0 reset (for Gigabit Ethernet CNM versions)

- Gigabit Ethernet versions of the Controller Network Module are supported on Cisco 28/37/38xx Series Integrated Services Routers running Cisco IOS Release 12.4(11)T2 or later.

Resetting the Controller to Default Settings

This section contains the following topics:
Information About Resetting the Controller to Default Settings

You can return the controller to its original configuration by resetting the controller to factory-default settings.

Resetting the Controller to Default Settings

This section contains the following topics:

- Resetting the Controller to Default Settings (GUI), page 4-117
- Resetting the Controller to Default Settings (CLI), page 4-117

Resetting the Controller to Default Settings (GUI)

Step 1  Start your Internet browser.
Step 2  Enter the controller IP address in the browser address line and press Enter. An Enter Network Password dialog box appears.
Step 3  Enter your username in the User Name text box. The default username is admin.
Step 4  Enter the wireless device password in the Password text box and press Enter. The default password is admin.
Step 5  Choose Commands > Reset to Factory Default.
Step 6  Click Reset.
Step 7  When prompted, confirm the reset.
Step 8  Reboot the controller without saving the configuration.
Step 9  Use the configuration wizard to enter configuration settings. See the “Configuring the Controller Using the GUI Configuration Wizard” section on page 3-1 for instructions.

Resetting the Controller to Default Settings (CLI)

Step 1  Enter the reset system command. At the prompt that asks whether you need to save changes to the configuration, enter N. The unit reboots.
Step 2  When you are prompted for a username, enter the recover-config command to restore the factory-default configuration. The controller reboots and displays this message:

Welcome to the Cisco WLAN Solution Wizard Configuration Tool

Step 3  Use the configuration wizard to enter configuration settings. See the “Configuring the Controller Using the GUI Configuration Wizard” section on page 3-1 for instructions.
CHAPTER 6

Configuring VideoStream

This chapter contains these sections:

- Information About VideoStream, page 6-1
- Guidelines and Limitations, page 6-1
- Configuring VideoStream, page 6-2

Information About VideoStream

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. As a result, if any multicast packet is lost in the air, it is not sent again which may cause an IP multicast stream unviewable.

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.

Guidelines and Limitations

Follow these guidelines when you configure VideoStream on the controller:

- The AP1100 and AP1200 do not support the reliable multicast feature.
- Make sure that the multicast feature is enabled. We recommend configuring IP multicast on the controller with multicast-multicast mode.
- Check for the IP address on the client machine. The machine should have an IP address from the respective VLAN.
- If there is a mismatch in the version of code on your controller, upgrade the controller code to 7.0.98.0 or later.
- Verify that the access points have joined the controllers.
- Make sure that the clients are able to associate to the configured WLAN at 802.11n speed.
- VideoStream is supported on the following access points: Cisco Aironet 3600, 3500, 1260, 1250, 1240, 1140, 1130, and 1040.
Configuring VideoStream

This section contains the following topics:

- Configuring the VideoStream on the Controller (GUI), page 6-2
- Configuring the VideoStream on the Controller (CLI), page 6-6
- Viewing and Debugging Media Streams, page 6-7

Configuring the VideoStream on the Controller (GUI)

**Step 1** Enable the multicast feature:

a. Select the **Multicast Direct Feature** check box to enable the multicast direct feature. The default value is disabled.

   **Note** Enabling the Multicast Direct feature does not automatically reset the existing client state. The wireless clients must rejoin the multicast stream after enabling the Multicast Direct feature on the controller.

b. Under the Session Message Config, select **Session announcement State** to enable the session announcement mechanism. If this feature is enabled, clients are informed each time a controller is not able to serve the multicast direct data to the client.

c. In the Session announcement URL text box, enter the URL where the client can find more information when an error occurs during the multicast media stream transmission.

d. In the Session announcement e-mail text box, enter the e-mail address of the person who can be contacted.

e. In the Session announcement Phone text box, enter the phone number of the person who can be contacted.

f. In the Session announcement Note text box, enter a reason as to why a particular client cannot be served with a multicast media.

g. Click **Apply** to commit your changes.

**Step 2** Add a media stream:

a. Choose **Wireless > Media Stream > Streams** to open the Media Stream page.

b. Click **Add New** to configure a new media stream. The Media Stream > New page appears.

   **Note** The Stream Name, Multicast Destination Start IP Address (IPv4 or IPv6), and Multicast Destination End IP Address (IPv4 or IPv6) text boxes are mandatory. You must enter information in these text boxes.

c. In the Stream Name text box, enter the media stream name. The stream name can be up to 64 characters.

d. In the Multicast Destination Start IP Address (IPv4 or IPv6) text box, enter the start IPv4 or IPv6 address of the multicast media stream.
Chapter 6 Configuring VideoStream

e. In the Multicast Destination End IP Address (IPv4 or IPv6) text box, enter the end IPv4 or IPv6 address of the multicast media stream.

f. In the Maximum Expected Bandwidth text box, enter the maximum expected bandwidth that you want to assign to the media stream. The values can range between 1 to 35000 kbps.

Note We recommend that you use a template to add a media stream to the controller.

g. From the Select from Predefined Templates drop-down list under Resource Reservation Control (RRC) Parameters, choose one of the following options to specify the details about the resource reservation control:
   - Very Coarse (below 300 kbps)
   - Coarse (below 500 kbps)
   - Ordinary (below 750 kbps)
   - Low (below 1 Mbps)
   - Medium (below 3 Mbps)
   - High (below 5 Mbps)

Note When you select a predefined template from the drop-down list, the following text boxes under the Resource Reservation Control (RRC) Parameters list their default values that are assigned with the template.

   - Average Packet Size (100-1500 bytes)—Specifies the average packet size. The value can be in the range of 100 to 1500 bytes. The default value is 1200.
   - RRC Periodic update—Enables the RRC (Resource Reservation Control Check) Periodic update. By default, this option is enabled. RRC periodically updates the admission decision on the admitted stream according to the correct channel load. As a result, it may deny certain low priority admitted stream requests.
   - RRC Priority (1-8)—Specifies the priority bit set in the media stream. The priority can be any number between 1 and 8. The larger the value means the higher the priority is. For example, a priority of 1 is the lowest value and a value of 8 is the highest value. The default priority is 4. The low priority stream may be denied in the RRC periodic update.
   - Traffic Profile Violation—Specifies the action to perform in case of a violation after a re-RRC. Choose an action from the drop-down list. The possible values are as follows:
     - Drop—Specifies that a stream is dropped on periodic reevaluation.
     - Fallback—Specifies that a stream is demoted to Best Effort class on periodic reevaluation. The default value is drop.

h. Click Apply to save the configuration changes.

Step 3 Enable the media stream for multicast-direct:

a. Choose WLANs > WLAN ID to open the WLANs > Edit page.

b. Choose the QoS tab and select Gold (Video) from the Quality of Service (QoS) drop-down list.

c. Enable Multicast Direct.

d. Click Apply to save the configuration changes.
Step 4 Set the EDCA parameters to voice and video optimized (optional):
   a. Choose Wireless > 802.11a/n or 802.11b/g/n > EDCA Parameters.
   b. From the EDCA Profile drop-down list, choose the Voice and Video Optimized option.
   c. Click Apply to save the changes made.

Step 5 Enable the admission control on a band for video (optional):

Note Keep the voice bandwidth allocation to a minimum for better performance.

   a. Choose Wireless > 802.11a/n or 802.11b/g/n > Media to open the 802.11a/n (5 GHZ) or 802.11b/g/n > Media page.
   b. Choose the Video tab.
   c. Select the Admission Control (ACM) check box to enable bandwidth-based CAC for this radio band. The default value is disabled.
   d. Click Apply to save the configuration changes.

Step 6 Configure the video bandwidth:

Note The template bandwidth that is configured for a media stream should be more than the bandwidth for the source media stream.

Note The voice configuration is optional. Keep the voice bandwidth allocation to a minimum for better performance.

   a. Choose Wireless > 802.11a/n or 802.11b/g/n > Media to open the 802.11a/n (5 GHZ) or 802.11b/g/n > Media page.
   b. Choose the Video tab.
   c. Select the Admission Control (ACM) check box to enable the video CAC for this radio band. The default value is disabled.
   d. In the Max RF Bandwidth field, enter the percentage of the maximum bandwidth allocated to clients for video applications on this radio band. Once the client reaches the value specified, the access point rejects new requests on this radio band.
   e. The range is 5 to 85%.
   f. The default value is 9%.
   g. Click Apply to commit your changes.
   h. Reenable all WMM WLANs and click Apply.

Step 7 Configure the media bandwidth:

   a. Choose Wireless > 802.11a/n or 802.11b/g/n > Media to open the 802.11a (or 802.11b) > Media > Parameters page.
   b. Choose the Media tab to open the Media page.
   c. Select the Unicast Video Redirect check box to enable Unicast Video Redirect. The default value is disabled.
d. In the Maximum Media Bandwidth (0-85%) text box, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches a specified value, the access point rejects new calls on this radio band.

e. The default value is 85%; valid values are from 0 to 85%.

f. In the Client Phy Rate field, enter the minimum transmission data rate to the client. If the transmission data rate is below the phy rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

g. In the Maximum Retry Percent (0-100%) field, enter the percentage of maximum retries that are allowed. The default value is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

h. Select the Multicast Direct Enable check box to enable the Multicast Direct Enable field. The default value is enabled.

i. From the Max Streams per Radio drop-down list, choose the maximum number of streams allowed per radio from the range 0 to 20. The default value is set to auto. If you choose auto, there is no limit set for the number of client subscriptions.

j. From the Max Streams per Client drop-down list, choose the maximum number of streams allowed per client from the range 0 to 20. The default value is set to auto. If you choose auto, there is no limit set for the number of client subscriptions.

k. Select the Best Effort QoS Admission check box to enable best-effort QoS admission.

l. Click Apply to save the configuration changes.

---

**Step 8**
Enable WLANs:

a. Choose WLANS > WLAN ID. The WLANs > Edit page appears.

b. Enable the VideoStream feature for the WLAN.

c. Select the Status check box to enable the WLAN.

d. Click Apply to commit your changes.

**Step 9**
Enable the 802.11 a/n or 802.11 b/g/n network:

a. Choose Wireless > Wireless > 802.11a/n or 802.11b/g/n > Network.

b. Select the 802.11a or 802.11b/g Network Status check box to enable the network status.

c. Click Apply to commit your changes.

**Step 10**
Verify that the clients are associated with the multicast groups and group-ides:


b. Check if the 802.11a or 802.11b/g network clients have the associated access points.


d. Select the MGID check box for the VideoStream to the clients.

e. Click MGID. The Multicast Group Detail page appears. Check the Multicast Status details.
Configuring the VideoStream on the Controller (CLI)

**Step 1** Configure the multicast-direct feature on WLANs media stream by entering this command:

```
config wlan media-stream multicast-direct {wlan_id | all} {enable | disable}
```

**Step 2** Enable or disable the multicast feature by entering this command:

```
config media-stream multicast-direct {enable | disable}
```

**Step 3** Configure various message configuration parameters by entering this command:

```
config media-stream message {state [enable | disable] | url url | email email | phone phone_number | note note}
```

**Step 4** Save your changes by entering this command:

```
save config
```

**Step 5** Configure various global media-stream configurations by entering this command:

```
config media-stream add multicast-direct stream-name media_stream_name start_IP end_IP [template {very-coarse | coarse | ordinary | low-resolution | med-resolution | high-resolution}] [detail {Max_bandwidth bandwidth | packet_size packet_size | Re-evaluation re-evaluation {periodic | initial}}] video video priority {drop | fallback}
```

**Note**
- The Resource Reservation Control (RRC) parameters are assigned with the predefined values based on the values assigned to the template.
- The following templates are used to assign RRC parameters to the media stream:
  - Very Coarse (below 3000 kbps)
  - Coarse (below 500 kbps)
  - Ordinary (below 750 kbps)
  - Low Resolution (below 1 mbps)
  - Medium Resolution (below 3 mbps)
  - High Resolution (below 5 mbps)

**Step 6** Delete a media stream by entering this command:

```
config media-stream delete media_stream_name
```

**Step 7** Enable a specific enhanced distributed channel access (EDC) profile by entering this command:

```
config advanced {801.11a | 802.11b} edca-parameters optimized-video-voice
```

**Step 8** Enable the admission control on the desired bandwidth by entering the following commands:

- Enable bandwidth-based voice CAC for 802.11a or 802.11b/g network by entering this command:
  
  ```
  config {802.11a | 802.11b} cac voice acm enable
  ```
- Set the percentage of the maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network by entering this command:
  
  ```
  config {802.11a | 802.11b} cac voice max-bandwidth bandwidth
  ```
- Configure the percentage of the maximum allocated bandwidth reserved for roaming voice clients on the 802.11a or 802.11b/g network by entering this command:
  
  ```
  config {802.11a | 802.11b} cac voice roam-bandwidth bandwidth
  ```
Chapter 6  Configuring VideoStream

Step 9  Set the maximum number of streams per radio and/or per client by entering these commands:

- Set the maximum limit to the number multicast streams per radio by entering this command:
  `config {802.11a | 802.11b} media-stream multicast-direct radio-maximum [value | ‘no-limit’]

- Set the maximum number of multicast streams per client by entering this command:
  `config {802.11a | 802.11b} media-stream multicast-direct client-maximum [value | ‘no-limit’]

Step 10  Save your changes by entering this command:
`save config`

Viewing and Debugging Media Streams

- See the configured media streams by entering this command:
  `show wlan wlan_id`

- See the details of the media stream name by entering this command:
  `show 802.11{a | b | h} media-stream media-stream_name`

- See the clients for a media stream by entering this command:
  `show 802.11a media-stream client media-stream-name`

- See a summary of the media stream and client information by entering this command:
  `show media-stream group summary`

- See details about a particular media stream group by entering this command:
  `show media-stream group detail media_stream_name`

- See details of the 802.11a or 802.11b media resource reservation configuration by entering this command:
  `show {802.11a | 802.11b} media-stream rrc`

- Enable debugging of the media stream history by entering this command:
  `debug media-stream history {enable | disable}`
CHAPTER 7

Configuring Security Solutions

This chapter contains the following sections:

- Configuring RADIUS, page 7-3
- Configuring TACACS+, page 7-17
- Configuring Maximum Local Database Entries, page 7-26
- Configuring Local Network Users on the Controller, page 7-27
- Configuring Password Policies, page 7-30
- Configuring LDAP, page 7-31
- Configuring Local EAP, page 7-36
- Configuring the System for SpectraLink NetLink Telephones, page 7-47
- Using Management Over Wireless, page 7-51
- Using Dynamic Interfaces for Management, page 7-52
- Configuring DHCP Option 82, page 7-53
- Configuring and Applying Access Control Lists, page 7-56
- Configuring Management Frame Protection, page 7-66
- Configuring Client Exclusion Policies, page 7-72
- Configuring Identity Networking, page 7-75
- Managing Rogue Devices, page 7-81
- Configuring Cisco TrustSec SXP, page 7-102
- Configuring Cisco Intrusion Detection System, page 7-106
- Configuring wIPS, page 7-121
- Configuring Wi-Fi Direct Client Policy, page 7-129
- Configuring Web Auth Proxy, page 7-130
- Detecting Active Exploits, page 7-132
Information about Cisco Unified Wireless Network Solution Security

This section contains the following topics:

- Security Overview, page 7-2
- Layer 1 Solutions, page 7-2
- Layer 2 Solutions, page 7-2
- Layer 3 Solutions, page 7-3
- Integrated Security Solutions, page 7-3

Security Overview

The Cisco Unified Wireless Network (UWN) security solution bundles potentially complicated Layer 1, Layer 2, and Layer 3 802.11 Access Point security components into a simple policy manager that customizes system-wide security policies on a per-WLAN basis. The Cisco UWN security solution provides simple, unified, and systematic security management tools.

One of the biggest hurdles to WLAN deployment in the enterprise is WEP encryption, which is a weak standalone encryption method. A newer problem is the availability of low-cost access points, which can be connected to the enterprise network and used to mount man-in-the-middle and denial-of-service attacks.

Layer 1 Solutions

The Cisco UWN security solution ensures that all clients gain access within a user-set number of attempts. If a client fails to gain access within that limit, it is automatically excluded (blocked from access) until the user-set timer expires. The operating system can also disable SSID broadcasts on a per-WLAN basis.

Layer 2 Solutions

If a higher level of security and encryption is required, you can also implement industry-standard security solutions such as Extensible Authentication Protocol (EAP), Wi-Fi Protected Access (WPA), and WPA2. The Cisco UWN solution WPA implementation includes AES (Advanced Encryption Standard), TKIP and Michael (temporal key integrity protocol and message integrity code checksum) dynamic keys, or WEP (Wired Equivalent Privacy) static keys. Disabling is also used to automatically block Layer 2 access after a user-set number of failed authentication attempts.

Regardless of the wireless security solution selected, all Layer 2 wired communications between controllers and lightweight access points are secured by passing data through CAPWAP tunnels.

Cisco Aironet client adapter version 4.2 does not authenticate if WPA/WPA2 is used with CCKM as auth key management and a 2 second latency between the controller and AP.
Layer 3 Solutions

The WEP problem can be further solved using industry-standard Layer 3 security solutions such as passthrough VPNs (virtual private networks).

The Cisco UWN solution supports local and RADIUS MAC (media access control) filtering. This filtering is best suited to smaller client groups with a known list of 802.11 access card MAC addresses.

The Cisco UWN solution supports local and RADIUS user/password authentication. This authentication is best suited to small to medium client groups.

Integrated Security Solutions

The integrated security solutions are as follows:

- Cisco Unified Wireless Network (UWN) solution operating system security is built around a 802.1X AAA (authorization, authentication and accounting) engine, which allows users to rapidly configure and enforce a variety of security policies across the Cisco UWN solution.
- The controllers and lightweight access points are equipped with system-wide authentication and authorization protocols across all ports and interfaces, maximizing system security.
- Operating system security policies are assigned to individual WLANs, and lightweight access points simultaneously broadcast all (up to 16) configured WLANs, which can eliminate the need for additional access points, which can increase interference and degrade system throughput.
- Operating system security uses the RRM function to continually monitor the air space for interference and security breaches and to notify the user when they are detected.
- Operating system security works with industry-standard authorization, authentication, and accounting (AAA) servers.

Configuring RADIUS

This section contains the following topics:

- Information About RADIUS, page 7-3
- Guidelines and Limitations, page 7-4
- Configuring RADIUS on the ACS, page 7-5
- Configuring RADIUS, page 7-6
- RADIUS Authentication Attributes Sent by the Access Point, page 7-14
- RADIUS Accounting Attributes, page 7-16

Information About RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol that provides centralized security for users attempting to gain management access to a network. It serves as a backend database similar to local and TACACS+ and provides authentication and accounting services:

- Authentication—The process of verifying users when they attempt to log into the controller.
Users must enter a valid username and password in order for the controller to authenticate users to the RADIUS server. If multiple databases are configured, you can specify the sequence in which the backend database must be tried.

- **Accounting**—The process of recording user actions and changes.
  Whenever a user successfully executes an action, the RADIUS accounting server logs the changed attributes, the user ID of the person who made the change, the remote host where the user is logged in, the date and time when the command was executed, the authorization level of the user, and a description of the action performed and the values provided. If the RADIUS accounting server becomes unreachable, users are able to continue their sessions uninterrupted.

RADIUS uses User Datagram Protocol (UDP) for its transport. It maintains a database and listens on UDP port 1812 for incoming authentication requests and UDP port 1813 for incoming accounting requests. The controller, which requires access control, acts as the client and requests AAA services from the server. The traffic between the controller and the server is encrypted by an algorithm defined in the protocol and a shared secret key configured on both devices.

You can configure multiple RADIUS accounting and authentication servers. For example, you may want to have one central RADIUS authentication server but several RADIUS accounting servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the controller automatically tries the second one, then the third one if necessary, and so on.

### Guidelines and Limitations

This section contains the following topics:

- **RADIUS Server Support**, page 7-4
- **Radius ACS Support**, page 7-4
- **Primary and Fallback RADIUS Servers**, page 7-5

### RADIUS Server Support

- You can configure up to 17 RADIUS authentication and accounting servers each.
- If multiple RADIUS servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.
- To create a read-only controller user on the RADIUS server, you must set the service type to NAS prompt instead of Callback NAS prompt. If you set the service type to Callback NAS Prompt, the user authentication fails while setting it to NAS prompt gives the user read-only access to the controller.
  Also, the Callback Administrative service type gives the user the lobby ambassador privileges to the controller.

### Radius ACS Support

- You must configure RADIUS on both your CiscoSecure Access Control Server (ACS) and your controller.
- RADIUS is supported on CiscoSecure ACS version 3.2 and later releases. See the CiscoSecure ACS documentation for the version that you are running.
Primary and Fallback RADIUS Servers

The primary RADIUS server (the server with the lowest server index) is assumed to be the most preferable server for the controller. If the primary server becomes unresponsive, the controller switches to the next active backup server (the server with the next lowest server index). The controller continues to use this backup server, unless you configure the controller to fall back to the primary RADIUS server when it recovers and becomes responsive or to a more preferable server from the available backup servers.

Configuring RADIUS on the ACS

**Step 1** Choose Network Configuration on the ACS main page.

**Step 2** Choose Add Entry under AAA Clients to add your controller to the server. The Add AAA Client page appears.

**Step 3** In the AAA Client Hostname text box, enter the name of your controller.

**Step 4** In the AAA Client IP Address text box, enter the IP address of your controller.

**Step 5** In the Shared Secret text box, enter the shared secret key to be used for authentication between the server and the controller.

**Note** The shared secret key must be the same on both the server and the controller.
Step 6  From the Authenticate Using drop-down list, choose RADIUS (Cisco Aironet).
Step 7  Click Submit + Apply to save your changes.
Step 8  Choose Interface Configuration on the ACS main page.
Step 9  Choose RADIUS (Cisco Aironet). The RADIUS (Cisco Aironet) page appears.
Step 10 Under User Group, select the Cisco-Aironet-Session-Timeout check box.
Step 11 Click Submit to save your changes.
Step 12 On the ACS main page, from the left navigation pane, choose System Configuration.
Step 13 Choose Logging.
Step 14 When the Logging Configuration page appears, enable all of the events that you want to be logged and save your changes.
Step 15 On the ACS main page, from the left navigation pane, choose Group Setup.
Step 16 Choose a previously created group from the Group drop-down list.

Note  This step assumes that you have already assigned users to groups on the ACS according to the roles to which they will be assigned.

Step 17 Click Edit Settings. The Group Setup page appears.
Step 18 Under Cisco Aironet Attributes, select the Cisco-Aironet-Session-Timeout check box and enter a session timeout value in the edit box.
Step 19 Specify read-only or read-write access to controllers through RADIUS authentication, by setting the Service-Type attribute (006) to Callback NAS Prompt for read-only access or to Administrative for read-write privileges. If you do not set this attribute, the authentication process completes successfully (without an authorization error on the controller), but you might be prompted to authenticate again.

Note  If you set the Service-Type attribute on the ACS, make sure to select the Management check box on the RADIUS Authentication Servers page of the controller GUI. See Step 16 in the next section for more information.

Note  The “RADIUS Authentication Attributes Sent by the Access Point” section on page 7-14 lists the RADIUS attributes that are sent by a lightweight access point to a client in access-request and access-accept packets.

Step 20 Click Submit to save your changes.

Configuring RADIUS

This section contains the following topics:

- Configuring RADIUS (GUI), page 7-7
- Configuring RADIUS (CLI), page 7-10
Configuring RADIUS (GUI)

**Step 1** Choose Security > AAA > RADIUS.

**Step 2** Perform one of the following:
- If you want to configure a RADIUS server for authentication, choose Authentication.
- If you want to configure a RADIUS server for accounting, choose Accounting.

**Note** The pages used to configure authentication and accounting contain mostly the same text boxes. Therefore, these instructions walk through the configuration only once, using the Authentication pages as examples. You would follow the same steps to configure multiple services and/or multiple servers.

The RADIUS Authentication (or Accounting) Servers page appears.

**Figure 7-2 RADIUS Authentication Servers Page**

This page lists any RADIUS servers that have already been configured.
- If you want to delete an existing server, hover your cursor over the blue drop-down arrow for that server and choose Remove.
- If you want to make sure that the controller can reach a particular server, hover your cursor over the blue drop-down arrow for that server and choose Ping.

**Step 3** From the Call Station ID Type drop-down list, choose IP Address, System MAC Address, or AP MAC Address to specify whether the IP address, system MAC address, or AP MAC address of the originator will be sent to the RADIUS server in the Access-Request message.

**Step 4** Enable RADIUS-to-controller key transport using AES key wrap protection by selecting the Use AES Key Wrap check box. The default value is unselected. This feature is required for FIPS customers.

**Step 5** Click Apply to commit your changes. Perform one of the following:
- To edit an existing RADIUS server, click the server index number for that server. The RADIUS Authentication (or Accounting) Servers > Edit page appears.
- To add a RADIUS server, click New. The RADIUS Authentication (or Accounting) Servers > New page appears.

**Step 6** If you are adding a new server, choose a number from the Server Index (Priority) drop-down list to specify the priority order of this server in relation to any other configured RADIUS servers providing the same service.
Chapter 7     Configuring Security Solutions

Configuring RADIUS

Step 7  If you are adding a new server, enter the IP address of the RADIUS server in the Server IP Address text box.

Step 8  From the Shared Secret Format drop-down list, choose ASCII or Hex to specify the format of the shared secret key to be used between the controller and the RADIUS server. The default value is ASCII.

Step 9  In the Shared Secret and Confirm Shared Secret text boxes, enter the shared secret key to be used for authentication between the controller and the server.

**Note**  The shared secret key must be the same on both the server and the controller.

Step 10 If you are configuring a new RADIUS authentication server and want to enable AES key wrap, which makes the shared secret between the controller and the RADIUS server more secure, follow these steps:

**Note**  AES key wrap is designed for Federal Information Processing Standards (FIPS) customers and requires a key-wrap compliant RADIUS authentication server.

a. Select the Key Wrap check box.
b. From the Key Wrap Format drop-down list, choose ASCII or HEX to specify the format of the AES key wrap keys: Key Encryption Key (KEK) and Message Authentication Code Key (MACK).
c. In the Key Encryption Key (KEK) text box, enter the 16-byte KEK.
d. In the Message Authentication Code Key (MACK) text box, enter the 20-byte KEK.

Step 11 If you are adding a new server, enter the RADIUS server’s UDP port number for the interface protocols in the Port Number text box. The valid range is 1 to 65535, and the default value is 1812 for authentication and 1813 for accounting.

Step 12 From the Server Status text box, choose Enabled to enable this RADIUS server or choose Disabled to disable it. The default value is enabled.

Step 13 If you are configuring a new RADIUS authentication server, choose Enabled from the Support for RFC 3576 drop-down list to enable RFC 3576, which is an extension to the RADIUS protocol that allows dynamic changes to a user session, or choose Disabled to disable this feature. The default value is Enabled. RFC 3576 includes support for disconnecting users and changing authorizations applicable to a user session and supports disconnect and change-of-authorization (CoA) messages. Disconnect messages cause a user session to be terminated immediately where CoA messages modify session authorization attributes such as data filters.

Step 14 In the Server Timeout text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

**Note**  We recommend that you increase the timeout value if you experience repeated reauthentication attempts or the controller falls back to the backup server when the primary server is active and reachable.

Step 15 Select the Network User check box to enable network user authentication (or accounting), or unselect it to disable this feature. The default value is selected. If you enable this feature, this entry is considered the RADIUS authentication (or accounting) server for network users. If you did not configure a RADIUS server entry on the WLAN, you must enable this option for network users.
Step 16  If you are configuring a RADIUS authentication server, select the Management check box to enable management authentication, or unselect it to disable this feature. The default value is selected. If you enable this feature, this entry is considered the RADIUS authentication server for management users, and authentication requests go to the RADIUS server.

Step 17  Select the IPSec check box to enable the IP security mechanism, or unselect it to disable this feature. The default value is unselected.

Note  The IPsec option appears only if a crypto card is installed in the controller.

Step 18  If you enabled IPsec in Step 17, follow these steps to configure additional IPsec parameters:

a. From the IPSec drop-down list, choose one of the following options as the authentication protocol to be used for IP security: HMAC MD5 or HMAC SHA1. The default value is HMAC SHA1.

   A message authentication code (MAC) is used between two parties that share a secret key to validate information transmitted between them. HMAC (Hash MAC) is based on cryptographic hash functions. It can be used in combination with any iterated cryptographic hash function. HMAC MD5 and HMAC SHA1 are two constructs of the HMAC using the MD5 hash function and the SHA1 hash function. HMAC also uses a secret key for calculation and verification of the message authentication values.

b. From the IPSec Encryption drop-down list, choose one of the following options to specify the IP security encryption mechanism:

   • DES—Data Encryption Standard that is a method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.
   • 3DES—Data Encryption Standard that applies three keys in succession. This is the default value.
   • AES CBS—Advanced Encryption Standard that uses keys with a length of 128, 192, or 256 bits to encrypt data blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses a 128-bit data path in Cipher Clock Chaining (CBC) mode.

c. From the IKE Phase 1 drop-down list, choose one of the following options to specify the Internet Key Exchange (IKE) protocol: Aggressive or Main. The default value is Aggressive.

   IKE Phase 1 is used to negotiate how IKE should be protected. Aggressive mode passes more information in fewer packets with the benefit of slightly faster connection establishment at the cost of transmitting the identities of the security gateways in the clear.

d. In the Lifetime text box, enter a value (in seconds) to specify the timeout interval for the session. The valid range is 1800 to 57600 seconds, and the default value is 1800 seconds.

e. From the IKE Diffie Hellman Group drop-down list, choose one of the following options to specify the IKE Diffie Hellman group: Group 1 (768 bits), Group 2 (1024 bits), or Group 5 (1536 bits). The default value is Group 1 (768 bits).

   Diffie-Hellman techniques are used by two devices to generate a symmetric key through which they can publicly exchange values and generate the same symmetric key. Although all three groups provide security from conventional attacks, Group 5 is considered more secure because of its larger key size. However, computations involving Group 1 and Group 2 based keys might occur slightly faster because of their smaller prime number size.

Step 19  Click Apply to commit your changes.

Step 20  Click Save Configuration to save your changes.

Step 21  Repeat the previous steps if you want to configure any additional services on the same server or any additional RADIUS servers.
Chapter 7  Configuring Security Solutions

Step 22  Specify the RADIUS server fallback behavior, as follows:

a. Choose Security > AAA > RADIUS > Fallback to open the RADIUS > Fallback Parameters to open the fallback parameters page.

b. From the Fallback Mode drop-down list, choose one of the following options:
   - Off—Disables RADIUS server fallback. This is the default value.
   - Passive—Causes the controller to revert to a server with a lower priority from the available backup servers without using extraneous probe messages. The controller ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
   - Active—Causes the controller to revert to a server with a lower priority from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller ignores all inactive servers for all active RADIUS requests. Once the primary server receives a response from the recovered ACS server, the active fallback RADIUS server no longer sends probe messages to the server requesting the active probe authentication.

c. If you enabled Active fallback mode in Step b, enter the name to be sent in the inactive server probes in the Username text box. You can enter up to 16 alphanumeric characters. The default value is “cisco-probe.”

d. If you enabled Active fallback mode in Step b, enter the probe interval value (in seconds) in the Interval in Sec text box. The interval serves as inactive time in passive mode and probe interval in active mode. The valid range is 180 to 3600 seconds, and the default value is 300 seconds.

Step 23  Specify the order of authentication when multiple databases are configured by choosing Security > Priority Order > Management User. The Priority Order > Management User page appears.

Step 24  In the Order Used for Authentication text box, specify which servers have priority when the controller attempts to authenticate management users. Use the > and < buttons to move servers between the Not Used and Order Used for Authentication text boxes. After the desired servers appear in the Order Used for Authentication text box, use the Up and Down buttons to move the priority server to the top of the list.

By default, the local database is always queried first. If the username is not found, the controller switches to the RADIUS server if configured for RADIUS or to the TACACS+ server if configured for TACACS+. The default setting is local and then RADIUS.

Step 25  Click Apply to commit your changes.

Step 26  Click Save Configuration to save your changes.

### Configuring RADIUS (CLI)

Step 1  Specify whether the IP address, system MAC address, or AP MAC address of the originator will be sent to the RADIUS server in the Access-Request message by entering this command:

```
config radius callStationIdType {ip_address | mac_address | ap_mac_address | ap_macaddr_ssid}
```

Note  The default is MAC address.
### Step 2

Specify the delimiter to be used in the MAC addresses that are sent to the RADIUS authentication or accounting server in Access-Request messages by entering this command:

```
config radius { auth | acct } mac-delimiter { colon | hyphen | single-hyphen | none }
```

where
- **colon** sets the delimiter to a colon (the format is xx:xx:xx:xx:xx:xx).
- **hyphen** sets the delimiter to a hyphen (the format is xx-xx-xx-xx-xx-xx). This is the default value.
- **single-hyphen** sets the delimiter to a single hyphen (the format is xxxxxx-xxxxxx).
- **none** disables delimiters (the format is xxxxxxxxxxx).

### Step 3

Configure a RADIUS authentication server by entering these commands:

- **config radius auth add index server_ip_address port# { ascii | hex } shared_secret**—Adds a RADIUS authentication server.
- **config radius auth keywrap { enable | disable }**—Enables AES key wrap, which makes the shared secret between the controller and the RADIUS server more secure. AES key wrap is designed for Federal Information Processing Standards (FIPS) customers and requires a key-wrap compliant RADIUS authentication server.
- **config radius auth keywrap add { ascii | hex } kek mack index**—Configures the AES key wrap attributes
  where
  - **kek** specifies the 16-byte Key Encryption Key (KEK).
  - **mack** specifies the 20-byte Message Authentication Code Key (MACK).
  - **index** specifies the index of the RADIUS authentication server on which to configure the AES key wrap.
- **config radius auth rfc3576 { enable | disable } index**—Enables or disables RFC 3576, which is an extension to the RADIUS protocol that allows dynamic changes to a user session. RFC 3576 includes support for disconnecting users and changing authorizations applicable to a user session and supports disconnect and change-of-authorization (CoA) messages. Disconnect messages cause a user session to be terminated immediately where CoA messages modify session authorization attributes such as data filters.
- **config radius auth retransmit-timeout index timeout**—Configures the network login retransmission timeout value for a RADIUS authentication server.
- **config radius auth mgmt-retransmit-timeout index timeout**—Configures the management login retransmission timeout value for a RADIUS authentication server.
- **config radius auth network index { enable | disable }**—Enables or disables network user authentication. If you enable this feature, this entry is considered the RADIUS authentication server for network users. If you did not configure a RADIUS server entry on the WLAN, you must enable this option for network users.
- **config radius auth management index { enable | disable }**—Enables or disables management authentication. If you enable this feature, this entry is considered the RADIUS authentication server for management users, and authentication requests go to the RADIUS server.
- **config radius auth ipsec { enable | disable } index**—Enables or disables the IP security mechanism.
Chapter 7  Configuring Security Solutions

Step 4  Configure a RADIUS authentication server by entering these commands:

- `config radius auth add index server_ip_address port# {ascii | hex} shared_secret`— Adds a RADIUS authentication server.
- `config radius auth ipsec authentication {hmac-md5 | hmac-sha1} index`— Configures the IP security authentication protocol to be used.
- `config radius auth ipsec encryption {3des | aes | des | none} index`— Configures the IP security encryption mechanism.
- `config radius auth ipsec ike dh-group {group-1 | group-2 | group-5} index`— Configures the IKE Diffie Hellman group.
- `config radius auth ipsec ike lifetime interval index`— Configures the timeout interval for the session.
- `config radius auth ipsec ike phase1 {aggressive | main} index`— Configures the Internet Key Exchange (IKE) protocol.
- `config radius auth {enable | disable} index`— Enables or disables a RADIUS authentication server.
- `config radius auth delete index`— Deletes a previously added RADIUS authentication server.

Step 5  Configure the RADIUS server fallback behavior by entering this command:

```
config radius fallback-test mode {off | passive | active}
```

where

- `off` disables RADIUS server fallback.
- `passive` causes the controller to revert to a server with a lower priority from the available backup servers without using extraneous probe messages. The controller simply ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
• **active** causes the controller to revert to a server with a lower priority from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller simply ignores all inactive servers for all active RADIUS requests. Once the primary server receives a response from the recovered ACS server, the active fallback RADIUS server no longer sends probe messages to the server requesting the active probe authentication.

**Step 6** If you enabled Active mode in Step 5, enter these commands to configure additional fallback parameters:

- `config radius fallback-test username username`—Specifies the name to be sent in the inactive server probes. You can enter up to 16 alphanumeric characters for the *username* parameter.
- `config radius fallback-test interval interval`—Specifies the probe interval value (in seconds).

**Step 7** Save your changes by entering this command:

`save config`

**Step 8** Configure the order of authentication when multiple databases are configured by entering this command:

`config aaa auth mgmt AAA_server_type AAA_server_type`

where *AAA_server_type* is local, radius, or tacacs.

To see the current management authentication server order, enter the `show aaa auth` command.

**Step 9** See RADIUS statistics by entering these commands:

- `show radius summary`—Shows a summary of RADIUS servers and statistics.
- `show radius auth statistics`—Shows the RADIUS authentication server statistics.
- `show radius acct statistics`—Shows the RADIUS accounting server statistics.
- `show radius rfc3576 statistics`—Shows a summary of the RADIUS RFC-3576 server.

**Step 10** See active security associations by entering these commands:

- `show ike {brief | detailed} ip_or_mac_addr`—Shows a brief or detailed summary of active IKE security associations.
- `show ipsec {brief | detailed} ip_or_mac_addr`—Shows a brief or detailed summary of active IPSec security associations.

**Step 11** Clear the statistics for one or more RADIUS servers by entering this command:

`clear stats radius {auth | acct} {index | all}`

**Step 12** Make sure that the controller can reach the RADIUS server by entering this command:

`ping server_ip_address`
RADIUS Authentication Attributes Sent by the Access Point

Table 7-1 through Table 7-5 identify the RADIUS authentication attributes sent by a lightweight access point to a client in access-request and access-accept packets.

**Table 7-1** Authentication Attributes Sent in Access-Request Packets

<table>
<thead>
<tr>
<th>Attribute ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-Name</td>
</tr>
<tr>
<td>2</td>
<td>Password</td>
</tr>
<tr>
<td>3</td>
<td>CHAP-Password</td>
</tr>
<tr>
<td>4</td>
<td>NAS-IP-Address</td>
</tr>
<tr>
<td>5</td>
<td>NAS-Port</td>
</tr>
<tr>
<td>6</td>
<td>Service-Type&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td>12</td>
<td>Framed-MTU</td>
</tr>
<tr>
<td>30</td>
<td>Called-Station-ID (MAC address)</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-ID (MAC address)</td>
</tr>
<tr>
<td>32</td>
<td>NAS-Identifier</td>
</tr>
<tr>
<td>33</td>
<td>Proxy-State</td>
</tr>
<tr>
<td>60</td>
<td>CHAP-Challenge</td>
</tr>
<tr>
<td>61</td>
<td>NAS-Port-Type</td>
</tr>
<tr>
<td>79</td>
<td>EAP-Message</td>
</tr>
<tr>
<td>243</td>
<td>TPLUS-Role</td>
</tr>
</tbody>
</table>

1. To specify read-only or read-write access to controllers through RADIUS authentication, you must set the Service-Type attribute (6) on the RADIUS server to **Callback NAS Prompt** for read-only access or to **Administrative** for read-write privileges. See Step 19 in the “Configuring RADIUS on the ACS” section for more information.

**Table 7-2** Authentication Attributes Honored in Access-Accept Packets (Cisco)

<table>
<thead>
<tr>
<th>Attribute ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cisco-LEAP-Session-Key</td>
</tr>
<tr>
<td>2</td>
<td>Cisco-Keywrap-NonCE</td>
</tr>
<tr>
<td>3</td>
<td>Cisco-Keywrap-NonCE</td>
</tr>
<tr>
<td>4</td>
<td>Cisco-Keywrap-Key</td>
</tr>
<tr>
<td>5</td>
<td>Cisco-URL-Redirect</td>
</tr>
<tr>
<td>6</td>
<td>Cisco-URL-Redirect-ACL</td>
</tr>
</tbody>
</table>

>Note These Cisco-specific attributes are not supported: Auth-Algo-Type and SSID.
### Table 7-3  Authentication Attributes Honored in Access-Accept Packets (Standard)

<table>
<thead>
<tr>
<th>Attribute ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Service-Type. To specify read-only or read-write access to controllers through RADIUS authentication, you must set the Service-Type attribute (6) on the RADIUS server to Callback NAS Prompt for read-only access or to Administrative for read-write privileges.</td>
</tr>
<tr>
<td>8</td>
<td>Framed-IP-Address</td>
</tr>
<tr>
<td>25</td>
<td>Class</td>
</tr>
<tr>
<td>26</td>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>27</td>
<td>Timeout</td>
</tr>
<tr>
<td>29</td>
<td>Termination-Action</td>
</tr>
<tr>
<td>40</td>
<td>Acct-Status-Type</td>
</tr>
<tr>
<td>64</td>
<td>Tunnel-Type</td>
</tr>
<tr>
<td>79</td>
<td>EAP-Message</td>
</tr>
<tr>
<td>81</td>
<td>Tunnel-Group-ID</td>
</tr>
</tbody>
</table>

**Note**  Message authentication is not supported.

### Table 7-4  Authentication Attributes Honored in Access-Accept Packets (Microsoft)

<table>
<thead>
<tr>
<th>Attribute ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>MS-CHAP-Challenge</td>
</tr>
<tr>
<td>16</td>
<td>MS-MPPE-Send-Key</td>
</tr>
<tr>
<td>17</td>
<td>MS-MPPE-Receive-Key</td>
</tr>
<tr>
<td>25</td>
<td>MS-MSCHAP2-Response</td>
</tr>
<tr>
<td>26</td>
<td>MS-MSCHAP2-Success</td>
</tr>
</tbody>
</table>
Table 7-6 Accounting Attributes for Accounting Requests

<table>
<thead>
<tr>
<th>Attribute ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-Name</td>
</tr>
<tr>
<td>4</td>
<td>NAS-IP-Address</td>
</tr>
<tr>
<td>5</td>
<td>NAS-Port</td>
</tr>
<tr>
<td>8</td>
<td>Framed-IP-Address</td>
</tr>
<tr>
<td>25</td>
<td>Class</td>
</tr>
<tr>
<td>30</td>
<td>Called-Station-ID (MAC address)</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-ID (MAC address)</td>
</tr>
<tr>
<td>32</td>
<td>NAS-Identifier</td>
</tr>
<tr>
<td>40</td>
<td>Accounting-Status-Type</td>
</tr>
<tr>
<td>41</td>
<td>Accounting-Delay-Time (Stop and interim messages only)</td>
</tr>
<tr>
<td>42</td>
<td>Accounting-Input-Octets (Stop and interim messages only)</td>
</tr>
<tr>
<td>43</td>
<td>Accounting-Output-Octets (Stop and interim messages only)</td>
</tr>
<tr>
<td>44</td>
<td>Accounting-Session-ID</td>
</tr>
<tr>
<td>45</td>
<td>Accounting-Authentic</td>
</tr>
<tr>
<td>46</td>
<td>Accounting-Session-Time (Stop and interim messages only)</td>
</tr>
<tr>
<td>47</td>
<td>Accounting-Input-Packets (Stop and interim messages only)</td>
</tr>
<tr>
<td>48</td>
<td>Accounting-Output-Packets (Stop and interim messages only)</td>
</tr>
<tr>
<td>49</td>
<td>Accounting-Terminate-Cause (Stop messages only)</td>
</tr>
</tbody>
</table>

RADIUS Accounting Attributes

Table 7-6 identifies the RADIUS accounting attributes for accounting requests sent from a controller to the RADIUS server. Table 7-7 lists the different values for the Accounting-Status-Type attribute (40).
Chapter 7  Configuring Security Solutions

Table 7-6  Accounting Attributes for Accounting Requests (continued)

<table>
<thead>
<tr>
<th>Attribute ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>Tunnel-Type</td>
</tr>
<tr>
<td>65</td>
<td>Tunnel-Medium-Type</td>
</tr>
<tr>
<td>81</td>
<td>Tunnel-Group-ID</td>
</tr>
</tbody>
</table>

Table 7-7  Accounting-Status-Type Attribute Values

<table>
<thead>
<tr>
<th>Attribute ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Start</td>
</tr>
<tr>
<td>2</td>
<td>Stop</td>
</tr>
<tr>
<td>3</td>
<td>Interim-Update</td>
</tr>
<tr>
<td>7</td>
<td>Accounting-On</td>
</tr>
<tr>
<td>8</td>
<td>Accounting-Off</td>
</tr>
<tr>
<td>9-14</td>
<td>Reserved for Tunneling Accounting</td>
</tr>
<tr>
<td>15</td>
<td>Reserved for Failed</td>
</tr>
</tbody>
</table>

Configuring TACACS+

This section contains the following topics:

- Information About TACACS+, page 7-17
- Guidelines and Limitations, page 7-19
- Configuring TACACS+ on the ACS, page 7-19
- Configuring TACACS+, page 7-21
- Viewing the TACACS+ Administration Server Logs, page 7-24

Information About TACACS+

Terminal Access Controller Access Control System Plus (TACACS+) is a client/server protocol that provides centralized security for users attempting to gain management access to a controller. It serves as a backend database similar to local and RADIUS. However, local and RADIUS provide only authentication support and limited authorization support while TACACS+ provides three services:

- Authentication—The process of verifying users when they attempt to log into the controller.

Users must enter a valid username and password in order for the controller to authenticate users to the TACACS+ server. The authentication and authorization services are tied to one another. For example, if authentication is performed using the local or RADIUS database, then authorization would use the permissions associated with the user in the local or RADIUS database (which are read-only, read-write, and lobby-admin) and not use TACACS+. Similarly, when authentication is performed using TACACS+, authorization is tied to TACACS+. 
When multiple databases are configured, you can use the controller GUI or CLI to specify the sequence in which the backend databases should be tried.

- **Authorization**—The process of determining the actions that users are allowed to take on the controller based on their level of access.

  For TACACS+, authorization is based on privilege (or role) rather than specific actions. The available roles correspond to the seven menu options on the controller GUI: MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, and COMMANDS. An additional role, LOBBY, is available for users who require only lobby ambassador privileges. The roles to which users are assigned are configured on the TACACS+ server. Users can be authorized for one or more roles. The minimum authorization is MONITOR only, and the maximum is ALL, which authorizes the user to execute the functionality associated with all seven menu options. For example, a user who is assigned the role of SECURITY can make changes to any items appearing on the Security menu (or designated as security commands in the case of the CLI). If users are not authorized for a particular role (such as WLAN), they can still access that menu option in read-only mode (or the associated CLI `show` commands). If the TACACS+ authorization server becomes unreachable or unable to authorize, users are unable to log into the controller.

- **Accounting**—The process of recording user actions and changes.

  Whenever a user successfully executes an action, the TACACS+ accounting server logs the changed attributes, the user ID of the person who made the change, the remote host where the user is logged in, the date and time when the command was executed, the authorization level of the user, and a description of the action performed and the values provided. If the TACACS+ accounting server becomes unreachable, users are able to continue their sessions uninterrupted.

  TACACS+ uses Transmission Control Protocol (TCP) for its transport, unlike RADIUS which uses User Datagram Protocol (UDP). It maintains a database and listens on TCP port 49 for incoming requests. The controller, which requires access control, acts as the client and requests AAA services from the server. The traffic between the controller and the server is encrypted by an algorithm defined in the protocol and a shared secret key configured on both devices.

  You can configure up to three TACACS+ authentication, authorization, and accounting servers each. For example, you may want to have one central TACACS+ authentication server but several TACACS+ authorization servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the controller automatically tries the second one and then the third one if necessary.

  If multiple TACACS+ servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.
**TACACS+ VSA**

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific attributes (VSAs) between the network access server and the TACACS+ server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use.

The Cisco TACACS+ implementation supports one vendor-specific option using the format recommended in the IETF specification. The Cisco vendor ID is 9, and the supported option is vendor type 1, which is named cisco-av-pair. The value is a string with the following format:

```
protocol : attribute separator value *
```

The protocol is a Cisco attribute for a particular type of authorization, the separator is = (equal sign) for mandatory attributes, and * (asterisk) indicates optional attributes.

**Guidelines and Limitations**

- You must configure TACACS+ on both your Cisco Secure Access Control Server (ACS) and your controller. You can configure the controller through either the GUI or the CLI.
- TACACS+ is supported on Cisco Secure ACS version 3.2 and later releases. See the CiscoSecure ACS documentation for the version that you are running.

**Configuring TACACS+ on the ACS**

1. Choose **Network Configuration** on the ACS main page.
2. Choose **Add Entry** under AAA Clients to add your controller to the server. The Add AAA Client page appears.
Configuring TACACS+

Step 3  In the AAA Client Hostname text box, enter the name of your controller.
Step 4  In the AAA Client IP Address text box, enter the IP address of your controller.
Step 5  In the Shared Secret text box, enter the shared secret key to be used for authentication between the server and the controller.

**Note** The shared secret key must be the same on both the server and the controller.

Step 6  From the Authenticate Using drop-down list, choose **TACACS+ (Cisco IOS)**.
Step 7  Click **Submit + Apply** to save your changes.
Step 8  On the ACS main page, in the left navigation pane, choose **Interface Configuration**.
Step 9  Choose **TACACS+ (Cisco IOS)**. The TACACS+ (Cisco) page appears.
Step 10 Under TACACS+ Services, select the **Shell (exec)** check box.
Step 11 Under New Services, select the first check box and enter `ciscowlc` in the Service text box and `common` in the Protocol text box.
Step 12 Under Advanced Configuration Options, select the **Advanced TACACS+ Features** check box.
Step 13 Click **Submit** to save your changes.
Step 14 On the ACS main page, in the left navigation pane, choose **System Configuration**.
Step 15 Choose **Logging**.
Step 16 When the Logging Configuration page appears, enable all of the events that you want to be logged and save your changes.
Step 17 On the ACS main page, in the left navigation pane, choose **Group Setup**.
Chapter 7  Configuring Security Solutions

Step 18  From the Group drop-down list, choose a previously created group.

Note  This step assumes that you have already assigned users to groups on the ACS according to the roles to which they will be assigned.

Step 19  Click Edit Settings. The Group Setup page appears.

Step 20  Under TACACS+ Settings, select the ciscowlc common check box.

Step 21  Select the Custom Attributes check box.

Step 22  In the text box below Custom Attributes, specify the roles that you want to assign to this group. The available roles are MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, ALL, and LOBBY. The first seven correspond to the menu options on the controller GUI and allow access to those particular controller features. You can enter one or multiple roles, depending on the group’s needs. Use ALL to specify all seven roles or LOBBY to specify the lobby ambassador role. Enter the roles using this format:

role\x3dROLE

For example, to specify the WLAN, CONTROLLER, and SECURITY roles for a particular user group, you would enter the following text:

role1\x3dWLAN
role2\x3dCONTROLLER
role3\x3dSECURITY

To give a user group access to all seven roles, you would enter the following text:

role1\x3dALL

Note  Make sure to enter the roles using the format shown above. The roles must be in all uppercase letters, and there can be no spaces within the text.

Note  You should not combine the MONITOR role or the LOBBY role with any other roles. If you specify one of these two roles in the Custom Attributes text box, users will have MONITOR or LOBBY privileges only, even if additional roles are specified.

Step 23  Click Submit to save your changes.

Configuring TACACS+

This section contains the following topics:

- Configuring TACACS+ (GUI), page 7-21
- Configuring TACACS+ (CLI), page 7-23

Configuring TACACS+ (GUI)

Step 1  Choose Security > AAA > TACACS+.
Step 2
Perform one of the following:

- If you want to configure a TACACS+ server for authentication, choose **Authentication**.
- If you want to configure a TACACS+ server for authorization, choose **Authorization**.
- If you want to configure a TACACS+ server for accounting, choose **Accounting**.

**Note**

The pages used to configure authentication, authorization, and accounting all contain the same text boxes. Therefore, these instructions walk through the configuration only once, using the Authentication pages as examples. You would follow the same steps to configure multiple services and/or multiple servers.

**Note**

For basic management authentication via TACACS+ to succeed, it is required to configure authentication and authorization servers on the WLC. Accounting configuration is optional.

The TACACS+ (Authentication, Authorization, or Accounting) Servers page appears. This page lists any TACACS+ servers that have already been configured.

- If you want to delete an existing server, hover your cursor over the blue drop-down arrow for that server and choose **Remove**.
- If you want to make sure that the controller can reach a particular server, hover your cursor over the blue drop-down arrow for that server and choose **Ping**.

Step 3
Perform one of the following:

- To edit an existing TACACS+ server, click the server index number for that server. The TACACS+ (Authentication, Authorization, or Accounting) Servers > Edit page appears.
- To add a TACACS+ server, click **New**. The TACACS+ (Authentication, Authorization, or Accounting) Servers > New page appears.

Step 4
If you are adding a new server, choose a number from the Server Index (Priority) drop-down list to specify the priority order of this server in relation to any other configured TACACS+ servers providing the same service. You can configure up to three servers. If the controller cannot reach the first server, it tries the second one in the list and then the third if necessary.

Step 5
If you are adding a new server, enter the IP address of the TACACS+ server in the Server IP Address text box.

Step 6
From the Shared Secret Format drop-down list, choose **ASCII** or **Hex** to specify the format of the shared secret key to be used between the controller and the TACACS+ server. The default value is ASCII.

Step 7
In the Shared Secret and Confirm Shared Secret text boxes, enter the shared secret key to be used for authentication between the controller and the server.

**Note**

The shared secret key must be the same on both the server and the controller.

Step 8
If you are adding a new server, enter the TACACS+ server’s TCP port number for the interface protocols in the Port Number text box. The valid range is 1 to 65535, and the default value is 49.

Step 9
In the Server Status text box, choose **Enabled** to enable this TACACS+ server or choose **Disabled** to disable it. The default value is Enabled.

Step 10
In the Server Timeout text box, enter the number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.
Step 11  Click **Apply** to commit your changes.

Step 12  Click **Save Configuration** to save your changes.

Step 13  Repeat the previous steps if you want to configure any additional services on the same server or any additional TACACS+ servers.

Step 14  Specify the order of authentication when multiple databases are configured by choosing **Security > Priority Order > Management User**. The Priority Order > Management User page appears.

Step 15  In the Order Used for Authentication text box, specify which servers have priority when the controller attempts to authenticate management users. Use the > and < buttons to move servers between the Not Used and Order Used for Authentication text boxes. After the desired servers appear in the Order Used for Authentication text box, use the **Up** and **Down** buttons to move the priority server to the top of the list.

By default, the local database is always queried first. If the username is not found, the controller switches to the RADIUS server if configured for RADIUS or to the TACACS+ server if configured for TACACS+. The default setting is local and then RADIUS.

Step 16  Click **Apply** to commit your changes.

Step 17  Click **Save Configuration** to save your changes.

### Configuring TACACS+ (CLI)

- Configure a TACACS+ authentication server by entering these commands:
  
  ```
  config tacacs auth add index server_ip_address port# [ascii | hex] shared_secret—Adds a TACACS+ authentication server.
  config tacacs auth delete index—Deletes a previously added TACACS+ authentication server.
  config tacacs auth (enable | disable) index—Enables or disables a TACACS+ authentication server.
  config tacacs auth server-timeout index timeout—Configures the network login retransmission timeout value for a TACACS+ authentication server.
  config tacacs auth mgmt-server-timeout index timeout—Configures the management login retransmission timeout value for a TACACS+ authentication server.
  ```

- Configure a TACACS+ authorization server by entering these commands:
  
  ```
  config tacacs athr add index server_ip_address port# [ascii | hex] shared_secret—Adds a TACACS+ authorization server.
  config tacacs athr delete index—Deletes a previously added TACACS+ authorization server.
  config tacacs athr (enable | disable) index—Enables or disables a TACACS+ authorization server.
  config tacacs athr server-timeout index timeout—Configures the network login retransmission timeout value for a TACACS+ authorization server.
  ```
- **config tacacs mgmt-athr server-timeout index timeout**—Configures the management login retransmission timeout value for a TACACS+ authorization server.

- Configure a TACACS+ accounting server by entering these commands:
  - **config tacacs acct add index server_ip_address port# {ascii | hex} shared_secret**—Adds a TACACS+ accounting server.
  - **config tacacs acct delete index**—Deletes a previously added TACACS+ accounting server.
  - **config tacacs acct (enable | disable) index**—Enables or disables a TACACS+ accounting server.
  - **config tacacs acct server-timeout index timeout**—Configures the retransmission timeout value for a TACACS+ accounting server.

- See TACACS+ statistics by entering these commands:
  - **show tacacs summary**—Shows a summary of TACACS+ servers and statistics.
  - **show tacacs auth stats**—Shows the TACACS+ authentication server statistics.
  - **show tacacs athr stats**—Shows the TACACS+ authorization server statistics.
  - **show tacacs acct stats**—Shows the TACACS+ accounting server statistics.

- Clear the statistics for one or more TACACS+ servers by entering this command:
  - **clear stats tacacs [auth | athr | acct] {index | all}**

- Configure the order of authentication when multiple databases are configured by entering this command. The default setting is **local** and then **radius**.
  - **config aaa auth mgmt [radius | tacacs]**

- See the current management authentication server order by entering the **show aaa auth** command.

- Make sure the controller can reach the TACACS+ server by entering this command:
  - **ping server_ip_address**

- Enable or disable TACACS+ debugging by entering this command:
  - **debug aaa tacacs {enable | disable}**

- Save your changes by entering this command:
  - **save config**

---

**Viewing the TACACS+ Administration Server Logs**

**Prerequisites**

You must have configured TACACS+ accounting server on the controller.

---

**Step 1**  
On the ACS main page, in the left navigation pane, choose **Reports and Activity**.

**Step 2**  
Under Reports, choose **TACACS+ Administration**.

**Step 3**  
Click the .csv file corresponding to the date of the logs you want to view. The TACACS+ Administration .csv page appears.
This page displays the following information:

- Date and time the action was taken
- Name and assigned role of the user who took the action
- Group to which the user belongs
- Specific action that the user took
- Privilege level of the user who executed the action
- IP address of the controller
- IP address of the laptop or workstation from which the action was executed

Sometimes a single action (or command) is logged multiple times, once for each parameter in the command. For example, if you enter the `snmp community ipaddr ip_address subnet_mask community_name` command, the IP address may be logged on one line while the subnet mask and community name are logged as “E.” On another line, the subnet mask may be logged while the IP address and community name are logged as “E.” See the first and third lines in the example in Figure 7-5.
Configuring Maximum Local Database Entries

This section contains the following topics:

- Information About Configuring Maximum Local Database Entries, page 7-26
- Configuring Maximum Local Database Entries (GUI), page 7-26
- Configuring Maximum Local Database Entries (CLI), page 7-27

Information About Configuring Maximum Local Database Entries

You can configure the controller to specify the maximum number of local database entries used for storing user authentication information. The database entries include local management users (including lobby ambassadors), local network users (including guest users), MAC filter entries, exclusion list entries, and access point authorization list entries. Together, they cannot exceed the configured maximum value.

Configuring Maximum Local Database Entries (GUI)

Step 1  Choose Security > AAA > General to open the General page.
Step 2 In the Maximum Local Database Entries text box, enter a value for the maximum number of entries that can be added to the local database the next time the controller reboots. The currently configured value appears in parentheses to the right of the text box. The valid range is 512 to 2048, and the default setting is 2048.

The Number of Entries, Already Used text box shows the number of entries currently in the database.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your settings.

---

**Configuring Maximum Local Database Entries (CLI)**

Step 1 Specify the maximum number of entries that can be added to the local database the next time the controller reboots by entering this command:

```
config database size max_entries
```

Step 2 Save your changes by entering this command:

```
save config
```

Step 3 View the maximum number of database entries and the current database contents by entering this command:

```
show database summary
```

---

**Configuring Local Network Users on the Controller**

This section contains the following topics:

- Information About Local Network Users on Controller, page 7-28
- Configuring Local Network Users for the Controller, page 7-28
- Additional References, page 7-30
Information About Local Network Users on Controller

You can add local network users to the local user database on the controller. The local user database stores the credentials (username and password) of all the local network users. These credentials are then used to authenticate the users. For example, local EAP may use the local user database as its backend database to retrieve user credentials.

Note

The controller passes client information to the RADIUS authentication server first. If the client information does not match a RADIUS database entry, the local user database is polled. Clients located in this database are granted access to network services if the RADIUS authentication fails or does not exist.

Configuring Local Network Users for the Controller

This section contains the following topics:

- Configuring Local Network Users for the Controller (GUI), page 7-28
- Configuring Local Network Users for the Controller (CLI), page 7-29

Configuring Local Network Users for the Controller (GUI)

Step 1  Choose Security > AAA > Local Net Users to open the Local Net Users page.

Figure 7-7  Local Net Users Page

This page lists any local network users that have already been configured. It also specifies any guest users and the QoS role to which they are assigned (if applicable).

Note

If you want to delete an existing user, hover your cursor over the blue drop-down arrow for that user and choose Remove.

Step 2  Perform one of the following:

- To edit an existing local network user, click the username for that user. The Local Net Users > Edit page appears.
- To add a local network user, click New. The Local Net Users > New page appears.
Step 3  If you are adding a new user, enter a username for the local user in the User Name text box. You can enter up to 24 alphanumeric characters.

*Note*  Local network usernames must be unique because they are all stored in the same database.

Step 4  In the Password and Confirm Password text boxes, enter a password for the local user. You can enter up to 24 alphanumeric characters.

Step 5  If you are adding a new user, select the **Guest User** check box if you want to limit the amount of time that the user has access to the local network. The default setting is unselected.

Step 6  If you are adding a new user and you selected the Guest User check box, enter the amount of time (in seconds) that the guest user account is to remain active in the Lifetime text box. The valid range is 60 to 2,592,000 seconds (30 days) inclusive, and the default setting is 86,400 seconds.

Step 7  If you are adding a new user, you selected the Guest User check box, and you want to assign a QoS role to this guest user, select the **Guest User Role** check box. The default setting is unselected.

*Note*  If you do not assign a QoS role to a guest user, the bandwidth contracts for this user are defined in the QoS profile for the WLAN.

Step 8  If you are adding a new user and you selected the Guest User Role check box, choose the QoS role that you want to assign to this guest user from the Role drop-down list.

Step 9  From the WLAN Profile drop-down list, choose the name of the WLAN that is to be accessed by the local user. If you choose Any WLAN, which is the default setting, the user can access any of the configured WLANs.

Step 10  In the Description text box, enter a descriptive title for the local user (such as “User 1”).

Step 11  Click **Apply** to commit your changes.

Step 12  Click **Save Configuration** to save your changes.

---

**Configuring Local Network Users for the Controller (CLI)**

- Configure a local network user by entering these commands:
  
  ```
  - config netuser add username password wlan wlan_id userType permanent description description—Adds a permanent user to the local user database on the controller.
  ```

  ```
  - config netuser add username password {wlan | guestlan} {wlan_id | guest_lan_id} userType guestlifetime seconds description description—Adds a guest user on a WLAN or wired guest LAN to the local user database on the controller.
  ```

  *Note*  Instead of adding a permanent user or a guest user to the local user database from the controller, you can choose to create an entry on the RADIUS server for the user and enable RADIUS authentication for the WLAN on which web authentication is performed.

- `config netuser delete username`—Deletes a user from the local user database on the controller.

*Note*  Local network usernames must be unique because they are all stored in the same database.
• See information related to the local network users configured on the controller by entering these commands:
  - `show netuser detail username`—Shows the configuration of a particular user in the local user database.
  - `show netuser summary`—Lists all the users in the local user database.
• Save your changes by entering this command:
  `save config`

Additional References

To know more about configuring local network users, see “Configuring Local EAP” section on page 7-36 for more information.

If you want to create a new QoS role, see the “Configuring Quality of Service” section on page 4-66 for instructions.

Configuring Password Policies

This section contains the following topics:
• Information About Password Policies, page 7-30
• Configuring Password Policies (GUI), page 7-30
• Configuring Password Policies (CLI), page 7-31

Information About Password Policies

The password policies allows you 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 and access point user configuration is affected.

Configuring Password Policies (GUI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Security &gt; AAA &gt; Password Policies</strong> to open the Password Policies page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the <strong>Password must contain characters from at least 3 different classes</strong> check box if you want your password to contain characters from at least three of the following classes: lower case letters, upper case letters, digits, and special characters.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>No character can be repeated more than 3 times consecutively</strong> check box if you do not want character in the new password to repeat more than three times consecutively.</td>
</tr>
</tbody>
</table>
Step 4  Select the **Password cannot be the default words like cisco, admin** check box if you do not want the password to contain words such as Cisco, ocsic, admin, nimda, or any variant obtained by changing the capitalization of letters or by substituting 1, [, or! or substituting 0 for o or substituting $ for $.

Step 5  Select the **Password cannot contain username or reverse of username** check box if you do not want the password to contain a username or the reverse letters of a username.

Step 6  Click **Apply** to commit your changes.

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

---

**Configuring Password Policies (CLI)**

**Step 1**  Enable or disable strong password check for AP and WLC by entering this command:

```
config switchconfig strong-pwd { case-check | consecutive-check | default-check | username-check | all-check } { enable | disable }
```

where

- **case-check**—Checks the occurrence of same character thrice consecutively
- **consecutive-check**—Checks the default values or its variants are being used.
- **default-check**—Checks either username or its reverse is being used.
- **all-checks**—Enables/disables all the strong password checks.

**Step 2**  See the configured options for strong password check by entering this command:

```
show switchconfig
```

**Example: Show Command for Password Policies**

Information similar to the following appears:

```
802.3x Flow Control Mode............................... Disabled
FIPS prerequisite features......................... Disabled
secret obfuscation................................. Enabled
Strong Password Check Features:
    case-check ............Enabled
    consecutive-check ....Enabled
    default-check ........Enabled
    username-check ......Enabled
```

---

**Configuring LDAP**

This section explains how to configure a Lightweight Directory Access Protocol (LDAP) server as a backend database, similar to a RADIUS or local user database.

This section contains the following topics:

- **Information About LDAP**, page 7-32
- **Configuring LDAP (GUI)**, page 7-32
Information About LDAP

An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user. For example, local EAP may use an LDAP server as its backend database to retrieve user credentials.

Note

The LDAP backend database supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC. LEAP, EAP-FAST/MSCHAPv2, and PEAPv0/MSCHAPv2 are also supported but only if the LDAP server is set up to return a clear-text password.

Note


Configuring LDAP (GUI)

Step 1

Choose Security > AAA > LDAP to open the LDAP Servers page.

This page lists any LDAP servers that have already been configured.

- If you want to delete an existing LDAP server, hover your cursor over the blue drop-down arrow for that server and choose Remove.
- If you want to make sure that the controller can reach a particular server, hover your cursor over the blue drop-down arrow for that server and choose Ping.

Step 2

Perform one of the following:

- To edit an existing LDAP server, click the index number for that server. The LDAP Servers > Edit page appears.
To add an LDAP server, click **New**. The LDAP Servers > New page appears. If you are adding a new server, choose a number from the Server Index (Priority) drop-down list to specify the priority order of this server in relation to any other configured LDAP servers. You can configure up to 17 servers. If the controller cannot reach the first server, it tries the second one in the list and so on.

**Step 3**
If you are adding a new server, enter the IP address of the LDAP server in the Server IP Address text box.

**Step 4**
If you are adding a new server, enter the LDAP server’s TCP port number in the Port Number text box. The valid range is 1 to 65535, and the default value is 389.

**Step 5**
Select the **Enable Server Status** check box to enable this LDAP server or unselect it to disable it. The default value is disabled.

**Step 6**
From the Simple Bind drop-down list, choose **Anonymous** or **Authenticated** to specify the local authentication bind method for the LDAP server. The Anonymous method allows anonymous access to the LDAP server. The Authenticated method requires that a username and password be entered to secure access. The default value is **Anonymous**.

**Step 7**
If you chose Authenticated in **Step 6**, follow these steps:

a. In the Bind Username text box, enter a username to be used for local authentication to the LDAP server. The username can contain up to 80 characters.

   **Note**
   If the username starts with “cn=” (in lowercase letters), the controller assumes that the username includes the entire LDAP database path and does not append the user base DN. This designation allows the authenticated bind user to be outside the user base DN.

b. In the Bind Password and Confirm Bind Password text boxes, enter a password to be used for local authentication to the LDAP server. The password can contain up to 32 characters.

**Step 8**
In the User Base DN text box, enter the distinguished name (DN) of the subtree in the LDAP server that contains a list of all the users. For example, ou=organizational unit,.ou=next organizational unit, and o=corporation.com. If the tree containing users is the base DN, type **o=corporation.com** or **dc=corporation,dc=com**.

**Step 9**
In the User Attribute text box, enter the name of the attribute in the user record that contains the username. You can obtain this attribute from your directory server.

**Step 10**
In the User Object Type text box, enter the value of the LDAP objectType attribute that identifies the record as a user. Often, user records have several values for the objectType attribute, some of which are unique to the user and some of which are shared with other object types.

**Step 11**
In the Server Timeout text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

**Step 12**
Click **Apply** to commit your changes.

**Step 13**
Click **Save Configuration** to save your changes.

**Step 14**
Specify LDAP as the priority backend database server for local EAP authentication as follows:

a. Choose **Security > Local EAP > Authentication Priority** to open the Priority Order > Local-Auth page.

b. Highlight **LOCAL** and click < to move it to the left User Credentials box.

c. Highlight **LDAP** and click > to move it to the right User Credentials box. The database that appears at the top of the right User Credentials box is used when retrieving user credentials.
If both LDAP and LOCAL appear in the right User Credentials box with LDAP on the top and LOCAL on the bottom, local EAP attempts to authenticate clients using the LDAP backend database and fails over to the local user database if the LDAP servers are not reachable. If the user is not found, the authentication attempt is rejected. If LOCAL is on the top, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.

d. Click **Apply** to commit your changes.

e. Click **Save Configuration** to save your changes.

**Step 15**

(Optional) Assign specific LDAP servers to a WLAN as follows:

a. Choose **WLANs** to open the WLANs page.

b. Click the ID number of the desired WLAN.

c. When the WLANs > Edit page appears, choose the **Security > AAA Servers** tabs to open the WLANs > Edit (Security > AAA Servers) page.

d. From the LDAP Servers drop-down lists, choose the LDAP server(s) that you want to use with this WLAN. You can choose up to three LDAP servers, which are tried in priority order.

**Note** These LDAP servers apply only to WLANs with web authentication enabled. They are not used by local EAP.

e. Click **Apply** to commit your changes.

f. Click **Save Configuration** to save your changes.

---

**Configuring LDAP (CLI)**

- Configure an LDAP server by entering these commands:
  - `config ldap add index server_ip_address port# user_base user_attr user_type`— Adds an LDAP server.
  - `config ldap delete index`—Deletes a previously added LDAP server.
  - `config ldap {enable | disable} index`—Enables or disables an LDAP server.
  - `config ldap simple-bind [anonymous index | authenticated index username username password password]`—Specifies the local authentication bind method for the LDAP server. The anonymous method allows anonymous access to the LDAP server whereas the authenticated method requires that a username and password be entered to secure access. The default value is anonymous.

**Note** The username can contain up to 80 characters.
Note
If the username starts with "cn=" (in lowercase letters), the controller assumes that the username includes the entire LDAP database path and does not append the user base DN. This designation allows the authenticated bind user to be outside the user base DN.

- **`config ldap retransmit-timeout index timeout`**—Configures the number of seconds between retransmissions for an LDAP server.

- **Specify LDAP as the priority backend database server by entering this command:**

  ```
  config local-auth user-credentials ldap
  ```

  **Note**
  If you enter the `config local-auth user-credentials ldap local` command, local EAP attempts to authenticate clients using the LDAP backend database and fails over to the local user database if the LDAP servers are not reachable. If the user is not found, the authentication attempt is rejected. If you enter the `config local-auth user-credentials local ldap` command, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.

- **(Optional) Assign specific LDAP servers to a WLAN by entering these commands:**

  - `config wlan ldap add wlan_id server_index`—Links a configured LDAP server to a WLAN.

    **Note**
    The LDAP servers specified in this command apply only to WLANs with web authentication enabled. They are not used by local EAP.

  - `config wlan ldap delete wlan_id {all | index}`—Deletes a specific or all configured LDAP server(s) from a WLAN.

- **View information pertaining to configured LDAP servers by entering these commands:**

  - `show ldap summary`—Shows a summary of the configured LDAP servers.

    | Idx | Server Address | Port | Enabled |
    |-----|----------------|------|---------|
    | 1   | 2.3.1.4        | 389  | No      |
    | 2   | 10.10.20.22    | 389  | Yes     |

  - `show ldap index`—Shows detailed LDAP server information. Information similar to following appears:

    ```
    Server Index......................... 2
    Address.................................... 10.10.20.22
    Port...................................... 389
    Enabled................................... Yes
    User DN....................................
    ou=active,ou=employees,ou=people, o=cisco.com
    User Attribute.......................... uid
    User Type............................... Person
    Retransmit Timeout..................... 2 seconds
    Bind Method............................. Authenticated
    Bind Username.......................... user1
    ```

  - `show ldap statistics`—Shows LDAP server statistics.

    | Idx | Server Index |
    |-----|--------------|
    | 1   | 1            |
Server statistics:
  Initialized OK................................. 0
  Initialization failed...................... 0
  Initialization retries..................... 0
  Closed OK..................................... 0
Request statistics:
  Received....................................... 0
  Sent........................................... 0
  OK............................................. 0
  Success........................................ 0
  Authentication failed...................... 0
  Server not found............................ 0
  No received attributes..................... 0
  No passed username.......................... 0
  Not connected to server.................... 0
  Internal error................................ 0
  Retries........................................ 0

Server Index..................................... 2

- `show wlan wlan_id`—Shows the LDAP servers that are applied to a WLAN.

- Make sure the controller can reach the LDAP server by entering this command:
  `ping server_ip_address`

  - Save your changes by entering this command:
    `save config`

  - Enable or disable debugging for LDAP by entering this command:
    `debug aaa ldap {enable | disable}

Additional References

For more information about configuring LEAP, see the “Configuring Local EAP” section on page 7-36.

Configuring Local EAP

This section contains the following topics:

- Information About Local EAP, page 7-36
- Configuring Local EAP (GUI), page 7-38
- Configuring Local EAP (CLI), page 7-42
- Additional References, page 7-47

Information About Local EAP

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, which removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user
database or the LDAP backend database to authenticate users. Local EAP supports LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC authentication between the controller and wireless clients.

**Note**
The LDAP backend database supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC. LEAP, EAP-FAST/MSCHAPv2, and PEAPv0/MSCHAPv2 are also supported but only if the LDAP server is set up to return a clear-text password.

Cisco wireless LAN controllers support Local EAP authentication against external LDAP databases such as Microsoft Active Directory and Novell’s eDirectory. For more information about configuring the controller for Local EAP authentication against Novell’s eDirectory, see the *Configure Unified Wireless Network for Authentication Against Novell’s eDirectory Database* whitepaper at http://www.cisco.com/en/US/products/ps6366/products_white_paper09186a0080b4cd24.shtml.

If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP. If you never want the controller to try to authenticate clients using an external RADIUS server, enter these CLI commands in this order:

- `config wlan disable wlan_id`
- `config wlan radius_server auth disable wlan_id`
- `config wlan enable wlan_id`
Guidelines and Limitations

Local EAP Profiles are not supported on AP602 OEAP.

Configuring Local EAP (GUI)

**Note**

EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC use certificates for authentication, and EAP-FAST uses either certificates or PACs. The controller is shipped with Cisco-installed device and Certificate Authority (CA) certificates. However, if you want to use your own vendor-specific certificates, they must be imported on the controller.

**Step 1**
If you are configuring local EAP to use one of the EAP types listed in the note above, make sure that the appropriate certificates and PACs (if you will use manual PAC provisioning) have been imported on the controller.

**Step 2**
If you want the controller to retrieve user credentials from the local user database, make sure that you have properly configured the local network users on the controller.

**Step 3**
If you want the controller to retrieve user credentials from an LDAP backend database, make sure that you have properly configured an LDAP server on the controller.
Step 4 Specify the order in which user credentials are retrieved from the backend database servers as follows:

a. Choose Security > Local EAP > Authentication Priority to open the Priority Order > Local-Auth page.

b. Determine the priority order in which user credentials are to be retrieved from the local and/or LDAP databases. For example, you may want the LDAP database to be given priority over the local user database, or you may not want the LDAP database to be considered at all.

c. When you have decided on a priority order, highlight the desired database. Then use the left and right arrows and the Up and Down buttons to move the desired database to the top of the right User Credentials box.

Note If both LDAP and LOCAL appear in the right User Credentials box with LDAP on the top and LOCAL on the bottom, local EAP attempts to authenticate clients using the LDAP backend database and fails over to the local user database if the LDAP servers are not reachable. If the user is not found, the authentication attempt is rejected. If LOCAL is on the top, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.

d. Click Apply to commit your changes.

Step 5 Specify values for the local EAP timers as follows:

a. Choose Security > Local EAP > General to open the General page.

b. In the Local Auth Active Timeout text box, enter the amount of time (in seconds) in which the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fails. The valid range is 1 to 3600 seconds, and the default setting is 100 seconds.

c. In the Identity Request Timeout text box, enter the amount of time (in seconds) in which the controller attempts to send an EAP identity request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.

d. In the Identity Request Max Retries text box, enter the maximum number of times that the controller attempts to retransmit the EAP identity request to wireless clients using local EAP. The valid range is 1 to 20 retries, and the default setting is 20 retries.

e. In the Dynamic WEP Key Index text box, enter the key index used for dynamic wired equivalent privacy (WEP). The default value is 0, which corresponds to a key index of 1; the valid values are 0 to 3 (key index of 1 to 4).

f. In the Request Timeout text box, enter the amount of time (in seconds) in which the controller attempts to send an EAP request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.

g. In the Request Max Retries text box, enter the maximum number of times that the controller attempts to retransmit the EAP request to wireless clients using local EAP. The valid range is 1 to 120 retries, and the default setting is 20 retries.

h. From the Max-Login Ignore Identity Response drop-down list, choose Enable to limit the number of devices that can be connected to the controller with the same username. You can log in up to eight times from different devices (PDA, laptop, IP phone, and so on) on the same controller. The default value is enabled.

i. In the EAPOL-Key Timeout text box, enter the amount of time (in seconds) in which the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 1 to 5 seconds, and the default setting is 1 second.
Note If the controller and access point are separated by a WAN link, the default timeout of 1 second may not be sufficient.

j. In the EAPOL-Key Max Retries text box, enter the maximum number of times that the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 0 to 4 retries, and the default setting is 2 retries.

k. Click Apply to commit your changes.

Step 6 Create a local EAP profile, which specifies the EAP authentication types that are supported on the wireless clients as follows:

a. Choose Security > Local EAP > Profiles to open the Local EAP Profiles page.

This page lists any local EAP profiles that have already been configured and specifies their EAP types. You can create up to 16 local EAP profiles.

Note If you want to delete an existing profile, hover your cursor over the blue drop-down arrow for that profile and choose Remove.

b. Click New to open the Local EAP Profiles > New page.

c. In the Profile Name text box, enter a name for your new profile and then click Apply.

Note You can enter up to 63 alphanumeric characters for the profile name. Make sure not to include spaces.

d. When the Local EAP Profiles page reappears, click the name of your new profile. The Local EAP Profiles > Edit page appears.

e. Select the LEAP, EAP-FAST, EAP-TLS, and/or PEAP check boxes to specify the EAP type that can be used for local authentication.

Note You can specify more than one EAP type per profile. However, if you choose multiple EAP types that use certificates (such as EAP-FAST with certificates, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC), all of the EAP types must use the same certificate (from either Cisco or another vendor).

Note If you select the PEAP check box, both PEAPv0/MSCHAPv2 or PEAPv1/GTC are enabled on the controller.

f. If you chose EAP-FAST and want the device certificate on the controller to be used for authentication, select the Local Certificate Required check box. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unselected, which is the default setting.

Note This option applies only to EAP-FAST because device certificates are not used with LEAP and are mandatory for EAP-TLS and PEAP.
Chapter 7  Configuring Security Solutions

Configuring Local EAP

Step 7

If you created an EAP-FAST profile, follow these steps to configure the EAP-FAST parameters:

a. Choose Security > Local EAP > EAP-FAST Parameters to open the EAP-FAST Method Parameters page.

b. In the Server Key and Confirm Server Key text boxes, enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.

c. In the Time to Live for the PAC text box, enter the number of days for the PAC to remain viable. The valid range is 1 to 1000 days, and the default setting is 10 days.

d. In the Authority ID text box, enter the authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters, but you must enter an even number of characters.

e. In the Authority ID Information text box, enter the authority identifier of the local EAP-FAST server in text format.

f. If you want to enable anonymous provisioning, select the Anonymous Provision check box. This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If you disable this feature, PACs must be manually provisioned. The default setting is enabled.

Note  If the local and/or client certificates are required and you want to force all EAP-FAST clients to use certificates, unselect the Anonymous Provision check box.

g. Click Apply to commit your changes.
Step 8  Enable local EAP on a WLAN as follows:
   a. Choose WLANs to open the WLANs page.
   b. Click the ID number of the desired WLAN.
   c. When the WLANs > Edit page appears, choose the Security > AAA Servers tabs to open the
      WLANs > Edit (Security > AAA Servers) page.
   d. Select the Local EAP Authentication check box to enable local EAP for this WLAN.
   e. From the EAP Profile Name drop-down list, choose the EAP profile that you want to use for this
      WLAN.
   f. If desired, choose the LDAP server that you want to use with local EAP on this WLAN from the
      LDAP Servers drop-down lists.
   g. Click Apply to commit your changes.

Step 9  Click Save Configuration to save your changes.

Configuring Local EAP (CLI)

Note  EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC use certificates for authentication, and EAP-FAST
uses either certificates or PACs. The controller is shipped with Cisco-installed device and Certificate
Authority (CA) certificates. However, if you want to use your own vendor-specific certificates, they must
be imported on the controller.

Step 1  If you are configuring local EAP to use one of the EAP types listed in the note above, make sure that the
appropriate certificates and PACs (if you will use manual PAC provisioning) have been imported on the
controller.

Step 2  If you want the controller to retrieve user credentials from the local user database, make sure that you
have properly configured the local network users on the controller.

Step 3  If you want the controller to retrieve user credentials from an LDAP backend database, make sure that
you have properly configured an LDAP server on the controller.

Step 4  Specify the order in which user credentials are retrieved from the local and/or LDAP databases by
entering this command:

```
config local-auth user-credentials {local | ldap}
```

Note  If you enter the config local-auth user-credentials ldap local command, local EAP attempts to
authenticate clients using the LDAP backend database and fails over to the local user database if the
LDAP servers are not reachable. If the user is not found, the authentication attempt is rejected. If you enter the config local-auth user-credentials local ldap command, local EAP
attempts to authenticate using only the local user database. It does not fail over to the LDAP
backend database.

Step 5  Specify values for the local EAP timers by entering these commands:
- `config local-auth active-timeout timeout`—Specifies the amount of time (in seconds) in which the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fails. The valid range is 1 to 3600 seconds, and the default setting is 100 seconds.

- `config advanced eap identity-request-timeout timeout`—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP identity request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.

- `config advanced eap identity-request-retries retries`—Specifies the maximum number of times that the controller attempts to retransmit the EAP identity request to wireless clients using local EAP. The valid range is 1 to 20 retries, and the default setting is 20 retries.

- `config advanced eap key-index index`—Specifies the key index used for dynamic wired equivalent privacy (WEP). The default value is 0, which corresponds to a key index of 1; the valid values are 0 to 3 (key index of 1 to 4).

- `config advanced eap request-timeout timeout`—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.

- `config advanced eap request-retries retries`—Specifies the maximum number of times that the controller attempts to retransmit the EAP request to wireless clients using local EAP. The valid range is 1 to 120 retries, and the default setting is 20 retries.

- `config advanced eap eapol-key-timeout timeout`—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 1 to 5 seconds, and the default setting is 1 second.

- `config advanced eap eapol-key-retries retries`—Specifies the maximum number of times that the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 0 to 4 retries, and the default setting is 2 retries.

- `config advanced eap max-login-ignore-identity-response {enable | disable}`—When enabled, this command limits the number of devices that can be connected to the controller with the same username. You can log in up to eight times from different devices (PDA, laptop, IP phone, and so on) on the same controller. The default value is enabled.

**Step 6** Create a local EAP profile by entering this command:

```
config local-auth eap-profile add profile_name
```

**Note** Do not include spaces within the profile name.

**Note** To delete a local EAP profile, enter the `config local-auth eap-profile delete profile_name` command.

**Step 7** Add an EAP method to a local EAP profile by entering this command:

```
config local-auth eap-profile method add method profile_name
```

The supported methods are leap, fast, tls, and peap.

Note
If you choose peap, both PEAPv0/MSCHAPv2 or PEAPv1/GTC are enabled on the controller.

Note
You can specify more than one EAP type per profile. However, if you create a profile with multiple EAP types that use certificates (such as EAP-FAST with certificates, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC), all of the EAP types must use the same certificate (from either Cisco or another vendor).

Note
To delete an EAP method from a local EAP profile, enter the config local-auth eap-profile method delete method profile_name command:

Step 8
Configure EAP-FAST parameters if you created an EAP-FAST profile by entering this command:

```
config local-auth method fast
```

where ? is one of the following:

- `anon-prov {enable | disable}` — Configures the controller to allow anonymous provisioning, which allows PACs to be sent automatically to clients that do not have one during PAC provisioning.
- `authority-id auth_id` — Specifies the authority identifier of the local EAP-FAST server.
- `pac-ttl days` — Specifies the number of days for the PAC to remain viable.
- `server-key key` — Specifies the server key used to encrypt and decrypt PACs.

Step 9
Configure certificate parameters per profile by entering these commands:

- `config local-auth eap-profile method fast local-cert {enable | disable} profile_name` — Specifies whether the device certificate on the controller is required for authentication.

  Note
  This command applies only to EAP-FAST because device certificates are not used with LEAP and are mandatory for EAP-TLS and PEAP.

- `config local-auth eap-profile method fast client-cert {enable | disable} profile_name` — Specifies whether wireless clients are required to send their device certificates to the controller in order to authenticate.

  Note
  This command applies only to EAP-FAST because client certificates are not used with LEAP or PEAP and are mandatory for EAP-TLS.

- `config local-auth eap-profile cert-issuer {cisco | vendor} profile_name` — If you specified EAP-FAST with certificates, EAP-TLS, or PEAP, specifies whether the certificates that will be sent to the client are from Cisco or another vendor.

- `config local-auth eap-profile cert-verify ca-issuer {enable | disable} profile_name` — If you chose EAP-FAST with certificates or EAP-TLS, specifies whether the incoming certificate from the client is to be validated against the CA certificates on the controller.

- `config local-auth eap-profile cert-verify cn-verify {enable | disable} profile_name` — If you chose EAP-FAST with certificates or EAP-TLS, specifies whether the common name (CN) in the incoming certificate is to be validated against the CA certificates’ CN on the controller.
• `config local-auth eap-profile cert-verify date-valid {enable | disable} profile_name`—If you chose EAP-FAST with certificates or EAP-TLS, specifies whether the controller is to verify that the incoming device certificate is still valid and has not expired.

**Step 10**
Enable local EAP and attach an EAP profile to a WLAN by entering this command:

```
config wlan local-auth enable profile_name wlan_id
```

---

**Note**
To disable local EAP for a WLAN, enter the `config wlan local-auth disable wlan_id` command.

**Step 11**
Save your changes by entering this command:

```
save config
```

**Step 12**
View information pertaining to local EAP by entering these commands:

• `show local-auth config`—Shows the local EAP configuration on the controller.

  User credentials database search order:
  Primary ..................................... Local DB

  Timer:
  Active timeout .............................. 300

  Configured EAP profiles:
  Name ........................................ fast-cert
  Certificate issuer ......................... vendor
  Peer verification options:
  Check against CA certificates ............ Enabled
  Verify certificate CN identity ............ Disabled
  Check certificate date validity .......... Enabled
  EAP-FAST configuration:
  Local certificate required ............... Yes
  Client certificate required .............. Yes
  Enabled methods ........................... fast
  Configured on WLANS ...................... 1

  Name ........................................ tls
  Certificate issuer ......................... vendor
  Peer verification options:
  Check against CA certificates ............ Enabled
  Verify certificate CN identity ............ Disabled
  Check certificate date validity .......... Enabled
  EAP-FAST configuration:
  Local certificate required ............... No
  Client certificate required .............. No
  Enabled methods ........................... tls
  Configured on WLANS ...................... 2

  EAP Method configuration:
  EAP-FAST:
  Server key ................................ <hidden>
  TTL for the PAC ............................ 10
  Anonymous provision allowed ............. Yes
  Accept client on auth prov ............... No
  Authority ID .............................. 436973636f000000000000000000000000
  Authority Information ................... Cisco A-ID

• `show local-auth statistics`—Shows the local EAP statistics.

• `show local-auth certificates`—Shows the certificates available for local EAP.
Chapter 7  Configuring Security Solutions

- **show local-auth user-credentials**—Shows the priority order that the controller uses when retrieving user credentials from the local and/or LDAP databases.

- **show advanced eap**—Shows the timer values for local EAP.

  EAP-Identity-Request Timeout (seconds)........... 1
  EAP-Identity-Request Max Retries...................... 20
  EAP Key-Index for Dynamic WEP......................... 0
  EAP Max-Login Ignore Identity Response............. enable
  EAP-Request Timeout (seconds)....................... 20
  EAP-Request Max Retries........................... 20
  EAPOL-Key Timeout (seconds)....................... 1
  EAPOL-Key Max Retries........................... 2

- **show ap stats wlan Cisco_AP**—Shows the EAP timeout and failure counters for a specific access point for each WLAN.

- **show client detail client_mac**—Shows the EAP timeout and failure counters for a specific associated client. These statistics are useful in troubleshooting client association issues.

  ```
  Client Statistics:
  Number of Bytes Received................. 10
  Number of Bytes Sent....................... 10
  Number of Packets Received............... 2
  Number of Packets Sent..................... 2
  Number of EAP Id Request Msg Timeouts..... 0
  Number of EAP Id Request Msg Failures..... 0
  Number of EAP Request Msg Timeouts........ 2
  Number of EAP Request Msg Failures........ 1
  Number of EAP Key Msg Timeouts............. 0
  Number of EAP Key Msg Failures............. 0
  Number of Policy Errors................... 0
  Radio Signal Strength Indicator.......... Unavailable
  Signal to Noise Ratio...................... Unavailable
  ```

- **show wlan wlan_id**—Shows the status of local EAP on a particular WLAN.

  **Step 13** (Optional) Troubleshoot local EAP sessions by entering these commands:

  - **debug aaa local-auth eap method { all | errors | events | packets | sm } { enable | disable }**—Enables or disables debugging of local EAP methods.

  - **debug aaa local-auth eap framework { all | errors | events | packets | sm } { enable | disable }**—Enables or disables debugging of the local EAP framework.

  **Note** In these two debug commands, *sm* is the state machine.

- **clear stats local-auth**—Clears the local EAP counters.

- **clear stats ap wlan Cisco_AP**—Clears the EAP timeout and failure counters for a specific access point for each WLAN.

  ```
  WLAN  1
  EAP Id Request Msg Timeouts............... 0
  EAP Id Request Msg Timeouts Failures..... 0
  EAP Request Msg Timeouts................... 2
  EAP Request Msg Timeouts Failures......... 1
  EAP Key Msg Timeouts....................... 0
  EAP Key Msg Timeouts Failures............... 0
  WLAN  2
  EAP Id Request Msg Timeouts............... 1
  EAP Id Request Msg Timeouts Failures..... 0
  EAP Request Msg Timeouts................... 0
  ```
Information About SpectraLink NetLink Telephones

For the best integration with the Cisco UWN solution, SpectraLink NetLink Telephones require an extra operating system configuration step: enable long preambles. The radio preamble (sometimes called a header) is a section of data at the head of a packet that contains information that wireless devices need when sending and receiving packets. Short preambles improve throughput performance, so they are enabled by default. However, some wireless devices, such as SpectraLink NetLink phones, require long preambles.

Configuring SpectraLink NetLink Phones

This section contains the following topics:
- Enabling Long Preambles (GUI), page 7-47
- Enabling Long Preambles (CLI), page 7-48
- Configuring Enhanced Distributed Channel Access (CLI), page 7-49

Enabling Long Preambles (GUI)

1. Choose Wireless > 802.11b/g/n > Network to open the 802.11b/g Global Parameters page.
2. If the Short Preamble check box is selected, continue with this procedure. However, if the Short Preamble check box is unselected (which means that long preambles are enabled), the controller is already optimized for SpectraLink NetLink phones and you do not need to continue this procedure.
3. Unselect the Short Preamble check box to enable long preambles.
4. Click Apply to update the controller configuration.
Step 5  Choose Commands > Reboot > Reboot > Save and Reboot to reboot the controller. Click OK in response to this prompt:

Configuration will be saved and the controller will be rebooted. Click ok to confirm.

The controller reboots.

Step 6  Log back into the controller GUI to verify that the controller is properly configured.

Step 7  Choose Wireless > 802.11b/g/n > Network to open the 802.11b Global Parameters page. If the Short Preamble check box is unselected, the controller is optimized for SpectraLink NetLink phones.

---

**Enabling Long Preambles (CLI)**

Step 1  Log on to the controller CLI.

Step 2  Enter the show 802.11b command and select the Short preamble mandatory parameter. If the parameter indicates that short preambles are enabled, continue with this procedure. This example shows that short preambles are enabled:

Short Preamble mandatory....................... Enabled

However, if the parameter shows that short preambles are disabled (which means that long preambles are enabled), the controller is already optimized for SpectraLink NetLink phones and you do not need to continue this procedure.

Step 3  Disable the 802.11b/g network by entering this command:

```
config 802.11b disable network
```

You cannot enable long preambles on the 802.11a network.

Step 4  Enable long preambles by entering this command:

```
config 802.11b preamble long
```

Step 5  Reenable the 802.11b/g network by entering this command:

```
config 802.11b enable network
```

Step 6  Enter the reset system command to reboot the controller. Enter y at the prompt to save the system changes. The controller reboots.

Step 7  Verify that the controller is properly configured by logging back into the CLI and entering the show 802.11b command to view these parameters:

```
802.11b Network................................ Enabled
Short Preamble mandatory....................... Disabled
```

These parameters show that the 802.11b/g network is enabled and that short preambles are disabled.
Configuring Enhanced Distributed Channel Access (CLI)

To configure 802.11 enhanced distributed channel access (EDCA) parameters to support SpectraLink phones, enter this command:

```
config advanced edca-parameters {svp-voice | wmm-default}
```

where

- `svp-voice` enables SpectraLink voice priority (SVP) parameters and `wmm-default` enables wireless multimedia (WMM) default parameters.

**Note**
To propagate this command to all access points connected to the controller, make sure to disable and then reenable the 802.11b/g network after entering this command.

Configuring RADIUS NAC Support

This section contains the following topics:

- Information About RADIUS NAC Support, page 7-49
- Guidelines and Limitations, page 7-50
- Configuring RADIUS NAC Support (GUI), page 7-51
- Configuring RADIUS NAC Support (CLI), page 7-51

Information About RADIUS NAC Support

The Cisco Identity Services Engine (ISE) is a next-generation, context-based access control solution that provides the functions of Cisco Secure Access Control System (ACS) and Cisco Network Admission Control (NAC) in one integrated platform.

ISE has been introduced in the 7.0.116.0 release of the Cisco Unified Wireless Network. ISE can be used to provide advanced security for your deployed network. It is an authentication server that you can configure on your controller. When a client associates to the controller on a RADIUS NAC–enabled WLAN, the controller forwards the request to the ISE server.

The ISE server validates the user in the database and on successful authentication, the URL and pre-AUTH ACL are sent to the client. The client then moves to the Posture Required state and is redirected to the URL returned by the ISE server. The NAC agent in the client triggers the posture validation process. On successful posture validation by the ISE server, the client is moved to the run state.

Device Registration

To get devices such as tablets or smart phones to be connected to the corporate wireless network, the device must first be registered. The device is registered with the ISE server before being allowed complete access. Device registration occurs in an open WLAN with MAC filtering enabled before it is connected to the corporate network WLAN.
Central Web Authentication

In the case of Central Web Authentication (CWA), the web-authentication occurs on the ISE server. The web portal in the ISE server provides a login page to the client. Once the credentials are verified on the ISE server, the client is provisioned. The client remains in the POSTURE_REQD state until a CoA is reached. The credentials and ACLs are received from the ISE server.

Local Web Authentication

In the case of Local Web Authentication (LWA), the controller provides a web-auth login page against which the username and password are verified. Once the client credentials are verified, the ISE server with the restricted ACL and the URL are sent to the client.

The client remains in POSTURE_REQD state until a change of authorization (CoA) is reached.

Table 7-8 describes the possible combinations in a typical ISE deployment with device registration, CWA, and LWA enabled.

Guidelines and Limitations

- A RADIUS NAC-enabled WLAN supports Open Authentication and MAC filtering. If you are using local web authentication with RADIUS NAC, the Layer 3 web authentication must also be enabled.
- In local web authentication, the Web Auth priority order must be configured as RADIUS.
- RADIUS NAC functionality does not work if the configured accounting server is different from the authentication (ISE) server. You should configure the same server as the authentication and accounting server if ISE functions are used. If ISE is used only for ACS functionality, the accounting server can be flexible. Dot1x authentication must be enabled.
- When clients move from one WLAN to another, the controller retains the client’s audit session ID if it returns to the WLAN before the idle timeout occurs. As a result, when the clients join the controller before the idle timeout session expires, they are immediately moved to the RUN state. The clients are validated if they reassociate with the controller after the session timeout.
- Suppose you have two WLANs, where WLAN 1 is configured on a controller (WLC1) and WLAN2 is configured on another controller (WLC2) and both are RADIUS NAC enabled. The client first connects to WLC1 and moves to the RUN state after posture validation. Assume that the client now moves to WLC2. If the client connects back to WLC1 before the PMK expires for this client in WLC1, the posture validation is skipped for the client. The client directly moves to the RUN state and bypasses the posture validation because the controller retains the old audit session ID for the client that is already known to ISE.
- When deploying RADIUS NAC in your wireless network, do not configure a primary and secondary ISE server. Instead, we recommend that you configure HA between the two ISE servers. Having a primary and secondary ISE setup will require a posture validation to happen before the clients move to the RUN state. If HA is configured, the client is automatically moved to the RUN state in the fallback ISE server.
- The controller software configured with RADIUS NAC does not support a change of authorization (CoA) on the service port.
- Do not swap AAA server indexes in a live network because clients might get disconnected and have to reconnect to the RADIUS server, which might result in log messages to be appended to the ISE server logs.
- You must enable AAA override on the WLAN to use RADIUS NAC.
- WPA and WPA2 or dot1X must be enabled on the WLAN.
- During slow roaming, the client goes through posture validation.
- Guest tunneling mobility is not supported for ISE NAC–enabled WLANs.
- VLAN select is not supported
- Workgroup bridges are not supported.
- The AP Group over NAC is not supported over RADIUS NAC.
- FlexConnect local switching is not supported.
- With RADIUS NAC enabled, the RADIUS server overwrite interface is not supported.

### Configuring RADIUS NAC Support (GUI)

**Step 1** Choose the **WLANs** tab.

**Step 2** Click the WLAN ID of the WLAN for which you want to enable ISE.

The **WLANs > Edit** page appears.

**Step 3** Click the **Advanced** tab.

**Step 4** From the NAC State drop-down list, choose **Radius NAC**:

- **SNMP NAC**—Uses SNMP NAC for the WLAN.
- **Radius NAC**—Uses Radius NAC for the WLAN

**Note** AAA override is automatically enabled when you use RADIUS NAC on a WLAN.

**Step 5** Click **Apply**.

### Configuring RADIUS NAC Support (CLI)

```
config wlan nac radius {enable | disable} wlan wlan_id
```

### Using Management Over Wireless

This section contains the following topics:

- Information About Management Over Wireless, page 7-52
- Enabling Management over Wireless (GUI), page 7-52
- Enabling Management over Wireless (CLI), page 7-52
Information About Management Over Wireless

The management over wireless feature allows you to monitor and configure local controllers using a wireless client. This feature is supported for all management tasks except uploads to and downloads from (transfers to and from) the controller.

Enabling Management over Wireless (GUI)

Step 1  Choose Management > Mgmt Via Wireless to open the Management Via Wireless page.
Step 2  Select the Enable Controller Management to be accessible from Wireless Clients check box to enable management over wireless for the WLAN or unselect it to disable this feature. The default value is unselected.
Step 3  Click Apply to commit your changes.
Step 4  Click Save Configuration to save your changes.

Enabling Management over Wireless (CLI)

Step 1  Verify whether the management over wireless interface is enabled or disabled by entering this command:
show network summary
If disabled, continue with Step 2. Otherwise, continue with Step 3.
Step 2  Enable management over wireless by entering this command:
config network mgmt-via-wireless enable
Step 3  Use a wireless client to associate with an access point connected to the controller that you want to manage.
Step 4  Log into the CLI to verify that you can manage the WLAN using a wireless client by entering this command:
telnet controller-ip-address command

Using Dynamic Interfaces for Management

This section contains the following topics:
• Information About Using Dynamic Interfaces for Management, page 7-53
• Enabling Management using Dynamic Interfaces (CLI), page 7-53
Information About Using Dynamic Interfaces for Management

You can access the controller with one of its dynamic interface IP addresses. While wired computers can have only CLI access with the dynamic interface of the WLC, wireless clients have both CLI and GUI access with the dynamic interface.

When the management using dynamic interfaces is disabled, a device can open an SSH connection if the protocol is enabled. However, users are not prompted to log on. Additionally, the management address remains accessible from a dynamic interface VLAN unless a CPU ACL is in place.

Enabling Management using Dynamic Interfaces (CLI)

```
config network mgmt-via-dynamic-interface { enable | disable }
```

**Note**
When the management using dynamic interfaces feature is disabled, ensure that ports 22 and 443 on the dynamic interface are closed. Use the `config network ssh disable` command to close port 22; and use the `config network secureweb disable` command to close port 443.

Configuring DHCP Option 82

This section contains the following topics:
- Information About DHCP Option 82, page 7-53
- Guidelines and Limitations, page 7-54
- Configuring DHCP Option 82 (GUI), page 7-54
- Configuring DHCP Option 82 (CLI), page 7-55
- Additional References, page 7-56

Information About DHCP Option 82

DHCP option 82 provides additional security when DHCP is used to allocate network addresses. Specifically, it enables the controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. The controller can be configured to add option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.
Figure 7-10  
**DHCP Option 82**

The access point forwards all DHCP requests from a client to the controller. The controller adds the DHCP option 82 payload and forwards the request to the DHCP server. The payload can contain the MAC address or the MAC address and SSID of the access point, depending on how you configure this option.

![Diagram of DHCP Option 82](image)

**Note**
Any DHCP packets that already include a relay agent option are dropped at the controller.

**Guidelines and Limitations**

DHCP option 82 is not supported for use with auto-anchor mobility, which is described in Chapter 15, “Configuring Mobility Groups.”

In controller software release 4.0 or later releases, you can configure DHCP option 82 using the controller CLI. In controller software release 6.0 or later releases, you can configure this feature using either the GUI or CLI.

**Configuring DHCP Option 82 (GUI)**

**Step 1**  Choose **Controller > Advanced > DHCP** to open the DHCP Parameters page.

**Figure 7-11  **
**DHCP Parameters Page**

**Step 2**  Select the **Enable DHCP Proxy** check box to enable DHCP proxy.

**Step 3**  Choose one of the following options from the DHCP Option 82 Remote ID text box Format drop-down list to specify the format of the DHCP option 82 payload:

- **AP-MAC**—Adds the MAC address of the access point to the DHCP option 82 payload. This is the default value.
Configuring DHCP Option 82

- **AP-MAC-SSID**—Adds the MAC address and SSID of the access point to the DHCP option 82 payload.
- **AP-ETHMAC**—Adds the Ethernet MAC address of the access point to the DHCP option 82 payload.

**Note**
If the SSID is associated with a dynamic interface, then the DHCP Option 82 that you configure must be enabled on the dynamic interface.

**Step 4**
Click **Apply** to commit your changes.

**Step 5**
Click **Save Configuration** to save your changes.

### Configuring DHCP Option 82 (CLI)

- Configure the format of the DHCP option 82 payload by entering one of these commands:
  - **config dhcp opt-82 remote-id ap_mac**
    This command adds the MAC address of the access point to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id ap_mac:ssid**
    This command adds the MAC address and SSID of the access point to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id ap-ethmac**
    Adds the Ethernet MAC address of the access point to the DHCP option 82 payload.

- Override the global DHCP option 82 setting and disable (or enable) this feature for the AP-manager or management interface on the controller by entering this command:
  ```
  config interface dhcp {ap-manager | management} option-82 {disable | enable}
  ```

- See the status of DHCP option 82 on the controller by entering the **show interface detailed ap-manager** command.

```
Interface Name......................... ap-manager
MAC Address............................. 00:0a:88:25:10:c4
IP Address.............................. 10.30.16.13
IP Netmask.............................. 255.255.248.0
IP Gateway.............................. 10.30.16.1
External NAT IP State.................. Disabled
External NAT IP Address............... 0.0.0.0
External NAT IP Netmask................. 0.0.0.0
VLAN.................................... untagged
Active Physical Port.................. LAG (29)
Primary Physical Port................ LAG (29)
Backup Physical Port.................. Unconfigured
Primary DHCP Server................... 10.1.0.10
Secondary DHCP Server............... Unconfigured
DHCP Option 82......................... Enabled
ACL..................................... Unconfigured
AP Manager.............................. Yes
Guest Interface........................ No
```
Configuring and Applying Access Control Lists

This section contains the following topics:

- Information About Access Control Lists, page 7-56
- Guidelines and Limitations, page 7-56
- Configuring and Applying Access Control Lists (GUI), page 7-57
- Configuring and Applying Access Control Lists (CLI), page 7-63

Information About Access Control Lists

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 central processing unit (CPU) to control all traffic destined for the CPU.

You may also want to create a preauthentication ACL for web authentication. Such an ACL could be used to allow certain types of traffic before authentication is complete.

Both IPv4 and IPv6 ACLs are supported. IPv6 ACLs support the same options as IPv4 ACLs including source, destination, source and destination ports.

Guidelines and Limitations

- 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.
- ACLs in your network might need to be modified if CAPWAP uses different ports than LWAPP.
- Adding an ACL on the controller results in the degradation of throughput and could even result in packet loss.
- 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, a controller network module, you must configure a preauthentication ACL on the WLAN for the external web server.
• ACL counters are available only on the following controllers: 5500 series, 2500 series, Cisco WiSM2 and 7500 series Wireless LAN Controller Switch.
• 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 NCS templates. The ACL name must be unique.

**Configuring and Applying Access Control Lists (GUI)**

This section contains the following topics:
• Configuring Access Control Lists, page 7-57
• Applying an Access Control List to an Interface, page 7-60
• Applying an Access Control List to the Controller CPU, page 7-61
• Applying an Access Control List to a WLAN, page 7-61

**Configuring Access Control Lists**

**Step 1** Choose Security > Access Control Lists > Access Control Lists to open the Access Control Lists page.

**Figure 7-12 Access Control Lists Page**

This page lists all of the ACLs and their types (IPv4 or IPv6) that have been configured for this controller.

**Note** If you want to delete an existing ACL, hover your cursor over the blue drop-down arrow for that ACL and choose **Remove**.
Step 2 If you want to see if packets are hitting any of the ACLs configured on your controller, select the **Enable Counters** check box and click **Apply**. Otherwise, leave the check box unselected, which is the default value. This feature is useful when troubleshooting your system.

**Note** If you want to clear the counters for an ACL, hover your cursor over the blue drop-down arrow for that ACL and choose **Clear Counters**.

Step 3 Add a new ACL by clicking **New**. The Access Control Lists > New page appears.

Step 4 In the Access Control List Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 5 Choose the ACL type. There are two ACL types: IPv4 and IPv6.

Step 6 Click **Apply**. When the Access Control Lists page reappears, click the name of the new ACL.

Step 7 When the Access Control Lists > Edit page appears, click **Add New Rule**. The Access Control Lists > Rules > New page appears.

Step 8 Configure a rule for this ACL as follows:

a. The controller supports up to 64 rules for each ACL. These rules are listed in order from 1 to 64. In the Sequence text box, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL.

**Note** If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number for a rule, the sequence numbers for other rules adjust to maintain a continuous sequence. For instance, if you change a rule’s sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

b. From the Source drop-down list, choose one of these options to specify the source of the packets to which this ACL applies:
   - **Any**—Any source (this is the default value).
   - **IP Address**—A specific source. If you choose this option, enter the IP address and netmask of the source in the text boxes. If you are configuring an IPv6 ACL, enter the IPv6 address and prefix length of the destination in the text boxes.

c. From the Destination drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:
   - **Any**—Any destination (this is the default value).
   - **IP Address**—A specific destination. If you choose this option, enter the IP address and netmask of the destination in the text boxes. If you are configuring an IPv6 ACL, enter the IPv6 address and prefix length of the destination in the text boxes.

d. From the Protocol drop-down list, choose the protocol ID of the IP packets to be used for this ACL. These are the protocol options:
   - **Any**—Any protocol (this is the default value)
   - **TCP**—Transmission Control Protocol
   - **UDP**—User Datagram Protocol
   - **ICMP/ICMPv6**—Internet Control Message Protocol
Note: ICMPv6 is only available for IPv6 ACL.

- ESP—IP Encapsulating Security Payload
- AH—Authentication Header
- GRE—Generic Routing Encapsulation
- IP in IP—Internet Protocol (IP) in IP (permits or denies IP-in-IP packets)
- Eth Over IP—Ethernet-over-Internet Protocol
- OSPF—Open Shortest Path First
- Other—Any other Internet Assigned Numbers Authority (IANA) protocol

Note: If you choose Other, enter the number of the desired protocol in the Protocol text box. You can find the list of available protocols in the INAI website.

- The controller can permit or deny only IP packets in an ACL. Other types of packets (such as ARP packets) cannot be specified.

e. If you chose TCP or UDP in the previous step, two additional parameters appear: Source Port and Destination Port. These parameters enable you to choose a specific source port and destination port or port ranges. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications such as Telnet, SSH, HTTP, and so on.

Note: Source and Destination ports based on the ACL type.

f. From the DSCP drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header text box that can be used to define the quality of service across the Internet.
   - Any—Any DSCP (this is the default value)
   - Specific—A specific DSCP from 0 to 63, which you enter in the DSCP edit box

g. From the Direction drop-down list, choose one of these options to specify the direction of the traffic to which this ACL applies:
   - Any—Any direction (this is the default value)
   - Inbound—From the client
   - Outbound—To the client

Note: If you are planning to apply this ACL to the controller CPU, the packet direction does not have any significance, it is always ’Any’.

h. From the Action drop-down list, choose Deny to cause this ACL to block packets or Permit to cause this ACL to allow packets. The default value is Deny.

i. Click Apply to commit your changes. The Access Control Lists > Edit page reappears, showing the rules for this ACL.
The Deny Counters field shows the number of times that packets have matched the explicit deny ACL rule. The Number of Hits field shows the number of times that packets have matched an ACL rule. You must enable ACL counters on the Access Control Lists page to enable these fields.

**Note** If you want to edit a rule, click the sequence number of the desired rule to open the Access Control Lists > Rules > Edit page. If you want to delete a rule, hover your cursor over the blue drop-down arrow for the desired rule and choose Remove.

j. Repeat this procedure to add any additional rules for this ACL.

**Step 9** Click **Save Configuration** to save your changes.

**Step 10** Repeat this procedure to add any additional ACLs.

---

### Applying an Access Control List to an Interface

**Step 1** Choose **Controller > Interfaces**.

**Step 2** Click the name of the desired interface. The Interfaces > Edit page for that interface appears.

**Step 3** From the ACL Name drop-down list, choose the desired ACL and click **Apply**. The default is None.
Chapter 7 Configuring Security Solutions

Configuring and Applying Access Control Lists

**Note** Only IPv4 ACL are supported as interface ACL, see Chapter 4, “Configuring Ports and Interfaces,” for more information on configuring controller interfaces.

**Step 4** Click **Save Configuration** to save your changes.

---

**Applying an Access Control List to the Controller CPU**

**Step 1** Choose **Security > Access Control Lists > CPU Access Control Lists** to open the CPU Access Control Lists page.

**Step 2** Select the **Enable CPU ACL** check box to enable a designated ACL to control the traffic to the controller CPU or unselect the check box to disable the CPU ACL feature and remove any ACL that had been applied to the CPU. The default value is unselected.

**Step 3** From the ACL Name drop-down list, choose the ACL that will control the traffic to the controller CPU. None is the default value when the CPU ACL feature is disabled. If you choose None while the CPU ACL Enable check box is selected, an error message appears indicating that you must choose an ACL.

**Note** This parameter is available only if you have selected the CPU ACL Enable check box.

**Note** When CPU ACL is enabled, it is applicable to both wireless and wired traffic. Only IPv4 ACL are supported as CPU ACL.

**Step 4** Click **Apply** to commit your changes.

**Step 5** Click **Save Configuration** to save your changes.

---

**Applying an Access Control List to a WLAN**

**Step 1** Choose **WLANs** to open the WLANs page.

**Step 2** Click the ID number of the desired WLAN to open the WLANs > Edit page.

**Step 3** Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.
Step 4  From the Override Interface ACL drop-down list, choose the IPv4 or IPv6 ACL that you want to apply to this WLAN. The ACL that you choose overrides any ACL that is configured for the interface. None is the default value.

Note  To support centralized access control through an AAA server such as ISE or ACS, you must configure the IPv4 and IPv6 ACL on the controller and the WLAN must be configured with AAA override enabled feature.

Note  See Chapter 8, “Working with WLANs,” for more information on configuring WLANs.

Step 5  Click Apply to commit your changes.

Step 6  Click Save Configuration to save your changes.

Applying a Preauthentication Access Control List to a WLAN

Step 1  Choose WLANs to open the WLANs page.

Step 2  Click the ID number of the desired WLAN to open the WLANs > Edit page.
Step 3  Choose the Security and Layer 3 tabs to open the WLANs > Edit (Security > Layer 3) page.

Figure 7-15  WLANs > Edit (Security > Layer 3) Page

Step 4  Select the Web Policy check box.

Step 5  From the Preauthentication ACL drop-down list, choose the desired ACL and click Apply. None is the default value.

Note  See Chapter 8, “Working with WLANs,” for more information on configuring WLANs.

Step 6  Click Save Configuration to save your changes.

### Configuring and Applying Access Control Lists (CLI)

#### Configuring Access Control Lists

Step 1  See all of the ACLs that are configured on the controller by entering this command:

```
show acl summary
```

Information similar to the following appears:

<table>
<thead>
<tr>
<th>ACL Counter Status</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL Name</td>
<td>Applied</td>
</tr>
<tr>
<td>acl1</td>
<td>Yes</td>
</tr>
<tr>
<td>acl2</td>
<td>Yes</td>
</tr>
<tr>
<td>acl3</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Step 2  See all of the IPv6 ACLs that are configured on the controller by entering this command:

```
show ipv6 acl summary
```

Step 3  See detailed information for a particular ACL by entering this command:

```
show [ipv6] acl detailed acl_name
```

Information similar to the following appears:
## Configuring and Applying Access Control Lists

### Source

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Source Port Dest Port</th>
<th>DSCP</th>
<th>Action</th>
<th>Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dir IP Address/Netmask</td>
<td>IP Address/Netmask</td>
<td>Prot Range Range DSCP Action DenyCounter</td>
<td>0.0.0.0/0.0.0.0</td>
<td>0.0.0.0/0.0.0.0</td>
<td>Any 0-65535 0-65535</td>
</tr>
<tr>
<td>1 Any</td>
<td>200.200.200.0/255.255.255.0</td>
<td>6</td>
<td>80-80</td>
<td>0-65535</td>
<td>Any</td>
</tr>
</tbody>
</table>

DenyCounter : 0

The Counter text box increments each time a packet matches an ACL rule, and the DenyCounter text box increments each time a packet does not match any of the rules.

**Note** If a traffic/request is allowed from the controller by a permit rule, then the response to the traffic/request in the opposite direction also is allowed and cannot be blocked by a deny rule in the ACL.

### Step 4

Enable or disable ACL counters for your controller by entering this command:

```
config acl counter {start | stop}
```

**Note** If you want to clear the current counters for an ACL, enter the `clear acl counters acl_name` command.

**Note** ACL counters are available only on the Cisco 5500 Series Controller, Cisco 4400 Series Controller, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

### Step 5

Add a new ACL by entering this command:

```
config [ipv6] acl create acl_name
```

You can enter up to 32 alphanumeric characters for the `acl_name` parameter.

**Note** When you try to create an interface name with space, the controller CLI does not create an interface. For example, if you want to create an interface name `int 3`, the CLI will not create this since there is a space between int and 3. If you want to use `int 3` as the interface name, you need to enclose within single quotes like ‘int 3’.

### Step 6

Add a rule for an ACL by entering this command:

```
config [ipv6] acl rule add acl_name rule_index
```

### Step 7

Configure an ACL rule by entering this command:

```
config [ipv6] acl rule
```

- `action acl_name rule_index {permit | deny}`
- `change index acl_name old_index new_index`
- `destination address acl_name rule_index ip_address netmask`
- `destination port range acl_name rule_index start_port end_port`
- `direction acl_name rule_index {in | out | any}`
- `dscp acl_name rule_index dscp`
- `protocol acl_name rule_index protocol`
source address acl_name rule_index ip_address netmask |
source address [ipv6] acl_name rule_index prefix |
swap index acl_name index_1 index_2 |

See Step 8 of the “Configuring and Applying Access Control Lists (GUI)” section on page 7-57 for explanations of the rule parameters.

Step 8
Save your settings by entering this command:

save config

Note: To delete an ACL, enter the config [ipv6] acl delete acl_name command. To delete an ACL rule, enter the config [ipv6] acl rule delete acl_name rule_index command.

---

Applying Access Control Lists

Step 1
Perform any of the following:

- To apply an ACL to a management, AP-manager, or dynamic interface, enter this command:

  config interface acl {management | ap-manager | dynamic_interface_name} acl_name

  Note: To see the ACL that is applied to an interface, enter the show interface detailed {management | ap-manager | dynamic_interface_name} command. To remove an ACL that is applied to an interface, enter the config interface acl {management | ap-manager | dynamic_interface_name} none command.

  See Chapter 4, “Configuring Ports and Interfaces,” for more information on configuring controller interfaces.

- To apply an ACL to the data path, enter this command:

  config acl apply acl_name

- To apply an ACL to the controller CPU to restrict the type of traffic (wired, wireless, or both) reaching the CPU, enter this command:

  config acl cpu acl_name {wired | wireless | both}

  Note: To see the ACL that is applied to the controller CPU, enter the show acl cpu command. To remove the ACL that is applied to the controller CPU, enter the config acl cpu none command.

- To apply an ACL to a WLAN, enter this command:

  config wlan acl wlan_id acl_name

  Note: To see the ACL that is applied to a WLAN, enter the show wlan wlan_id command. To remove the ACL that is applied to a WLAN, enter the config wlan acl wlan_id none command.
To apply a preauthentication ACL to a WLAN, enter this command:

```plaintext
config wlan security web-auth acl wlan_id acl_name
```

See Chapter 8, “Working with WLANs,” for more information on configuring WLANs.

**Step 2**  Save your changes by entering this command:

```plaintext
save config
```

---

**Configuring Management Frame Protection**

This chapter contains the following topics:

- Information About Management Frame Protection, page 7-66
- Guidelines and Limitations, page 7-67
- Configuring Management Frame Protection (GUI), page 7-68
- Viewing the Management Frame Protection Settings (GUI), page 7-69
- Configuring Management Frame Protection (CLI), page 7-70
- Viewing the Management Frame Protection Settings (CLI), page 7-70
- Debugging Management Frame Protection Issues (CLI), page 7-72

---

**Information About Management Frame Protection**

Management frame protection (MFP) provides security for the otherwise unprotected and unencrypted 802.11 management messages passed between access points and clients. MFP provides both infrastructure and client support.

- **Infrastructure MFP**—Protects management frames by detecting adversaries that are invoking denial-of-service attacks, flooding the network with associations and probes, interjecting as rogue access points, and affecting network performance by attacking the QoS and radio measurement frames. It also provides a quick and effective means to detect and report phishing incidents.
  
  Specifically, infrastructure MFP protects 802.11 session management functions by adding message integrity check information elements (MIC IEs) to the management frames emitted by access points (and not those emitted by clients), which are then validated by other access points in the network. Infrastructure MFP is passive. It can detect and report intrusions but has no means to stop them.

- **Client MFP**—Shields authenticated clients from spoofed frames, preventing many of the common attacks against wireless LANs from becoming effective. Most attacks, such as deauthentication attacks, revert to simply degrading performance by contending with valid clients.
  
  Specifically, client MFP encrypts management frames are sent between access points and CCXv5 clients so that both the access points and clients can take preventative action by dropping spoofed class 3 management frames (that is, management frames passed between an access point and a client that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect the following types of class 3 unicast management frames: disassociation, deauthentication, and QoS (WMM) action. Client MFP protects a client-access point session from the most common type of denial-of-service attack. It protects class 3 management frames by using the same encryption method used for the session’s data frames. If a frame received by the access point or client fails decryption, it is dropped, and the event is reported to the controller.
To use client MFP, clients must support CCXv5 MFP and must negotiate WPA2 using either TKIP or AES-CCMP. EAP or PSK may be used to obtain the PMK. CCKM and controller mobility management are used to distribute session keys between access points for Layer 2 and Layer 3 fast roaming.

**Note**
To prevent attacks using broadcast frames, access points supporting CCXv5 will not emit any broadcast class 3 management frames (such as disassociation, deauthentication, or action). CCXv5 clients and access points must discard broadcast class 3 management frames.

Client MFP supplements infrastructure MFP rather than replaces it because infrastructure MFP continues to detect and report invalid unicast frames sent to clients that are not client-MFP capable as well as invalid class 1 and 2 management frames. Infrastructure MFP is applied only to management frames that are not protected by client MFP.

Infrastructure MFP consists of three main components:

- **Management frame protection**—The access point protects the management frames it transmits by adding a MIC IE to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving access point configured to detect MFP frames to report the discrepancy.

- **Management frame validation**—In infrastructure MFP, the access point validates every management frame that it receives from other access points in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an access point that is configured to transmit MFP frames, it reports the discrepancy to the network management system. In order for the timestamps to operate properly, all controllers must be Network Transfer Protocol (NTP) synchronized.

- **Event reporting**—The access point notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and can report the results through SNMP traps to the network management system.

**Note** Client MFP uses the same event reporting mechanisms as infrastructure MFP.

Infrastructure MFP is enabled by default and can be disabled globally. When you upgrade from a previous software release, infrastructure MFP is disabled globally if access point authentication is enabled because the two features are mutually exclusive. Once infrastructure MFP is enabled globally, signature generation (adding MICs to outbound frames) can be disabled for selected WLANs, and validation can be disabled for selected access points.

Client MFP is enabled by default on WLANs that are configured for WPA2. It can be disabled, or it can be made mandatory (in which case, only clients that negotiate MFP are allowed to associate) on selected WLANs.

**Guidelines and Limitations**

- Infrastructure MFP is a global setting only in the 7.0.98.0 release. In the earlier releases, there was an option for you to enable or disable the MFP infrastructure protection for WLANs and MFP infrastructure validation for APs. These options are no longer available in the GUI or CLI.

- Controller software release 4.1 or later releases support both infrastructure and client MFP while controller software release 4.0 supports only infrastructure MFP.

- MFP is supported for use with Cisco Aironet lightweight access points.
• Lightweight access points support infrastructure MFP in local and monitor modes and in FlexConnect mode when the access point is connected to a controller. They support client MFP in local, FlexConnect, and bridge modes.
• OEAP 600 Series Access points do not support MFP.
• Client MFP is supported for use only with CCXv5 clients using WPA2 with TKIP or AES-CCMP.
• Non-CCXv5 clients may associate to a WLAN if client MFP is disabled or optional.
• Error reports generated on a FlexConnect access point in standalone mode cannot be forwarded to the controller and are dropped.

Configuring Management Frame Protection (GUI)

Step 1 Choose Security > Wireless Protection Policies > AP Authentication/MFP to open the AP Authentication Policy page.

Step 2 From the Protection Type drop-down list, enable infrastructure MFP globally for the controller by choosing Management Frame Protection.

Step 3 Click Apply to commit your changes.

Note If more than one controller is included in the mobility group, you must configure a Network Time Protocol (NTP) server on all controllers in the mobility group that are configured for infrastructure MFP.

Step 4 Configure client MFP for a particular WLAN after infrastructure MFP has been enabled globally for the controller as follows:

a. Choose WLANs.
b. Click the profile name of the desired WLAN. The WLANs > Edit page appears.

c. Choose Advanced. The WLANs > Edit (Advanced) page appears.

Figure 7-17 WLANs > Edit (Advanced) Page

![WLANs > Edit (Advanced) Page]

Figure 7-17 WLANs > Edit (Advanced) Page

\[Image of WLANs > Edit (Advanced) Page\]

d. From the MFP Client Protection drop-down list choose Disabled, Optional, or Required. The default value is Optional. If you choose Required, clients are allowed to associate only if MFP is negotiated (that is, if WPA2 is configured on the controller and the client supports CCXv5 MFP and is also configured for WPA2).

Note For Cisco OEAP 600, MFP is not supported. It should either be Disabled or Optional.

e. Click Apply to commit your changes.

Step 5 Click Save Configuration to save your settings.

Viewing the Management Frame Protection Settings (GUI)

To see the controller’s current global MFP settings, choose Security > Wireless Protection Policies > Management Frame Protection. The Management Frame Protection Settings page appears.
Chapter 7 Configuring Security Solutions

Configuring Management Frame Protection

Figure 7-18 Management Frame Protection Settings Page

On this page, you can see the following MFP settings:

- The Management Frame Protection field shows if infrastructure MFP is enabled globally for the controller.
- The Controller Time Source Valid field indicates whether the controller time is set locally (by manually entering the time) or through an external source (such as the NTP server). If the time is set by an external source, the value of this field is “True.” If the time is set locally, the value is “False.” The time source is used for validating the timestamp on management frames between access points of different controllers within a mobility group.
- The Infrastructure Protection field shows if infrastructure MFP is enabled for individual WLANs.
- The Client Protection field shows if client MFP is enabled for individual WLANs and whether it is optional or required.

Configuring Management Frame Protection (CLI)

- Enable or disable infrastructure MFP globally for the controller by entering this command:
  ```
  config wps mfp infrastructure {enable | disable}
  ```
- Enable or disable client MFP on a specific WLAN by entering this command:
  ```
  config wlan mfp client {enable | disable} wlan_id [required]
  ```
  If you enable client MFP and use the optional required parameter, clients are allowed to associate only if MFP is negotiated.

Viewing the Management Frame Protection Settings (CLI)

- See the controller's current MFP settings by entering this command:
  ```
  show wps mfp summary
  ```
  Information similar to the following appears:
  ```
  Global Infrastructure MFP state.... Enabled
  Controller Time Source Valid.... False
  ```
  ```
  WLAN ID  WLAN Name Status  Infra. Protection  Client Protection
  -------  ---------- --------  ---------------  ---------------
  devvesh-AF1010  Enabled  Up  Full  Full
  devvesh-AF1010  Enabled  b/g  Up  Full  Full
  ```
### Configuring Management Frame Protection

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Validation</th>
<th>Radio</th>
<th>State</th>
<th>Protection</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mapAP</td>
<td>Disabled</td>
<td>a</td>
<td>Up</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>b/g</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rootAP2</td>
<td>Enabled</td>
<td>a</td>
<td>Up</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>b/g</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FlexConnect</td>
<td>*Enabled</td>
<td>b/g</td>
<td>Up</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>a</td>
<td>Down</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Command Examples

- **See the current MFP configuration for a particular WLAN by entering this command:**
  
  ```
  show wlan wlan_id
  ```

  Information similar to the following appears:

  ```
  WLAN Identifier........................... 1
  Profile Name.............................. test1
  Network Name (SSID)....................... test1
  Status.................................... Enabled
  MAC Filtering............................. Disabled
  Broadcast SSID............................ Enabled
  ...
  Local EAP Authentication.................. Enabled (Profile 'test')
  Diagnostics Channel....................... Disabled
  Security
  802.11 Authentication:..................... Open System
  Static WEP Keys............................ Disabled
  802.1x.................................... Enabled
  Encryption:................................ 104-bit WEP
  Wi-Fi Protected Access (WPA/WPA2)......... Disabled
  CKIP .................................... Disabled
  IP Security............................... Disabled
  IP Security Passthru....................... Disabled
  Web Based Authentication.................. Disabled
  Web-Passthrough........................... Disabled
  Conditional Web Redirect.................. Disabled
  Auto Anchor.............................. Enabled
  FlexConnect Local Switching............... Disabled
  Infrastructure MFP protection............ Enabled
  Client MFP................................ Required
  ...
  ```

- **See whether client MFP is enabled for a specific client by entering this command:**
  
  ```
  show client detail client_mac
  ```

  Information similar to the following appears:

  ```
  Policy Type...................................... WPA2
  Authentication Key Management............... PSK
  Encryption Cipher............................. CCMP (AES)
  Management Frame Protection.................. Yes
  ```

- **See MFP statistics for the controller by entering this command:**
  
  ```
  show wps mfp statistics
  ```

  Information similar to the following appears:
Note
This report contains no data unless an active attack is in progress. Examples of various error types are shown for illustration only. This table is cleared every 5 minutes when the data is forwarded to any network management stations.

<table>
<thead>
<tr>
<th>BSSID</th>
<th>Radio Validator</th>
<th>AP</th>
<th>Last Source Addr</th>
<th>Found</th>
<th>Error Type</th>
<th>Count</th>
<th>Frame Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:85:56:c1:a0</td>
<td>a</td>
<td>jatwo-1000b</td>
<td>00:01:02:03:04:05</td>
<td>Infra</td>
<td>Invalid MIC</td>
<td>183</td>
<td>Assoc Req</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Probe Req</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Beacon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Infra</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Out of seq</td>
<td>4</td>
<td>Assoc Req</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Beacon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Infra</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Unexpected MIC</td>
<td>85</td>
<td>Reassoc Req</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Beacon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Infra</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Client Decrypt err</td>
<td>1974</td>
<td>Reassoc Req</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Beacon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Infra</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Client Replay err</td>
<td>74</td>
<td>Reassoc Resp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Beacon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Infra</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Client Invalid ICV</td>
<td>174</td>
<td>Reassoc Resp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Beacon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Infra</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Client Invalid header</td>
<td>174</td>
<td>Reassoc Resp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Beacon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Infra</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Client Brdcst disass</td>
<td>174</td>
<td>Reassoc Resp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Beacon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Infra</td>
</tr>
<tr>
<td>00:0b:85:56:c1:a0</td>
<td>b/g</td>
<td>jatwo-1000b</td>
<td>00:01:02:03:04:05</td>
<td>Infra</td>
<td>Out of seq</td>
<td>185</td>
<td>Reassoc Resp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Beacon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Infra</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Client Not encrypted</td>
<td>174</td>
<td>Assoc Resp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Beacon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Infra</td>
</tr>
</tbody>
</table>
|           |                 |          |                  |        | Debugging Management Frame Protection Issues (CLI)

Use this command if you experience any problems with MFP:

- **debug wps mfp** ? {enable | disable}

  where ? is one of the following:

  - **client**—Configures debugging for client MFP messages.
  - **capwap**—Configures debugging for MFP messages between the controller and access points.
  - **detail**—Configures detailed debugging for MFP messages.
  - **report**—Configures debugging for MFP reporting.
  - **mm**—Configures debugging for MFP mobility (inter-controller) messages.

**Configuring Client Exclusion Policies**

This section contains the following topics:

- **Configuring Client Exclusion Policies (GUI)**, page 7-73
- **Configuring Client Exclusion Policies (CLI)**, page 7-73
Configuring Client Exclusion Policies (GUI)

**Step 1** Choose Security > Wireless Protection Policies > Client Exclusion Policies to open the Client Exclusion Policies page.

**Figure 7-19 Client Exclusion Policies Page**

- **Step 2** Select any of these check boxes if you want the controller to exclude clients for the condition specified. The default value for each exclusion policy is enabled.
  - **Excessive 802.11 Association Failures**—Clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
  - **Excessive 802.11 Authentication Failures**—Clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
  - **Excessive 802.1X Authentication Failures**—Clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
  - **IP Theft or IP Reuse**—Clients are excluded if the IP address is already assigned to another device.
  - **Excessive Web Authentication Failures**—Clients are excluded on the fourth web authentication attempt, after three consecutive failures.

- **Step 3** Click **Apply** to commit your changes.

- **Step 4** Click **Save Configuration** to save your changes.

Configuring Client Exclusion Policies (CLI)

**Step 1** Enable or disable the controller to exclude clients on the sixth 802.11 association attempt, after five consecutive failures by entering this command:

```
config wps client-exclusion 802.11-assoc {enable | disable}
```

**Step 2** Enable or disable the controller to exclude clients on the sixth 802.11 authentication attempt, after five consecutive failures by entering this command:

```
config wps client-exclusion 802.11-auth {enable | disable}
```

**Step 3** Enable or disable the controller to exclude clients on the fourth 802.1X authentication attempt, after three consecutive failures by entering this command:

```
config wps client-exclusion 802.1x-auth {enable | disable}
```
Step 4  Enable or disable the controller to exclude clients if the IP address is already assigned to another device by entering this command:

```
config wps client-exclusion ip-theft {enable | disable}
```

Step 5  Enable or disable the controller to exclude clients on the fourth web authentication attempt, after three consecutive failures by entering this command:

```
config wps client-exclusion web-auth {enable | disable}
```

Step 6  Enable or disable the controller to exclude clients for all of the above reasons by entering this command:

```
config wps client-exclusion all {enable | disable}
```

Step 7  Use the following command to add or delete client exclusion entries.

```
config exclusionlist {add MAC [description] | delete MAC | description MAC [description]}
```

Step 8  Save your changes by entering this command:

```
save config
```

Step 9  See a list of clients that have been dynamically excluded, by entering this command:

```
show exclusionlist
```

Information similar to the following appears:

```
Dynamically Disabled Clients
----------------------------
MAC Address             Exclusion Reason        Time Remaining (in secs)
-----------             ----------------        ------------------------
00:40:96:b4:82:55         802.1X Failure          51
```

Step 10 See the client exclusion policy configuration settings by entering this command:

```
show wps summary
```

Information similar to the following appears:

```
Auto-Immune
  Auto-Immune........................................ Disabled

Client Exclusion Policy
  Excessive 802.11-association failures........... Enabled
  Excessive 802.11-authentication failures........ Enabled
  Excessive 802.1x-authentication.................. Enabled
  IP-theft........................................... Enabled
  Excessive Web authentication failure......... Enabled

Signature Policy
  Signature Processing.......................... Enabled
```
Configuring Identity Networking

Information About Identity Networking

In most wireless LAN systems, each WLAN has a static policy that applies to all clients associated with an SSID. Although powerful, this method has limitations because it requires clients to associate with different SSIDs to inherit different QoS and security policies.

However, the Cisco Wireless LAN solution supports identity networking, which allows the network to advertise a single SSID but allows specific users to inherit different QoS or security policies based on their user profiles. The specific policies that you can control using identity networking are as follows:

- Quality of Service—When present in a RADIUS Access Accept, the QoS Level value overrides the QoS value specified in the WLAN profile.
- ACL—When the ACL attribute is present in the RADIUS Access Accept, the system applies the ACL name to the client station after it authenticates, which overrides any ACLs that are assigned to the interface.
- VLAN—When a VLAN Interface-name or VLAN tag is present in a RADIUS Access Accept, the system places the client on a specific interface.

Note: The VLAN feature only supports MAC filtering, 802.1X, and WPA. The VLAN feature does not support web authentication or IPsec.

- Tunnel Attributes.

Note: When any of the other RADIUS attributes (QoS-Level, ACL-Name, Interface-Name, or VLAN-Tag), which are described later in this section, are returned, the Tunnel Attributes must also be returned.

The operating system's local MAC filter database has been extended to include the interface name, allowing local MAC filters to specify to which interface the client should be assigned. A separate RADIUS server can also be used, but the RADIUS server must be defined using the Security menus.

RADIUS Attributes Used in Identity Networking

This section explains the RADIUS attributes used in identity networking. This section contains the following topics:

- QoS-Level, page 7-76
- ACL-Name, page 7-76
- Interface-Name, page 7-76
- VLAN-Tag, page 7-77
- Tunnel Attributes, page 7-78
QoS-Level

This attribute indicates the QoS level to be applied to the mobile client's traffic within the switching fabric, as well as over the air. This example shows a summary of the QoS-Level Attribute format. The text boxes are transmitted from left to right.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Vendor-Id</th>
</tr>
</thead>
</table>

Vendor-Id (cont.) | Vendor type | Vendor length |
| QoS Level |

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 2
- Vendor length – 4
- Value – Three octets:
  - 0 – Bronze (Background)
  - 1 – Silver (Best Effort)
  - 2 – Gold (Video)
  - 3 – Platinum (Voice)

ACL-Name

This attribute indicates the ACL name to be applied to the client. A summary of the ACL-Name Attribute format is shown below. The text boxes are transmitted from left to right.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Vendor-Id</th>
</tr>
</thead>
</table>

Vendor-Id (cont.) | Vendor type | Vendor length |
| ACL Name... |

- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179
- Vendor type – 6
- Vendor length – >0
- Value – A string that includes the name of the ACL to use for the client

Interface-Name

This attribute indicates the VLAN Interface a client is to be associated to. A summary of the Interface-Name Attribute format is shown below. The text boxes are transmitted from left to right.
### Configuring Identity Networking

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Vendor-Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor-Id (cont.)</td>
<td>Vendor type</td>
<td>Vendor length</td>
</tr>
</tbody>
</table>

| Interface Name... |

- **Type** – 26 for Vendor-Specific
- **Length** – >7
- **Vendor-Id** – 14179
- **Vendor type** – 5
- **Vendor length** – >0
- **Value** – A string that includes the name of the interface the client is to be assigned to.

**Note**

This Attribute only works when MAC filtering is enabled or if 802.1X or WPA is used as the security policy.

### VLAN-Tag

This attribute indicates the group ID for a particular tunneled session and is also known as the Tunnel-Private-Group-ID attribute.

This attribute might be included in the Access-Request packet if the tunnel initiator can predetermine the group resulting from a particular connection and should be included in the Access-Accept packet if this tunnel session is to be treated as belonging to a particular private group. Private groups may be used to associate a tunneled session with a particular group of users. For example, it may be used to facilitate routing of unregistered IP addresses through a particular interface. It should be included in Accounting-Request packets which contain Acct-Status-Type attributes with values of either Start or Stop and which pertain to a tunneled session.

A summary of the Tunnel-Private-Group-ID Attribute format is shown below. The text boxes are transmitted from left to right.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Tag</th>
<th>String...</th>
</tr>
</thead>
</table>

- **Type** – 81 for Tunnel-Private-Group-ID.
- **Length** – >= 3
- **Tag** – The Tag text box is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel. If the value of the Tag text box is greater than 0x00 and less than or equal to 0x1F, it should be interpreted as indicating which tunnel (of several alternatives) this attribute pertains. If the Tag text box is greater than 0x1F, it should be interpreted as the first byte of the following String text box.
- **String** – This text box must be present. The group is represented by the String text box. There is no restriction on the format of group IDs.
Tunnel Attributes

When any of the other RADIUS attributes (QoS-Level, ACL-Name, Interface-Name, or VLAN-Tag) are returned, the Tunnel Attributes must also be returned.

RFC 2868 defines RADIUS tunnel attributes used for authentication and authorization, and RFC 2867 defines tunnel attributes used for accounting. Where the IEEE 802.1X authenticator supports tunneling, a compulsory tunnel may be set up for the Supplicant as a result of the authentication.

In particular, it may be desirable to allow a port to be placed into a particular VLAN, defined in IEEE 8021Q, based on the result of the authentication. This configuration can be used, for example, to allow a wireless host to remain on the same VLAN as it moves within a campus network.

The RADIUS server typically indicates the desired VLAN by including tunnel attributes within the Access-Accept. However, the IEEE 802.1X authenticator may also provide a hint as to the VLAN to be assigned to the Supplicant by including Tunnel attributes within the AccessRequest.

For use in VLAN assignment, the following tunnel attributes are used:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

The VLAN ID is 12 bits, with a value between 1 and 4094, inclusive. Because the Tunnel-Private-Group-ID is of type String as defined in RFC 2868, for use with IEEE 802.1X, the VLANID integer value is encoded as a string.

When Tunnel attributes are sent, it is necessary to fill in the Tag text box. As noted in RFC 2868, section 3.1:

- The Tag text box is one octet in length and is intended to provide a means of grouping attributes in the same packet that refer to the same tunnel. Valid values for this text box are 0x01 through 0x1F, inclusive. If the Tag text box is unused, it must be zero (0x00).
- For use with Tunnel-Client-Endpoint, Tunnel-Server-Endpoint, Tunnel-Private-Group-ID, Tunnel-Assignment-ID, Tunnel-Client-Auth-ID or Tunnel-Server-Auth-ID attributes (but not Tunnel-Type, Tunnel-Medium-Type, Tunnel-Password, or Tunnel-Preference), a tag text box of greater than 0x1F is interpreted as the first octet of the following text box.
- Unless alternative tunnel types are provided, (e.g. for IEEE 802.1X authenticators that may support tunneling but not VLANs), it is only necessary for tunnel attributes to specify a single tunnel. As a result, where it is only desired to specify the VLANID, the tag text box should be set to zero (0x00) in all tunnel attributes. Where alternative tunnel types are to be provided, tag values between 0x01 and 0x1F should be chosen.

Configuring AAA Override

This section contains the following topics:

- Information About AAA Override, page 7-79
- Guidelines and Limitations, page 7-79
- Updating the RADIUS Server Dictionary File for Proper QoS Values, page 7-79
- Configuring AAA Override (GUI), page 7-80
Information About AAA Override

The Allow AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, QoS, and ACLs to individual clients based on the returned RADIUS attributes from the AAA server.

Guidelines and Limitations

- If a client moves to a new interface due to the AAA override and then you apply an ACL to that interface, the ACL does not take effect until the client reauthenticates. To work around this issue, apply the ACL and then enable the WLAN so that all clients connect to the ACL that is already configured on the interface, or disable and then reenable the WLAN after you apply the interface so that the clients can reauthenticate.
- When the interface group is mapped to a WLAN and clients connect to the WLAN, the client does not get the IP address in a round robin fashion.
- Most of the configuration for allowing AAA override is done at the RADIUS server, where you should configure the Access Control Server (ACS) with the override properties you would like it to return to the controller (for example, Interface-Name, QoS-Level, and VLAN-Tag).
- On the controller, enable the Allow AAA Override configuration parameter using the GUI or CLI. Enabling this parameter allows the controller to accept the attributes returned by the RADIUS server. The controller then applies these attributes to its clients.

Updating the RADIUS Server Dictionary File for Proper QoS Values

If you are using a Steel-Belted RADIUS (SBR), FreeRadius, or similar RADIUS server, clients may not obtain the correct QoS values after the AAA override feature is enabled. For these servers, which allow you to edit the dictionary file, you need to update the file to reflect the proper QoS values: Silver is 0, Gold is 1, Platinum is 2, and Bronze is 3. To update the RADIUS server dictionary file, follow these steps:

Note

This issue does not apply to the Cisco Secure Access Control Server (ACS).

To update the RADIUS server dictionary file, follow these steps:

Step 1: Stop the SBR service (or other RADIUS service).
Step 2: Save the following text to the Radius_Install_Directory\Service folder as ciscowlan.dct:

```plaintext
#CiscoWLAN.dct- Cisco Wireless Lan Controllers
#
#(See README.DCT for more details on the format of this file)
#Dictionary - Cisco WLAN Controllers
#
#Start with the standard Radius specification attributes
```
Configuring AAA Override

Step 3
Open the dictiona.dcm file (in the same directory) and add the line "@ciscowlan.dct."

Step 4
Save and close the dictiona.dcm file.

Step 5
Open the vendor.ini file (in the same directory) and add the following text:

```
vendor-product       = Cisco WLAN Controller
dictionary           = ciscowlan
ignore-ports         = no
port-number-usage    = per-port-type
help-id     =
```

Step 6
Save and close the vendor.ini file.

Step 7
Start the SBR service (or other RADIUS service).

Step 8
Launch the SBR Administrator (or other RADIUS Administrator).

Step 9
Add a RADIUS client (if not already added). Choose Cisco WLAN Controller from the Make/Model drop-down list.

---

**Configuring AAA Override (GUI)**

Step 1
Choose WLANs to open the WLANs page.

Step 2
Click the ID number of the WLAN that you want to configure. The WLANs > Edit page appears.

Step 3
Choose the Advanced tab to open the WLANs > Edit (Advanced) page.
Configure AAA Override (CLI)

```
config wlan aaa override {enable | disable} wlan_id
```
For `wlan_id`, enter an ID from 1 to 16.

Managing Rogue Devices

This section contains the following topics:

- Information About Rogue Devices, page 7-81
- Guidelines and Limitations, page 7-82
- WCS Interaction and Rogue Detection, page 7-83
- Configuring Rogue Detection (GUI), page 7-83
- Configuring Rogue Detection (CLI), page 7-85

Information About Rogue Devices

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 others 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.

Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad-hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees
generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. Even more alarming, wireless users frequently publish unsecure access point locations, increasing the odds of having enterprise security breached.

Detecting Rogue Devices

The controller continuously monitors all 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) to determine if the rogue is attached to your network.

You can configure the controller to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure the controller to use RLDP on all 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 either manually or automatically contain the detected rogue.

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 monitor mode access point.

The containment operation happens in following two ways:

- The container access point goes through the list of containments periodically and sends unicast containment frames. For rogue access point containment, the frames are sent only if there is a rogue client associated.
- Whenever a contained rogue activity is detected, containment frames are transmitted.

The individual rogue containment involves sending a sequence of unicast disassociation and deauthentication frames.

Guidelines and Limitations

- Starting in release 7.0.116.0 and later releases, the controller software provides enhanced rogue containment strategies. In previous releases, when a rogue device was detected, the controller sent containment frames at regular intervals to the rogue devices. In release 7.0.116.0 and later, the containment frames are sent immediately after authorization and associations are detected. The enhanced containment algorithm provides more effective containment of ad hoc clients.
- In a dense RF environment where maximum rogue access points are suspected, the chances of detecting rogue access points by a local and FlexConnect mode access point in channel 157 or 161 are less when compared to other channels. To mitigate this problem, we recommended that you use dedicated monitor mode access points.
- The local and FlexConnect mode access points are designed to serve associated clients and these access points spend relatively less time performing off-channel scanning. The access points spend about 50 milliseconds on each channel. If you want to perform high rogue detection, a monitor mode access point must be used. Alternatively, you can reduce the scan intervals from 180 seconds to a
lesser value, for example, 120 or 60 seconds, ensuring that the radio goes off-channel more frequently which improves the chances of rogue detection. However, the access point would still spend about 50 milliseconds on each channel.

- Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.
- Controller software release 5.0 or later releases improve the classification and reporting of rogue access points through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states. In previous releases, the controller listed all rogue access points on one page sorted by MAC address or BSSID.

**WCS Interaction and Rogue Detection**

WCS software release 5.0 or later releases also support rule-based classification. WCS uses the classification rules configured on the controller. The controller sends traps to WCS after the following events:

- If an unknown access point moves to Friendly for the first time, the controller sends a trap to WCS only if the rogue state is Alert. It does not send a trap if the rogue state is Internal or External.
- If a rogue entry is removed after the timeout expires, the controller sends a trap to WCS for rogue access points categorized as Malicious (Alert, Threat) or Unclassified (Alert). The controller does not remove rogue entries with the following rogue states: Contained, Contained Pending, Internal, and External.

**Configuring Rogue Detection (GUI)**

**Step 1** Make sure that rogue detection is enabled on the desired access points. Rogue detection is enabled by default for all access points joined to the controller (except for OfficeExtend access points). However, in controller software release 6.0 or later releases, you can enable or disable it for individual access points by selecting or unselecting the Rogue Detection check box on the All APs > Details for (Advanced) page.

**Step 2** Choose Security > Wireless Protection Policies > Rogue Policies > General to open the Rogue Policies page.

**Step 3** From the Rogue Location Discovery Protocol drop-down list, choose one of the following options:

- **Disable**—Disables RLDP on all access points. This is the default value.
- **All APs**—Enables RLDP on all access points.
- **Monitor Mode APs**—Enables RLDP only on access points in monitor mode.

**Step 4** In the Expiration Timeout for Rogue AP and Rogue Client Entries text box, enter the number of seconds after which the rogue access point and client entries expire and are removed from the list. The valid range is 240 to 3600 seconds, and the default value is 1200 seconds.

**Note** If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.

**Step 5** If desired, select the Validate Rogue Clients Against AAA check box to use the AAA server or local database to validate if rogue clients are valid clients. The default value is unselected.
Step 6 If desired, select the Detect and Report Ad-Hoc Networks check box to enable ad-hoc rogue detection and reporting. The default value is selected.

Step 7 In the Rogue Detection Report Interval text box, enter the time interval in seconds at which APs should send rogue detection report to the controller. The valid range is from 10 seconds to 300 seconds, and the default value is 10 seconds.

Note This feature is applicable to APs that are in monitor mode only.

Step 8 In the Rogue Detection Minimum RSSI text box, enter the minimum RSSI value that a rogue should have for APs to detect and for a rogue entry to be created in the controller. The valid range is from –128 dBm to 0 dBm, and the default value is 0 dBm.

Note 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.

Step 9 In the Rogue Detection Transient Interval text box, enter the time interval at which a rogue has to be scanned for by the AP after the first time that the rogue is scanned. After the rogue is scanned, updates are sent periodically to the controller. The APs filter transient rogues, which are active for a very short period and are then silent. The valid range is from 120 seconds to 1800 seconds, and the default value is 0.

Note This feature is applicable to APs that are in monitor mode 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.

Step 10 If you want the controller to automatically contain certain rogue devices, select the following check boxes. Otherwise, leave the check boxes unselected, which is the default value.

Caution When you enable any of these parameters, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- 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.

- **Auto Containment Level**—Set the auto containment level by selecting a value from the drop-down list. The default is 1.
- **Auto Containment only for monitor mode APs**—Enable the check box if you want to use only monitor mode access points for auto-containment.
- **Rogue on Wire**—Automatically contains rogues that are detected on the wired network.
• **Using Our SSID**—Automatically contains 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**—Automatically contains a rogue access point to which trusted clients are associated. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.

• **AdHoc Rogue AP**—Automatically contains ad-hoc networks detected by the controller. If you leave this parameter unselected, the controller only generates an alarm when such a network is detected.

**Step 11** Click **Apply** to commit your changes.

**Step 12** Click **Save Configuration** to save your changes.

---

**Configuring Rogue Detection (CLI)**

**Step 1** Make sure that rogue detection is enabled on the desired access points. Rogue detection is enabled by default for all access points joined to the controller (except for OfficeExtend access points). However, in controller software release 6.0 or later releases, you can enable or disable it for individual access points by entering the `config rogue detection` **{enable | disable} Cisco_AP** command.

#### Note
To see the current rogue detection configuration for a specific access point, enter the `show ap config general Cisco_AP` command.

#### Note
Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

**Step 2** Enable, disable, or initiate RLDP by entering these commands:

- `config rogue ap rldp enable alarm-only`—Enables RLDP on all access points.
- `config rogue ap rldp enable alarm-only monitor_ap_only`—Enables RLDP only on access points in monitor mode.
- `config rogue ap rldp initiate rogue_mac_address`—Initiates RLDP on a specific rogue access point.
- `config rogue ap rldp disable`—Disables RLDP on all access points.

**Step 3** Specify the number of seconds after which the rogue access point and client entries expire and are removed from the list by entering this command:

```
cfg ap timeout seconds
```

The valid range for the `seconds` parameter is 240 to 3600 seconds (inclusive), and the default value is 1200 seconds.

#### Note
If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.
Step 4  Enable or disable ad-hoc rogue detection and reporting by entering this command:

```
config rogue adhoc {enable | disable}
```

Step 5  Enable or disable the AAA server or local database to validate if rogue clients are valid clients by entering this command:

```
config rogue client aaa {enable | disable}
```

Step 6  Specify the time interval in seconds at which APs should send rogue detection report to the controller by entering the following command:

```
config rogue detection monitor-ap report-interval time in sec
```

Valid range for the `time in sec` parameter is 10 seconds to 300 seconds, and the default value is 10 seconds.

**Note**  This feature is applicable to APs that are in monitor mode only.

Step 7  Specify the minimum RSSI value that rogues should have for APs to detect and for rogue entry to be created in the controller by entering the following command:

```
config rogue detection min-rssi rssi in dBm
```

Valid range for the `rssi in dBm` parameter is –128 dBm to 0 dBm, and the default value is 0 dBm.

**Note**  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.

Step 8  Specify the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned for by entering the following command:

```
config rogue detection monitor-ap transient-rogue-interval time in sec
```

Valid range for the `time in sec` parameter is 120 seconds to 1800 seconds, and the default value is 0.

**Note**  This feature is applicable to APs that are in monitor mode only.

Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter the rogues based on their transient interval values.

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.

Step 9  If you want the controller to automatically contain certain rogue devices, enter these commands:
Caution

When you enter any of these commands, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- 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.

- `config rogue ap rldp enable auto-contain`—Automatically contains rogues that are detected on the wired network.

- `config rogue ap ssid auto-contain`—Automatically contains rogues that are advertising your network’s SSID.

  **Note** If you want the controller to only generate an alarm when such a rogue is detected, enter the `config rogue ap ssid alarm` command.

- `config rogue ap valid-client auto-contain`—Automatically contains a rogue access point to which trusted clients are associated.

  **Note** If you want the controller to only generate an alarm when such a rogue is detected, enter the `config rogue ap valid-client alarm` command.

- `config rogue adhoc auto-contain`—Automatically contains adhoc networks detected by the controller.

  **Note** If you want the controller to only generate an alarm when such a network is detected, enter the `config rogue adhoc alert` command.

- `configure rogue auto-containment level {1 - 4}`—Sets the auto containment level when you enter a value between 1 and 4. The default is 1.

- `config rogue auto-contain level 1 monitor_mode_ap_only`—Automatically contains only monitor mode access points.

**Step 10** Configure RLDP scheduling by entering this command:

- `config rogue ap rldp schedule add`—Enables you to schedule RLDP on a particular day of the week. You must enter the day of the week (for example `mon`, `tue`, `wed`, and so on) on which you want to schedule RLDP and the start time and end time in HH:MM:SS format. An example is as follows:

  ```
  config rogue ap rldp schedule add mon 22:00:00 23:00:00
  ```

  **Note** When you configure RLDP scheduling, it is assumed that the scheduling would occur in the future, that is, after the configuration is saved.

**Step 11** Save your changes by entering this command:

```
save config
```
Classifying Rogue Access Points

This section contains the following topics:

- Information About Classifying Rogue Access Points, page 7-88
- Configuring Rogue Classification Rules (GUI), page 7-90
- Viewing and Classifying Rogue Devices (GUI), page 7-93
- Configuring Rogue Classification Rules (CLI), page 7-96
- Viewing and Classifying Rogue Devices (CLI), page 7-98

Information About Classifying Rogue Access Points

The controller software now enables you to create rules that can organize and display rogue access points as Friendly, Malicious, or Unclassified.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, and unclassified) in the Alert state only.

Note
Rule-based rogue classification does not apply to ad-hoc rogues and rogue clients.

Note
You can configure up to 64 rogue classification rules per controller.

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies that the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.
2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.
3. If the rogue is already classified as Malicious, Alert, or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
4. The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.
5. If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.
6. The controller repeats the previous steps for all rogue access points.
7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.
8. If desired, you can manually move the access point to a different classification type and rogue state.

Table 7-9 Classification Mapping

<table>
<thead>
<tr>
<th>Rule-Based Classification Type</th>
<th>Rogue States</th>
</tr>
</thead>
</table>
| Friendly                      | • Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. An example is the access points in your lab network.   
• External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. An example is an access point that belongs to a neighboring coffee shop.   
• Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. |
| Malicious                     | • Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list.   
• Threat—The unknown access point is found to be on the network and poses a threat to WLAN security.   
• Contained—The unknown access point is contained.   
• Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources. |
| Unclassified                  | • Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point.   
• Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list.   
• Contained—The unknown access point is contained.   
• Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources. |

If you upgrade to controller software release 5.0 or later releases, the classification and state of the rogue access points are reconfigured as follows:

• From Known to Friendly, Internal
• From Acknowledged to Friendly, External
• From Contained to Malicious, Contained
As mentioned previously, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules, or you can manually move the unknown access point to a different classification type and rogue state.

### Table 7-10 Allowable Classification Type and Rogue State Transitions

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly (Internal, External, Alert)</td>
<td>Malicious (Alert)</td>
</tr>
<tr>
<td>Friendly (Internal, External, Alert)</td>
<td>Unclassified (Alert)</td>
</tr>
<tr>
<td>Friendly (Alert)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Malicious (Alert, Threat)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Malicious (Contained, Contained Pending)</td>
<td>Malicious (Alert)</td>
</tr>
<tr>
<td>Unclassified (Alert, Threat)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Unclassified (Contained, Contained Pending)</td>
<td>Unclassified (Alert)</td>
</tr>
<tr>
<td>Unclassified (Alert)</td>
<td>Malicious (Alert)</td>
</tr>
</tbody>
</table>

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

### Configuring Rogue Classification Rules (GUI)

**Step 1** Choose Security > Wireless Protection Policies > Rogue Policies > Rogue Rules to open the Rogue Rules page.

Any rules that have already been created are listed in priority order. The name, type, and status of each rule is provided.

**Note** If you ever want to delete a rule, hover your cursor over the blue drop-down arrow for that rule and click **Remove**.
Step 2  Create a new rule as follows:
   a. Click Add Rule. An Add Rule section appears at the top of the page.
   b. In the Rule Name text box, enter a name for the new rule. Make sure that the name does not contain any spaces.
   c. From the Rule Type drop-down list, choose Friendly or Malicious to classify rogue access points matching this rule as friendly or malicious.
   d. Click Add to add this rule to the list of existing rules, or click Cancel to discard this new rule.

Step 3  Edit a rule as follows:
   a. Click the name of the rule that you want to edit. The Rogue Rule > Edit page appears.

   b. From the Type drop-down list, choose Friendly or Malicious to classify rogue access points matching this rule as friendly or malicious.

   c. From the Match Operation text box, choose one of the following:
      • Match All—If this rule is enabled, a detected rogue access point must meet all of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule.
      • Match Any—If this rule is enabled, a detected rogue access point must meet any of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule. This is the default value.

   d. To enable this rule, select the Enable Rule check box. The default value is unselected.

   e. From the Add Condition drop-down list, choose one or more of the following conditions that the rogue access point must meet and click Add Condition.
      • SSID—Requires that the rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the User Configured SSID text box, and click Add SSID.

        Note  To delete an SSID, highlight the SSID and click Remove.

      • RSSI—Requires that the rogue access point have a minimum received signal strength indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the Minimum RSSI text box. The valid range is –95 to –50 dBm (inclusive), and the default value is 0 dBm.
Classifying Rogue Access Points

- **Duration**—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the Time Duration text box. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.

- **Client Count**—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the Minimum Number of Rogue Clients text box. The valid range is 1 to 10 (inclusive), and the default value is 0.

- **No Encryption**—Requires that the rogue access point’s advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option.

  **Note**  
  WCS refers to this option as “Open Authentication.”

- **Managed SSID**—Requires that the rogue access point’s managed SSID (the SSID configured for the WLAN) be known to the controller. No further configuration is required for this option.

  **Note**  
  The SSID and Managed SSID conditions cannot be used with the Match All operation because these two SSID lists are mutually exclusive. If you define a rule with Match All and have these two conditions configured, the rogue access points are never classified as friendly or malicious because one of the conditions can never be met.

You can add up to six conditions per rule. When you add a condition, it appears under the Conditions section.

  **Note**  
  If you ever want to delete a condition from this rule, hover your cursor over the blue drop-down arrow for that condition and click **Remove**.

f. Click **Apply** to commit your changes.

**Step 4** Click **Save Configuration** to save your changes.

**Step 5** If you want to change the order in which rogue classification rules are applied, follow these steps:

a. Click **Back** to return to the Rogue Rules page.

b. Click **Change Priority** to access the Rogue Rules > Priority page.

   The rogue rules are listed in priority order in the Change Rules Priority text box.

c. Highlight the rule for which you want to change the priority, and click **Up** to raise its priority in the list or **Down** to lower its priority in the list.

d. Continue to move the rules up or down until the rules are in the desired order.

e. Click **Apply** to commit your changes.

**Step 6** Classify any rogue access points as friendly and add them to the friendly MAC address list as follows:


b. In the MAC Address text box, enter the MAC address of the friendly rogue access point.

c. Click **Apply** to commit your changes.
d. Click **Save Configuration** to save your changes. This access point is added to the controller’s list of friendly access points and should now appear on the Friendly Rogue APs page.

---

**Viewing and Classifying Rogue Devices (GUI)**

---

**Caution** When you choose to **contain a rogue device**, the following warning appears: “There may be legal issues following this containment. Are you sure you want to continue?” The 2.4- 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.

---

**Step 1** Choose **Monitor > Rogues**.

**Step 2** Choose the following options to view the different types of rogue access points detected by the controller:

- Friendly APs
- Malicious APs
- Unclassified APs

---

**Figure 7-23 Rogue APs Page**

The Friendly Rogue APs page, Malicious Rogue APs page, and Unclassified Rogue APs page provide the following information: the MAC address and SSID of the rogue access point, Channel Number, the number of clients connected to the rogue access point, the number of radios that detected the rogue access point, and the current status of the rogue access point.

---

**Note** To remove acknowledged rogues from the database, go to the WLC UI and change the rogue state to Alert Unknown and click Save Configuration. If the rogue is no longer present, it will disappear from the database in 20 minutes.
Note If you ever want to delete a rogue access point from one of these pages, hover your cursor over the blue drop-down arrow and click Remove. To delete multiple rogue access points, check the check box corresponding to the row you want to delete and click Remove Selected.

### Step 3
Obtain more details about a rogue access point by clicking the MAC address of the access point. The Rogue AP Detail page appears.

This page provides the following information: the MAC address of the rogue device, the type of rogue device (such as an access point), whether the rogue device is on the wired network, the dates and times when the rogue device was first and last reported, and the current status of the device.

The Class Type text box shows the current classification for this rogue access point:

- **Friendly**—An unknown access point that matches the user-defined friendly rules or an existing known and acknowledged rogue access point. Friendly access points cannot be contained.
- **Malicious**—An unknown access point that matches the user-defined malicious rules or is moved manually by the user from the Friendly or Unclassified classification type.

Note Once an access point is classified as Malicious, you cannot apply rules to it in the future, and it cannot be moved to another classification type. If you want to move a malicious access point to the Unclassified classification type, you must delete the access point and allow the controller to reclassify it.

- **Unclassified**—An unknown access point that does not match the user-defined friendly or malicious rules. An unclassified access point can be contained. It can also be moved to the Friendly or Malicious classification type automatically in accordance with user-defined rules or manually by the user.

### Step 4
If you want to change the classification of this device, choose a different classification from the Class Type drop-down list.

Note A rogue access point cannot be moved to another class if its current state is Contain.

### Step 5
From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this rogue access point:

- **Internal**—The controller trusts this rogue access point. This option is available if the Class Type is set to Friendly.
- **External**—The controller acknowledges the presence of this rogue access point. This option is available if the Class Type is set to Friendly.
- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients. This option is available if the Class Type is set to Malicious or Unclassified.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action. This option is available if the Class Type is set to Malicious or Unclassified.

The bottom of the page provides information on both the access points that detected this rogue access point and any clients that are associated to it. To see more details for any of the clients, click Edit to open the Rogue Client Detail page.

### Step 6
Click Apply to commit your changes.

### Step 7
Click Save Configuration to save your changes.
Step 8 View any rogue clients that are connected to the controller by choosing **Rogue Clients**. The Rogue Clients page appears. This page shows the following information: the MAC address of the rogue client, the MAC address of the access point to which the rogue client is associated, the SSID of the rogue client, the number of radios that detected the rogue client, the date and time when the rogue client was last reported, and the current status of the rogue client.

Step 9 Obtain more details about a rogue client by clicking the MAC address of the client. The Rogue Client Detail page appears.

This page provides the following information: the MAC address of the rogue client, the MAC address of the rogue access point to which this client is associated, the SSID and IP address of the rogue client, the dates and times when the rogue client was first and last reported, and the current status of the rogue client.

Step 10 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this rogue client:

- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action.

The bottom of the page provides information on the access points that detected this rogue client.

Step 11 Click **Apply** to commit your changes.

Step 12 If desired, you can test the controller’s connection to this client by clicking **Ping**.

Step 13 Click **Save Configuration** to save your changes.

Step 14 See any ad-hoc rogues detected by the controller by choosing **Adhoc Rogues**. The Adhoc Rogues page appears.

This page shows the following information: the MAC address, BSSID, and SSID of the ad-hoc rogue, the number of radios that detected the ad-hoc rogue, and the current status of the ad-hoc rogue.

Step 15 Obtain more details about an ad-hoc rogue by clicking the MAC address of the rogue. The Adhoc Rogue Detail page appears.

This page provides the following information: the MAC address and BSSID of the ad-hoc rogue, the dates and times when the rogue was first and last reported, and the current status of the rogue.

Step 16 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this ad-hoc rogue:

- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action.
- **Internal**—The controller trusts this rogue access point.
- **External**—The controller acknowledges the presence of this rogue access point.

Step 17 From the Maximum Number of APs to Contain the Rogue drop-down list, choose one of the following options to specify the maximum number of access points used to contain this ad-hoc rogue: 1, 2, 3, or 4. The bottom of the page provides information on the access points that detected this ad-hoc rogue.

Step 18 Click **Apply** to commit your changes.

Step 19 Click **Save Configuration** to save your changes.

Step 20 View any access points that have been configured to be ignored by choosing **Rogue AP Ignore-List**. The Rogue AP Ignore-List page appears.
Chapter 7  Configuring Security Solutions

Classifying Rogue Access Points

This page shows the MAC addresses of any access points that are configured to be ignored. The rogue-ignore list contains a list of any autonomous access points that have been manually added to WCS maps by WCS users. The controller regards these autonomous access points as rogues even though WCS is managing them. The rogue-ignore list allows the controller to ignore these access points. The list is updated as follows:

• When the controller receives a rogue report, it checks to see if the unknown access point is in the rogue-ignore access point list.
• If the unknown access point is in the rogue-ignore list, the controller ignores this access point and continues to process other rogue access points.
• If the unknown access point is not in the rogue-ignore list, the controller sends a trap to WCS. If WCS finds this access point in its autonomous access point list, WCS sends a command to the controller to add this access point to the rogue-ignore list. This access point is then ignored in future rogue reports.
• If a user removes an autonomous access point from WCS, WCS sends a command to the controller to remove this access point from the rogue-ignore list.

---

Configuring Rogue Classification Rules (CLI)

Step 1  Create a rule by entering this command:

```
config rogue rule add ap priority priority classify {friendly | malicious} rule_name
```

*Note* If you later want to change the priority of this rule and shift others in the list accordingly, enter the `config rogue rule priority priority rule_name` command. If you later want to change the classification of this rule, enter the `config rogue rule classify {friendly | malicious} rule_name` command.

*Note* If you ever want to delete all of the rogue classification rules or a specific rule, enter the `config rogue rule delete {all | rule_name}` command.

Step 2  Disable all rules or a specific rule by entering this command:

```
config rogue rule disable {all | rule_name}
```

*Note* A rule must be disabled before you can modify its attributes.

Step 3  Add conditions to a rule that the rogue access point must meet by entering this command:

```
config rogue rule condition ap set condition_type condition_value rule_name
```

where `condition_type` is one of the following:

• `ssid`—Requires that the rogue access point have a specific SSID. You should add SSIDs that are not managed by the controller. If you choose this option, enter the SSID for the `condition_value parameter`. The SSID is added to the user-configured SSID list.
Chapter 7  Configuring Security Solutions

Classifying Rogue Access Points

Note If you ever want to delete all of the SSIDs or a specific SSID from the user-configured SSID list, enter the `config rogue rule condition ap delete ssid {all | ssid} rule_name` command.

- **rssi**—Requires that the rogue access point have a minimum RSSI value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value for the `condition_value parameter`. The valid range is –95 to –50 dBm (inclusive), and the default value is 0 dBm.

- **duration**—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period for the `condition_value parameter`. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.

- **client-count**—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point for the `condition_value parameter`. The valid range is 1 to 10 (inclusive), and the default value is 0.

- **no-encryption**—Requires that the rogue access point’s advertised WLAN does not have encryption enabled. A `condition_value parameter` is not required for this option.

- **managed-ssid**—Requires that the rogue access point’s SSID be known to the controller. A `condition_value parameter` is not required for this option.

Note You can add up to six conditions per rule. If you ever want to delete all of the conditions or a specific condition from a rule, enter the `config rogue rule condition ap delete {all | condition_type} condition_value rule_name` command.

**Step 4** Specify whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule by entering this command:

`config rogue rule match {all | any} rule_name`

**Step 5** Enable all rules or a specific rule by entering this command:

`config rogue rule enable {all | rule_name}`

Note For your changes to become effective, you must enable the rule.

**Step 6** Add a new friendly access point entry to the friendly MAC address list or delete an existing friendly access point entry from the list by entering this command:

`config rogue ap friendly {add | delete} ap_mac_address`

**Step 7** Save your changes by entering this command:

`save config`

**Step 8** View the rogue classification rules that are configured on the controller by entering this command:

`show rogue rule summary`

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Rule Name</th>
<th>State</th>
<th>Type</th>
<th>Match</th>
<th>Hit Count</th>
</tr>
</thead>
</table>
Classifying Rogue Access Points

1 Rule1 Disabled Friendly Any 0
2 Rule2 Enabled Malicious Any 339
3 Rule3 Disabled Friendly Any 0

Step 9  View detailed information for a specific rogue classification rule by entering this command:

show rogue rule detailed rule_name

Information similar to the following appears:

Priority............................................ 2
Rule Name........................................ Rule2
State............................................ Enabled
Type............................................. Malicious
Match Operation.................................. Any
Hit Count......................................... 352
Total Conditions................................. 6
Condition 1
  type............................................ Client-count
  value......................................... 10
Condition 2
  type............................................ Duration
  value (seconds)......................... 2000
Condition 3
  type............................................ Managed-ssid
  value......................................... Enabled
Condition 4
  type............................................ No-encryption
  value......................................... Enabled
Condition 5
  type............................................ Rssi
  value (dBm).......................... -50
Condition 6
  type............................................ Ssid
  SSID Count................................ 1
  SSID 1.............................. test

Viewing and Classify Rogue Devices (CLI)

- View a list of all rogue access points detected by the controller by entering this command:

  show rogue ap summary

  Information similar to the following appears:

  Rogue Location Discovery Protocol............ Enabled
  Rogue AP timeout............................. 1200

  MAC Address        Classification     # APs # Clients Last Heard
  -----------------  ------------------ ----- --------- -----------------------
  00:0a:b8:7f:08:c0  Friendly           0     0         Not Heard
  00:0b:85:01:30:3f  Malicious          1     0         Fri Nov 30 11:30:59 2007
  00:0b:85:63:70:6f  Malicious          1     0         Fri Nov 30 11:20:14 2007
  ...

- See a list of the friendly rogue access points detected by the controller by entering this command:

  show rogue ap friendly summary

  Information similar to the following appears:
Chapter 7      Configuring Security Solutions

Classifying Rogue Access Points

Number of APs.................................... 1

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>State</th>
<th># APs</th>
<th># Clients</th>
<th>Last Heard</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0a:b8:7f:08:c0</td>
<td>Internal</td>
<td>1</td>
<td>0</td>
<td>Tue Nov 27 13:52:04 2007</td>
</tr>
</tbody>
</table>

- See a list of the malicious rogue access points detected by the controller by entering this command:

  `show rogue ap malicious summary`

  Information similar to the following appears:

  Number of APs.................................... 264

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>State</th>
<th># APs</th>
<th># Clients</th>
<th>Last Heard</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:85:01:30:3f</td>
<td>Alert</td>
<td>1</td>
<td>0</td>
<td>Fri Nov 30 11:20:01 2007</td>
</tr>
<tr>
<td>00:0b:85:63:70:6f</td>
<td>Alert</td>
<td>1</td>
<td>0</td>
<td>Fri Nov 30 11:20:14 2007</td>
</tr>
<tr>
<td>00:0b:85:63:cd:dd</td>
<td>Alert</td>
<td>1</td>
<td>0</td>
<td>Fri Nov 30 11:27:03 2007</td>
</tr>
<tr>
<td>00:0b:85:63:cd:de</td>
<td>Alert</td>
<td>1</td>
<td>0</td>
<td>Fri Nov 30 11:26:23 2007</td>
</tr>
<tr>
<td>00:0b:85:63:cd:df</td>
<td>Alert</td>
<td>1</td>
<td>0</td>
<td>Fri Nov 30 11:26:50 2007</td>
</tr>
</tbody>
</table>
  ...

- See a list of the unclassified rogue access points detected by the controller by entering this command:

  `show rogue ap unclassified summary`

  Information similar to the following appears:

  Number of APs.................................... 164

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>State</th>
<th># APs</th>
<th># Clients</th>
<th>Last Heard</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:85:63:cd:bd</td>
<td>Alert</td>
<td>1</td>
<td>0</td>
<td>Fri Nov 30 11:12:52 2007</td>
</tr>
<tr>
<td>00:0b:85:63:cd:e7</td>
<td>Alert</td>
<td>1</td>
<td>0</td>
<td>Fri Nov 30 11:29:01 2007</td>
</tr>
<tr>
<td>00:0b:85:63:ce:05</td>
<td>Alert</td>
<td>1</td>
<td>0</td>
<td>Fri Nov 30 11:26:23 2007</td>
</tr>
<tr>
<td>00:0b:85:63:ce:07</td>
<td>Alert</td>
<td>1</td>
<td>0</td>
<td>Fri Nov 30 11:26:23 2007</td>
</tr>
</tbody>
</table>
  ...

- See detailed information for a specific rogue access point by entering this command:

  `show rogue ap detailed ap_mac_address`

  Information similar to the following appears:

  Rogue BSSID...................................... 00:1d:70:59:95:9d
  Rogue Radio Type................................ 802.11a
  State............................................ Alert
  First Time Rogue was Reported.................... Tue Sep 21 09:57:08 2010
  Last Time Rogue was Reported..................... Tue Sep 21 10:00:56 2010
  Rogue Client IP address.......................... Not known
  Reported By AP 1
  MAC Address.................................... 68:ef:bd:e1:fd:30
  Name.......................................... AP5475.d074.48e4
  RSSI........................................... -80 dBm
  SNR............................................ 18 dB
  Channel........................................ 40
  Last reported by this AP......................... Tue Sep 21 10:00:56 2010

- See the rogue report (which shows the number of rogue devices detected on different channel widths) for a specific 802.11a/n radio by entering this command:
show ap auto-rf 802.11a Cisco_AP

Information similar to the following appears:

Number Of Slots.................................. 2
AP Name.......................................... AP2
MAC Address....................................... 00:1b:d5:13:39:74
Radio Type..................................... RADIO_TYPE_80211a

Noise Information
Noise Profile.................................. PASSED
Channel 36...................................  -80 dBm
Channel 40...................................  -78 dBm

Interference Information
Interference Profile.......................... PASSED
Channel 36...................................  -81 dBm @ 8 % busy
Channel 40...................................  -66 dBm @ 4 % busy

Rogue Histogram (20/40_ABOVE/40_BELOW)
Channel 36................................... 21/ 1/ 0
Channel 40...................................  7/ 0/ 0

• See a list of all rogue clients that are associated to a rogue access point by entering this command:

  show rogue ap clients ap_mac_address

Information similar to the following appears:

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>State</th>
<th># APs</th>
<th>Last Heard</th>
</tr>
</thead>
</table>

• See a list of all rogue clients detected by the controller by entering this command:

  show rogue client summary

Information similar to the following appears:

Validate rogue clients against AAA............ Disabled

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>State</th>
<th># APs</th>
<th>Last Heard</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0a:8a:7d:f5:f5</td>
<td>Alert</td>
<td>1</td>
<td>Mon Dec 3 21:56:36 2007</td>
</tr>
<tr>
<td>00:18:ba:78:c4:44</td>
<td>Alert</td>
<td>1</td>
<td>Mon Dec 3 21:59:36 2007</td>
</tr>
<tr>
<td>00:18:ba:78:c4:d1</td>
<td>Alert</td>
<td>1</td>
<td>Mon Dec 3 21:47:36 2007</td>
</tr>
<tr>
<td>00:18:ba:78:ca:f8</td>
<td>Alert</td>
<td>1</td>
<td>Mon Dec 3 22:02:36 2007</td>
</tr>
</tbody>
</table>

• See detailed information for a specific rogue client by entering this command:

  show rogue client detailed client_mac_address

Information similar to the following appears:

Rogue BSSID...................................... 00:0b:85:23:ea:d1
State............................................ Alert
First Time Rogue was Reported.................... Mon Dec 3 21:50:36 2007
Last Time Rogue was Reported....................... Mon Dec 3 21:50:36 2007
Rogue Client IP address.......................... Not known
Reported By
  AP 1
  MAC Address.................................... 00:15:c7:82:6b:06
  Name.......................................... AP0016.47b2.31ea
  Radio Type.................................. 802.11a
  RSSI......................................... -71 dBm
  SNR......................................... 23 dB
Chapter 7  Configuring Security Solutions

Classifying Rogue Access Points

- See a list of all ad-hoc rogues detected by the controller by entering this command:
  
  **show rogue adhoc summary**

  Information similar to the following appears:

  Detect and report Ad-Hoc Networks: Enabled

<table>
<thead>
<tr>
<th>Client MAC Address</th>
<th>Adhoc BSSID</th>
<th>State</th>
<th># APs</th>
<th>Last Heard</th>
</tr>
</thead>
</table>

- See detailed information for a specific ad-hoc rogue by entering this command:
  
  **show rogue adhoc detailed rogue_mac_address**

  Information similar to the following appears:

  Adhoc Rogue MAC address: 02:61:ce:8e:a8:8c
  Adhoc Rogue BSSID: 02:61:ce:8e:a8:8c
  State: Alert
  First Time Adhoc Rogue was Reported: Tue Dec 11 20:45:45 2007
  Last Time Adhoc Rogue was Reported: Tue Dec 11 20:45:45 2007
  Reported By AP 1
  MAC Address: 00:14:1b:58:4a:e0
  Name: AP0014.1ced.2a60
  Radio Type: 802.11b
  SSID: rf4k3ap
  Channel: 3
  RSSI: -56 dBm
  SNR: 15 dB
  Encryption: Disabled
  ShortPreamble: Disabled
  WPA Support: Disabled
  Last reported by this AP: Tue Dec 11 20:45:45 2007

- See a list of rogue access points that are configured to be ignore by entering this command:
  
  **show rogue ignore-list**

  Information similar to the following appears:

  MAC Address
  10:bb:17:cc:01:ef

  **Note**
  See Step 20 of the “Viewing and Classifying Rogue Devices (GUI)” section on page 7-93 for more information on the rogue-ignore access point list.

- Classify a rogue access point as friendly by entering this command:
  
  **config rogue ap classify friendly state {internal | external} ap_mac_address**

  where

  - **internal** means that the controller trusts this rogue access point.
  - **external** means that the controller acknowledges the presence of this rogue access point.

  **Note**
  A rogue access point cannot be moved to the Friendly class if its current state is Contain.
• Mark a rogue access point as malicious by entering this command:

```
config rogue ap classify malicious state {alert | contain} ap_mac_address
```

where

- **alert** means that the controller forwards an immediate alert to the system administrator for further action.
- **contain** means that the controller contains the offending device so that its signals no longer interfere with authorized clients.

>Note: A rogue access point cannot be moved to the Malicious class if its current state is Contain.

• Mark a rogue access point as unclassified by entering this command:

```
config rogue ap classify unclassified state {alert | contain} ap_mac_address
```

>Note: A rogue access point cannot be moved to the Unclassified class if its current state is Contain.

• Specify how the controller should respond to a rogue client by entering one of these commands:

```
config rogue client alert client_mac_address—The controller forwards an immediate alert to the system administrator for further action.
```

```
config rogue client contain client_mac_address—The controller contains the offending device so that its signals no longer interfere with authorized clients.
```

• Specify how the controller should respond to an ad-hoc rogue by entering one these commands:

```
config rogue adhoc alert rogue_mac_address—The controller forwards an immediate alert to the system administrator for further action.
```

```
config rogue adhoc contain rogue_mac_address—The controller contains the offending device so that its signals no longer interfere with authorized clients.
```

```
config rogue adhoc external rogue_mac_address—The controller acknowledges the presence of this ad-hoc rogue.
```

• Save your changes by entering this command:

```
save config
```

---

**Configuring Cisco TrustSec SXP**

This section contains the following topics:

- Information About Cisco TrustSec SXP, page 7-103
- Guidelines and Limitations, page 7-103
- Configuring Cisco TrustSec SXP (GUI), page 7-104
Information About Cisco TrustSec SXP

Cisco TrustSec (CTS) 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. CTS 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 CTS architecture establishes 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 checks, and data-path replay protection mechanisms. CTS 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 CTS 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.

One of the components of the CTS architecture is the security group-based access control. 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 the CTS 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) that joins 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. 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 Layer 3 interface on the distribution switch.

For more information about CTS, see http://www.cisco.com/en/US/netsol/ns1051/index.html.

Guidelines and Limitations

- 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 controller always operates in the Speaker mode.
• 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.
• SXP is supported for both IPv4 and IPv6 clients.
• Static IP-SGT mapping for local authentication of users is not supported.
• IP-SGT mapping requires authentication with external ACS servers.
• SXP 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

### Configuring Cisco TrustSec SXP (GUI)

#### Step 1
Choose SECURITY > TrustSec SXP to open the SXP Configuration page.

This page lists the following SXP configuration details:
• Total SXP Connections—Number of SXP connections that are configured.
• SXP State—Status of SXP connections as either disabled or enabled.
• SXP Mode—SXP mode of the controller. The controller is always set to Speaker mode for SXP connections.
• Default Password—Password for MD5 authentication of SXP messages. We recommend that the password has a minimum of 6 characters.
• Default Source IP—IP address of the management interface. SXP uses the default source IP address for all new TCP connections.
Chapter 7  Configuring Security Solutions

Configuring Cisco TrustSec SXP

- Retry Period—SXP retry timer. The default value is 120 seconds (2 minutes). The valid range is 0 to 64000 seconds. The SXP retry period determines how often the controller retries for an SXP connection. When an SXP connection is not successfully set up, the controller makes a new attempt to set up the connection after the SXP retry period timer expires. Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

This page also displays the following information about SXP connections:
- Peer IP Address—The IP address of the next hop switch to which the controller is connected. There is no effect on the existing TCP connections when you configure a new peer connection.
- Source IP Address—The management IP address of the controller.
- Connection Status—Status of the SXP connection.

**Step 2**
To enable CTS SXP, from the SXP State drop-down list, choose **Enabled**.

**Step 3**
Enter the default password that should be used to make an SXP connection. We recommend that the password contain a minimum of 6 characters.

**Step 4**
In the Retry Period text box, enter the time in seconds that determines how often the Cisco TrustSec software retries for an SXP connection.

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

Creating a New SXP Connection (GUI)

**Step 1**
Choose **SECURITY > TrustSec SXP** and click **New** to open the SXP Connection > New page.

**Step 2**
In the Peer IP Address text box, enter the IP address of the next hop switch to which the controller is connected.

**Step 3**
Click **Apply**.

Configuring Cisco TrustSec SXP (CLI)

- To enable or disable the SXP on the controller, enter this command:
  ```
  config cts sxp {enable | disable}
  ```
- To configure the default password for MD5 Authentication of SXP messages, enter this command:
  ```
  config cts sxp default password password
  ```
- To configure the SXP retry period, enter the following command:
  ```
  config cts sxp retry period time-in-seconds
  ```
- To configure the IP address of the next hop switch with which the controller is connected, enter the command:
  ```
  config cts sxp connection peer ip-address
  ```
- To remove an SXP connection, enter this command:
  ```
  config cts sxp connection delete ip-address
  ```
- To see a summary of SXP configuration, enter this command:
show cts sxp summary

Information similar to the following appears:

- SXP State........................................ Enable
- SXP Mode......................................... Speaker
- Default Password................................. ****
- Default Source IP................................ 209.165.200.224
- Connection retry open period ................. 120

- To see the list of SXP connections that are configured, enter the following command:

show cts sxp connections

Information similar to the following appears:

- Total num of SXP Connections..................... 1
- SXP State........................................ Enable
- Peer IP            Source IP           Connection Status
- ---------------    ---------------     -----------------
- 209.165.200.229  209.165.200.224  On

Configuring Cisco Intrusion Detection System

This section contains the following topics:

- Information About Cisco Intrusion Detection System, page 7-106
- Additional Information, page 7-107
- Configuring IDS Sensors (GUI), page 7-107
- Configuring IDS Sensors (CLI), page 7-108
- Viewing Shunned Clients (CLI), page 7-110

Information About Cisco Intrusion Detection System

The Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/CIPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected at Layer 3 through Layer 7. This system offers significant network protection by helping to detect, classify, and stop threats including worms, spyware/adware, network viruses, and application abuse. Two methods are available to detect potential attacks:

- IDS sensors
- IDS signatures

You can configure IDS sensors to detect various types of IP-level attacks in your network. When the sensors identify an attack, they can alert the controller to shun the offending client. When you add a new IDS sensor, you register the controller with that IDS sensor so that the controller can query the sensor to get the list of shunned clients.

When an IDS sensor detects a suspicious client, it alerts the controller to shun this client. The shun entry is distributed to all controllers within the same mobility group. If the client to be shunned is currently joined to a controller in this mobility group, the anchor controller adds this client to the dynamic exclusion list, and the foreign controller removes the client. The next time that the client tries to connect to a controller, the anchor controller rejects the handoff and informs the foreign controller that the client is being excluded.
Additional Information

The Cisco wireless intrusion prevention system (wIPS) is also supported on the controller through WCS. See the “Configuring wIPS” section on page 7-121 for more information.

See Chapter 15, “Configuring Mobility Groups,” for more information on mobility groups.

Configuring IDS Sensors (GUI)

Step 1  Choose Security > Advanced > CIDs > Sensors to open the CIDS Sensors List page.

This page lists all of the IDS sensors that have been configured for this controller.

Note  If you want to delete an existing sensor, hover your cursor over the blue drop-down arrow for that sensor and choose Remove.

Step 2  Add an IDS sensor to the list by clicking New. The CIDS Sensor Add page appears.

Step 3  The controller supports up to five IDS sensors. From the Index drop-down list, choose a number (between 1 and 5) to determine the sequence in which the controller consults the IDS sensors. For example, if you choose 1, the controller consults this IDS sensor first.

Step 4  In the Server Address text box, enter the IP address of your IDS server.

Step 5  The Port text box contains the number of the HTTPS port through which the controller is to communicate with the IDS sensor. We recommend that you set this parameter to 443 because the sensor uses this value to communicate by default.

The default value is 443 and the range is 1 to 65535.

Step 6  In the Username text box, enter the name that the controller uses to authenticate to the IDS sensor.

Note  This username must be configured on the IDS sensor and have at least a read-only privilege.

Step 7  In the Password and Confirm Password text boxes, enter the password that the controller uses to authenticate to the IDS sensor.

Step 8  In the Query Interval text box, enter the time (in seconds) for how often the controller should query the IDS server for IDS events.

The default is 60 seconds and the range is 10 to 3600 seconds.
Step 9 Select the **State** check box to register the controller with this IDS sensor or unselected this check box to disable registration. The default value is disabled.

Step 10 In the Fingerprint text box, enter a 40-hexadecimal-character security key. This key is used to verify the validity of the sensor and is used to prevent security attacks.

**Note** Make sure you include colons that appear between every two bytes within the key. For example, enter AA:BB:CC:DD.

Step 11 Click **Apply**. Your new IDS sensor appears in the list of sensors on the CIDS Sensors List page.

Step 12 Click **Save Configuration** to save your changes.

### Viewing Shunned Clients (GUI)

**Step 1** Choose **Security > Advanced > CIDS > Shunned Clients** to open the CIDS Shun List page.

**Figure 7-26 CIDS Shun List Page**

This page shows the IP address and MAC address of each shunned client, the length of time that the client’s data packets should be blocked by the controller as requested by the IDS sensor, and the IP address of the IDS sensor that discovered the client.

**Step 2** Click **Re-sync** to purge and reset the list as desired.

### Configuring IDS Sensors (CLI)

**Step 1** Add an IDS sensor by entering this command:

```
config wps cids-sensor add index ids_ip_address username password
```

The **index** parameter determines the sequence in which the controller consults the IDS sensors. The controller supports up to five IDS sensors. Enter a number (between 1 and 5) to determine the priority of this sensor. For example, if you enter 1, the controller consults this IDS sensor first.
Chapter 7 Configuring Security Solutions

Configuring Cisco Intrusion Detection System

Note: The username must be configured on the IDS sensor and have at least a read-only privilege.

Step 2 (Optional) Specify the number of the HTTPS port through which the controller is to communicate with the IDS sensor by entering this command:

```
config wps cids-sensor port index port_number
```

For the `port-number` parameter, you can enter a value between 1 and 65535. The default value is 443. This step is optional because we recommend that you use the default value of 443. The sensor uses this value to communicate by default.

Step 3 Specify how often the controller should query the IDS server for IDS events by entering this command:

```
config wps cids-sensor interval index interval
```

For the `interval` parameter, you can enter a value between 10 and 3600 seconds. The default value is 60 seconds.

Step 4 Enter a 40-hexadecimal-character security key used to verify the validity of the sensor by entering this command:

```
config wps cids-sensor fingerprint index sha1 fingerprint
```

You can get the value of the fingerprint by entering `show tls fingerprint` on the sensor’s console.

Note: Make sure to include the colons that appear between every two bytes within the key (for example, AA:BB:CC:DD).

Step 5 Enable or disable this controller’s registration with an IDS sensor by entering this command:

```
config wps cids-sensor {enable | disable} index
```

Step 6 Enable or disable protection from DoS attacks by entering this command:

```
config wps auto-immune {enable | disable}
```

The default value is disabled.

Note: A potential attacker can use specially crafted packets to mislead the IDS into treating a legitimate client as an attacker. It causes the controller to wrongly disconnect this legitimate client and launches a DoS attack. The auto-immune feature, when enabled, is designed to protect against such attacks. However, conversations using Cisco 792x phones might be interrupted intermittently when the auto-immune feature is enabled. If you experience frequent disruptions when using 792x phones, you might want to disable this feature.

Step 7 Save your settings by entering this command:

```
save config
```

Step 8 See the IDS sensor configuration by entering one of these commands:

- `show wps cids-sensor summary`
- `show wps cids-sensor detail index`

The second command provides more information than the first.

Step 9 See the auto-immune configuration setting by entering this command:

```
show wps summary
```

Cisco Wireless LAN Controller Configuration Guide
OL-21524-03

7-109
Information similar to the following appears:

Auto-Immune
Auto-Immune................................. Disabled

Client Exclusion Policy
Excessive 802.11-association failures......... Enabled
Excessive 802.11-authentication failures....... Enabled
Excessive 802.1x-authentication................ Enabled
IP-theft..................................... Enabled
Excessive Web authentication failure.......... Enabled
Signature Policy
Signature Processing........................... Enabled

Step 10 Obtain debug information regarding IDS sensor configuration by entering this command:

dump wps cids enable

Note If you ever want to delete or change the configuration of a sensor, you must first disable it by entering the config wps cids-sensor disable index command. To delete the sensor, enter the config wps cids-sensor delete index command.

Viewing Shunned Clients (CLI)

Step 1 View the list of clients to be shunned by entering this command:

show wps shun-list

Step 2 Force the controller to synchronize with other controllers in the mobility group for the shun list by entering this command:

config wps shun-list re-sync

Configuring IDS Signatures

This section contains the following topics:

- Information About IDS Signatures, page 7-111
- Configuring IDS Signatures (GUI), page 7-113
- Viewing IDS Signature Events (GUI), page 7-116
- Configure IDS Signatures (CLI), page 7-118
- Viewing IDS Signature Events (CLI), page 7-119
Information About IDS Signatures

You can configure IDS signatures, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, appropriate mitigation is initiated.

Cisco supports 17 standard signatures on the controller as shown on the Standard Signatures page.

These signatures are divided into six main groups. The first four groups contain management signatures, and the last two groups contain data signatures.

- **Broadcast deauthentication frame signatures**—During a broadcast deauthentication frame attack, a hacker sends an 802.11 deauthentication frame to the broadcast MAC destination address of another client. This attack causes the destination client to disassociate from the access point and lose its connection. If this action is repeated, the client experiences a denial of service. When the broadcast deauthentication frame signature (precedence 1) is used to detect such an attack, the access point listens for clients transmitting broadcast deauthentication frames that match the characteristics of the signature. If the access point detects such an attack, it alerts the controller. Depending on how your system is configured, the offending device is contained so that its signals no longer interfere with authorized clients, or the controller forwards an immediate alert to the system administrator for further action, or both.
• NULL probe response signatures—During a NULL probe response attack, a hacker sends a NULL probe response to a wireless client adapter. As a result, the client adapter locks up. When a NULL probe response signature is used to detect such an attack, the access point identifies the wireless client and alerts the controller. The NULL probe response signatures are as follows:
  - NULL probe resp 1 (precedence 2)
  - NULL probe resp 2 (precedence 3)

• Management frame flood signatures—During a management frame flood attack, a hacker floods an access point with 802.11 management frames. The result is a denial of service to all clients associated or attempting to associate to the access point. This attack can be implemented with different types of management frames: association requests, authentication requests, reassociation requests, probe requests, disassociation requests, deauthentication requests, and reserved management subtypes.

  When a management frame flood signature is used to detect such an attack, the access point identifies management frames matching the entire characteristic of the signature. If the frequency of these frames is greater than the value of the frequency set in the signature, an access point that hears these frames triggers an alarm. The controller generates a trap and forwards it to WCS.

  The management frame flood signatures are as follows:
  - Assoc flood (precedence 4)
  - Auth flood (precedence 5)
  - Reassoc flood (precedence 6)
  - Broadcast probe flood (precedence 7)
  - Disassoc flood (precedence 8)
  - Deauth flood (precedence 9)
  - Reserved mgmt 7 (precedence 10)
  - Reserved mgmt F (precedence 11)

  The reserved management frame signatures 7 and F are reserved for future use.

• Wellenreiter signature—Wellenreiter is a wireless LAN scanning and discovery utility that can reveal access point and client information. When the Wellenreiter signature (precedence 17) is used to detect such an attack, the access point identifies the offending device and alerts the controller.

• EAPOL flood signature—During an EAPOL flood attack, a hacker floods the air with EAPOL frames that contain 802.1X authentication requests. As a result, the 802.1X authentication server cannot respond to all of the requests and fails to send successful authentication responses to valid clients. The result is a denial of service to all affected clients. When the EAPOL flood signature (precedence 12) is used to detect such an attack, the access point waits until the maximum number of allowed EAPOL packets is exceeded. It then alerts the controller and proceeds with the appropriate mitigation.

• NetStumbler signatures—NetStumbler is a wireless LAN scanning utility that reports access point broadcast information (such as operating channel, RSSI information, adapter manufacturer name, SSID, WEP status, and the latitude and longitude of the device running NetStumbler when a GPS is attached). If NetStumbler succeeds in authenticating and associating to an access point, it sends a data frame with the following strings, depending on the NetStumbler version:

<table>
<thead>
<tr>
<th>Version</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.0</td>
<td>“Flurble gronk bloopit, bnip Frundletrune”</td>
</tr>
</tbody>
</table>
Chapter 7  Configuring Security Solutions

Configuring IDS Signatures

When a NetStumbler signature is used to detect such an attack, the access point identifies the offending device and alerts the controller. The NetStumbler signatures are as follows:

- NetStumbler 3.2.0 (precedence 13)
- NetStumbler 3.2.3 (precedence 14)
- NetStumbler 3.3.0 (precedence 15)
- NetStumbler generic (precedence 16)

A standard signature file exists on the controller by default. You can upload this signature file from the controller, or you can create a custom signature file and download it to the controller or modify the standard signature file to create a custom signature.

Configuring IDS Signatures (GUI)

This section contains the following topics:

- Uploading or Downloading IDS Signatures, page 7-113
- Enabling or Disabling IDS Signatures, page 7-115

Uploading or Downloading IDS Signatures

<table>
<thead>
<tr>
<th>Version</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.3</td>
<td>“All your 802.11b are belong to us”</td>
</tr>
<tr>
<td>3.3.0</td>
<td>Sends white spaces</td>
</tr>
</tbody>
</table>

When a NetStumbler signature is used to detect such an attack, the access point identifies the offending device and alerts the controller. The NetStumbler signatures are as follows:

<table>
<thead>
<tr>
<th>Version</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.3</td>
<td>“All your 802.11b are belong to us”</td>
</tr>
<tr>
<td>3.3.0</td>
<td>Sends white spaces</td>
</tr>
</tbody>
</table>

Step 1 If desired, create your own custom signature file.

Step 2 Make sure that you have a Trivial File Transfer Protocol (TFTP) server available. Follow these guidelines when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the Cisco WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.

Step 3 If you are downloading a custom signature file (*.sig), copy it to the default directory on your TFTP server.

Step 4 Choose Commands to open the Download File to Controller page.
Step 5 Perform one of the following:
- If you want to download a custom signature file to the controller, choose **Signature File** from the File Type drop-down list on the Download File to Controller page.
- If you want to upload a standard signature file from the controller, choose **Upload File** and then **Signature File** from the File Type drop-down list on the Upload File from Controller page.

Step 6 From the Transfer Mode drop-down list, choose **TFTP** or **FTP**.

Step 7 In the IP Address text box, enter the IP address of the TFTP or FTP server.

Step 8 If you are downloading the signature file using a TFTP server, enter the maximum number of times that the controller should attempt to download the signature file in the Maximum retries text box.

The range is 1 to 254 and the default value is 10.

Step 9 If you are downloading the signature file using a TFTP server, enter the amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout text box.

The range is 1 to 254 seconds and the default is 6 seconds.

Step 10 In the File Path text box, enter the path of the signature file to be downloaded or uploaded. The default value is “/.”

Step 11 In the File Name text box, enter the name of the signature file to be downloaded or uploaded.

**Note** When uploading signatures, the controller uses the filename that you specify as a base name and then adds “_std.sig” and “_custom.sig” to it in order to upload both standard and custom signature files to the TFTP server. For example, if you upload a signature file called “ids1,” the controller automatically generates and uploads both ids1_std.sig and ids1_custom.sig to the TFTP server. If desired, you can then modify ids1_custom.sig on the TFTP server (making sure to set “Revision = custom”) and download it by itself.

Step 12 If you are using an FTP server, follow these steps:
- a. In the Server Login Username text box, enter the username to log into the FTP server.
- b. In the Server Login Password text box, enter the password to log into the FTP server.
- c. In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 13 Choose **Download** to download the signature file to the controller or **Upload** to upload the signature file from the controller.
Enabling or Disabling IDS Signatures

Step 1  Choose Security > Wireless Protection Policies > Standard Signatures or Custom Signatures to open the Standard Signatures page or the Custom Signatures page.

The Standard Signatures page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. This page shows the following information for each signature:

- The order, or precedence, in which the controller performs the signature checks.
- The name of the signature, which specifies the type of attack that the signature is trying to detect.
- The frame type on which the signature is looking for a security attack. The possible frame types are data and management.
- The action that the controller is directed to take when the signature detects an attack. The possible actions are None and Report.
- The state of the signature, which indicates whether the signature is enabled to detect security attacks.
- A description of the type of attack that the signature is trying to detect.

Step 2  Perform one of the following:

- If you want to allow all signatures (both standard and custom) whose individual states are set to Enabled to remain enabled, select the Enable Check for All Standard and Custom Signatures check box at the top of either the Standard Signatures page or the Custom Signatures page.
default value is enabled (or selected). When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.

- If you want to disable all signatures (both standard and custom) on the controller, unselect the Enable Check for All Standard and Custom Signatures check box. If you unselected this check box, all signatures are disabled, even the ones whose individual states are set to Enabled.

**Step 3** Click Apply to commit your changes.

**Step 4** Click the precedence number of the desired signature to enable or disable an individual signature. The Standard Signature (or Custom Signature) > Detail page appears.

This page shows much of the same information as the Standard Signatures and Custom Signatures pages but provides these additional details:

- The tracking method used by the access points to perform signature analysis and report the results to the controller. The possible values are as follows:
  - Per Signature—Signature analysis and pattern matching are tracked and reported on a per-signature and per-channel basis.
  - Per MAC—Signature analysis and pattern matching are tracked and reported separately for individual client MAC addresses on a per-channel basis.
  - Per Signature and MAC—Signature analysis and pattern matching are tracked and reported on a per-signature and per-channel basis as well as on a per-MAC-address and per-channel basis.

- The pattern that is being used to detect a security attack

**Step 5** In the Measurement Interval text box, enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds, and the default value varies per signature.

**Step 6** In the Signature Frequency text box, enter the number of matching packets per interval that must be identified at the individual access point level before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value varies per signature.

**Step 7** In the Signature MAC Frequency text box, enter the number of matching packets per interval that must be identified per client per access point before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value varies per signature.

**Step 8** In the Quiet Time text box, enter the length of time (in seconds) after which no attacks have been detected at the individual access point level and the alarm can stop. The range is 60 to 32,000 seconds, and the default value varies per signature.

**Step 9** Select the State check box to enable this signature to detect security attacks or unselect it to disable this signature. The default value is enabled (or selected).

**Step 10** Click Apply to commit your changes. The Standard Signatures or Custom Signatures page reflects the signature’s updated state.

**Step 11** Click Save Configuration to save your changes.

---

**Viewing IDS Signature Events (GUI)**

**Step 1** Choose Security > Wireless Protection Policies > Signature Events Summary to open the Signature Events Summary page.
Figure 7-30  Signature Events Summary Page

This page shows the number of attacks detected by the enabled signatures.

**Step 2**
Click the signature type link for that signature to see more information on the attacks detected by a particular signature. The Signature Events Detail page appears.

This page shows the following information:

- The MAC addresses of the clients identified as attackers
- The method used by the access point to track the attacks
- The number of matching packets per second that were identified before an attack was detected.
- The number of access points on the channel on which the attack was detected
- The day and time when the access point detected the attack

**Step 3**
Click the Detail link for that attack to see more information for a particular attack. The Signature Events Track Detail page appears.

Figure 7-31  Signature Events Track Detail Page

This page shows the following information:

- The MAC address of the access point that detected the attack
- The name of the access point that detected the attack
- The type of radio (802.11a or 802.11b/g) used by the access point to detect the attack
- The radio channel on which the attack was detected
- The day and time when the access point reported the attack
Configure IDS Signatures (CLI)

Step 1  If desired, create your own custom signature file.

Step 2  Make sure that you have a TFTP server available. See the guidelines for setting up a TFTP server in Step 2 of the “Uploading or Downloading IDS Signatures” section on page 7-113.

Step 3  Copy the custom signature file (*.sig) to the default directory on your TFTP server.

Step 4  Specify the download or upload mode by entering the transfer {download | upload} mode tftp command.

Step 5  Specify the type of file to be downloaded or uploaded by entering the transfer {download | upload} datatype signature command.

Step 6  Specify the IP address of the TFTP server by entering the transfer {download | upload} serverip tftp-server-ip-address command.

Note  Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

Step 7  Specify the download or upload path by entering the transfer {download | upload} path absolute-tftp-server-path-to-file command.

Step 8  Specify the file to be downloaded or uploaded by entering the transfer {download | upload} filename filename.sig command.

Note  When uploading signatures, the controller uses the filename you specify as a base name and then adds “.std.sig” and “.custom.sig” to it in order to upload both standard and custom signature files to the TFTP server. For example, if you upload a signature file called “ids1,” the controller automatically generates and uploads both ids1_std.sig and ids1_custom.sig to the TFTP server. If desired, you can then modify ids1_custom.sig on the TFTP server (making sure to set “Revision = custom”) and download it by itself.

Step 9  Enter the transfer {download | upload} start command and answer y to the prompt to confirm the current settings and start the download or upload.

Step 10  Specify the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval by entering this command:

```
config wps signature interval signature_id interval
```

where signature_id is a number used to uniquely identify a signature. The range is 1 to 3600 seconds, and the default value varies per signature.

Step 11  Specify the number of matching packets per interval that must be identified at the individual access point level before an attack is detected by entering this command:

```
config wps signature frequency signature_id frequency
```

The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 12  Specify the number of matching packets per interval that must be identified per client per access point before an attack is detected by entering this command:

```
config wps signature mac-frequency signature_id mac_frequency
```

The range is 1 to 32,000 packets per interval, and the default value varies per signature.
Step 13 Specify the length of time (in seconds) after which no attacks have been detected at the individual access point level and the alarm can stop by entering by entering this command:

```
cfg wps signature quiet-time signature_id quiet_time
```

The range is 60 to 32,000 seconds, and the default value varies per signature.

Step 14 Perform one of the following:

- To enable or disable an individual IDS signature, enter this command:

```
cfg wps signature {standard | custom} state signature_id {enable | disable}
```

- To enable or disable IDS signature processing, which enables or disables the processing of all IDS signatures, enter this command:

```
cfg wps signature {enable | disable}
```

**Note** If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Step 15 Save your changes by entering this command:

```
save config
```

Step 16 If desired, you can reset a specific signature or all signatures to default values. To do so, enter this command:

```
cfg wps signature reset {signature_id | all}
```

**Note** You can reset signatures to default values only through the controller CLI.

### Viewing IDS Signature Events (CLI)

- See whether IDS signature processing is enabled or disabled on the controller by entering this command:

```
show wps summary
```

Information similar to the following appears:

```
Auto-Immune
   Auto-Immune.............................. Disabled

Client Exclusion Policy
   Excessive 802.11-association failures....... Enabled
   Excessive 802.11-authentication failures..... Enabled
   Excessive 802.1x-authentication................ Enabled
   IP-theft.................................. Enabled
   Excessive Web authentication failure......... Enabled

Signature Policy
   Signature Processing........................ Enabled
```
Note: If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

- See individual summaries of all of the standard and custom signatures installed on the controller by entering this command:

```
show wps signature summary
```

Information similar to the following appears:

```
Signature-ID................................. 1
Precedence..................................... 1
Signature Name................................. Bcast deauth
Type............................................ standard
FrameType........................................ management
State............................................ enabled
Action.......................................... report
Tracking......................................... per Signature and Mac
Signature Frequency.......................... 50 pkts/interval
Signature Mac Frequency...................... 30 pkts/interval
Interval........................................ 1 sec
Quiet Time..................................... 300 sec
Description.................................... Broadcast Deauthentication Frame
Patterns:
  0 (Header):0x00c0:0x00ff
  4 (Header):0x01:0x01
```

- See the number of attacks detected by the enabled signatures by entering this command:

```
show wps signature events summary
```

Information similar to the following appears:

```
Precedence Signature Name Type # Events
---------- ------------------ ----- -----------
1 Bcast deauth Standard 2
2 NULL probe resp 1 Standard 1
```

- See more information on the attacks detected by a particular standard or custom signature by entering this command:

```
show wps signature events {standard | custom} precedence# summary
```

Information similar to the following appears:

```
Precedence..................................... 1
Signature Name................................. Bcast deauth
Type............................................ Standard
Number of active events...................... 2

Source MAC Addr Track Method Frequency No. APs Last Heard
----------------- ------------ --------- -------- ------------------------
00:01:02:03:04:01 Per Signature 4 3 Tue Dec 6 00:17:44 2005
00:01:02:03:04:01 Per Mac 6 2 Tue Dec 6 00:30:04 2005
```

- See information on attacks that are tracked by access points on a per-signature and per-channel basis by entering this command:

```
show wps signature events {standard | custom} precedence# detailed per-signature source_mac
```

- See information on attacks that are tracked by access points on an individual-client basis (by MAC address) by entering this command:

```
show wps signature events {standard | custom} precedence# detailed per-mac source_mac
```
Information similar to the following appears:

Source MAC....................................... 00:01:02:03:04:01
Precedence....................................... 1
Signature Name................................... Bcast deauth
Type............................................. Standard
Track............................................ Per Mac
Frequency........................................ 6
Reported By
   AP 1
      MAC Address.............................. 00:0b:85:01:4d:80
      Name..................................... Test_AP_1
      Radio Type............................... 802.11bg
      Channel.................................. 4
      Last reported by this AP................ Tue Dec 6 00:17:49 2005
   AP 2
      MAC Address.............................. 00:0b:85:26:91:52
      Name..................................... Test_AP_2
      Radio Type............................... 802.11bg
      Channel.................................. 6
      Last reported by this AP................ Tue Dec 6 00:30:04 2005

Configuring wIPS

This section contains the following topics:

- Information About wIPS, page 7-121
- Guidelines and Limitations, page 7-126
- Additional References, page 7-126
- Configuring wIPS on an Access Point (GUI), page 7-126
- Configuring wIPS on an Access Point (CLI), page 7-127
- Viewing wIPS Information (CLI), page 7-128

Information About wIPS

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 3300 Series 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 WCS integration into the MSE, the wIPS service can configure, monitor, and report wIPS policies and alarms.

Note

If your wIPS deployment consists of a controller, access point, and MSE, you must set all the three entities to the UTC time zone.
The Cisco Adaptive wIPS is not configured on the controller. Instead, WCS 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 just ELM AP. You can configure an access point to work in wIPS mode if the access point is in any of the following modes:

- Monitor
- Local
- FlexConnect

wIPS ELM has limited capability of detecting off-channel alarms. The access point periodically goes off-channel, and monitors the non-serving channels for a short duration, and triggers alarms if any attack is detected on the channel. But the off-channel alarm detection is best effort and it takes longer time to detect attacks and trigger alarms, which might cause the ELM AP intermittently detect an alarm and clear it because it is not visible. Access points in any of the above modes can periodically send alarms based on the policy profile to the wIPS service through the controller. The wIPS service stores and processes the alarms and generates SNMP traps. WCS configures its IP address as a trap destination to receive SNMP traps from the MSE.

Table 7-11 lists all the SNMP trap controls and their respective traps. When a trap control is enabled, all the traps of the trap control are also enabled.

<table>
<thead>
<tr>
<th>Tab Name</th>
<th>Trap Control</th>
<th>Trap</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Link (Port) Up/Down</td>
<td>linkUp, linkDown</td>
</tr>
<tr>
<td></td>
<td>Spanning Tree</td>
<td>newRoot, topologyChange,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>stpInstanceNewRootTrap,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>stpInstanceTopologyChangeTrap</td>
</tr>
<tr>
<td></td>
<td>Config Save</td>
<td>bsnDot11EssCreated,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bsnDot11EssDeleted,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bsnConfigSaved,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ciscoLwappScheduledResetNotif,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ciscoLwappClearResetNotif,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ciscoLwappResetFailedNotif,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ciscoLwappSysInvalidXmlConfig</td>
</tr>
<tr>
<td>AP</td>
<td>AP Register</td>
<td>bsnAPDisassociated,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bsnAPAssociated</td>
</tr>
<tr>
<td></td>
<td>Ap Interface Up/Down</td>
<td>bsnAPIfUp, bsnAPIfDown</td>
</tr>
<tr>
<td>Client Traps</td>
<td>802.11 Association</td>
<td>bsnDot11StationAssociate</td>
</tr>
<tr>
<td></td>
<td>802.11 Disassociation</td>
<td>bsnDot11StationDisassociate</td>
</tr>
<tr>
<td></td>
<td>802.11 Deauthentication</td>
<td>bsnDot11StationDeauthenticate</td>
</tr>
<tr>
<td></td>
<td>802.11 Failed Authentication</td>
<td>bsnDot11StationAuthenticateFail</td>
</tr>
<tr>
<td></td>
<td>802.11 Failed Association</td>
<td>bsnDot11StationAssociateFail</td>
</tr>
<tr>
<td></td>
<td>Exclusion</td>
<td>bsnDot11StationBlacklisted</td>
</tr>
<tr>
<td>Tab Name</td>
<td>Trap Control</td>
<td>Trap</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security Traps</td>
<td>User Authentication</td>
<td>bsnTooManyUnsuccessLoginAttempts, cLWAGuestUserLoggedln, cLWAGuestUserLoggedOut</td>
</tr>
<tr>
<td></td>
<td>RADIUS Servers Not Responding</td>
<td>bsnRADIUSServerNotResponding, ciscoLwappAAARadiusReqTimedOut</td>
</tr>
<tr>
<td></td>
<td>WEP Decrypt Error</td>
<td>bsnWepKeyDecryptError</td>
</tr>
<tr>
<td></td>
<td>SNMP Authentication</td>
<td>agentSnmpAuthenticationTrapFlag</td>
</tr>
<tr>
<td></td>
<td>Multiple Users</td>
<td>multipleUsersTrap</td>
</tr>
<tr>
<td>Auto RF Profile Traps</td>
<td>Load Profile</td>
<td>bsnAPLoadProfileFailed</td>
</tr>
<tr>
<td></td>
<td>Noise Profile</td>
<td>bsnAPNoiseProfileFailed</td>
</tr>
<tr>
<td></td>
<td>Interference Profile</td>
<td>bsnAPInterferenceProfileFailed</td>
</tr>
<tr>
<td></td>
<td>Coverage Profile</td>
<td>bsnAPCoverageProfileFailed</td>
</tr>
<tr>
<td>Auto RF Update Traps</td>
<td>Channel Update</td>
<td>bsnAPCurrentChannelChanged</td>
</tr>
<tr>
<td></td>
<td>Tx Power Update</td>
<td>bsnAPCurrentTxPowerChanged</td>
</tr>
<tr>
<td>Mesh Traps</td>
<td>Child Excluded Parent</td>
<td>ciscoLwappMeshChildExcludedParent</td>
</tr>
<tr>
<td></td>
<td>Parent Change</td>
<td>ciscoLwappMeshParentChange</td>
</tr>
<tr>
<td></td>
<td>Authfailure Mesh</td>
<td>ciscoLwappMeshAuthorizationFailure</td>
</tr>
<tr>
<td></td>
<td>Child Moved</td>
<td>ciscoLwappMeshChildMoved</td>
</tr>
<tr>
<td></td>
<td>Excessive Parent Change</td>
<td>ciscoLwappMeshExcessiveParentChange</td>
</tr>
<tr>
<td></td>
<td>Excessive Children</td>
<td>ciscoLwappMeshExcessiveChildren</td>
</tr>
<tr>
<td></td>
<td>Poor SNR</td>
<td>ciscoLwappMeshAbateSNR, ciscoLwappMeshOnsetSNR</td>
</tr>
<tr>
<td></td>
<td>Console Login</td>
<td>ciscoLwappMeshConsoleLogin</td>
</tr>
<tr>
<td></td>
<td>Excessive Association</td>
<td>ciscoLwappMeshExcessiveAssociation</td>
</tr>
<tr>
<td></td>
<td>Default Bridge Group Name</td>
<td>ciscoLwappMeshDefaultBridgeGroupName</td>
</tr>
</tbody>
</table>
The following are the trap description for the traps mentioned in the Table 7-11 above:

- **General Traps**
  - SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated.
  
  **Note** When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

  - Link (Port) Up/Down—Link changes status from up or down.
  - Multiple Users—Two users login with the same login ID.
  - Spanning Tree—Spanning Tree traps. See the STP specifications for descriptions of individual parameters.
  - Rogue AP—Whenever a rogue access point is detected this trap will be sent with its MAC Address; When a rogue access point that was detected earlier and it no longer exists this trap is sent.
  - Config Save—Notification sent when the controller configuration is modified.

- **Cisco AP Traps**
  - AP Register—Notification sent when an access point associates or disassociates with the controller.
  - AP Interface Up/Down—Notification sent when access point interface (802.11a or 802.11b/g) status goes up or down.

- **Client Related Traps**
  - 802.11 Association—The associate notification is sent when the client sends an association frame.
  - 802.11 Disassociation—The disassociate notification is sent when the client sends a disassociation frame.
  - 802.11 Deauthentication—The deauthenticate notification is sent when the client sends a deauthentication frame.
  - 802.11 Failed Authentication—The authenticate failure notification is sent when the client sends an authentication frame with a status code other than 'successful'.
  - 802.11 Failed Association—The associate failure notification is sent when the client sends an association frame with a status code other than 'successful'.
  - Exclusion—The associate failure notification is sent when a client is excluded.

- **Security Traps**
  - User Auth Failure—This trap is to inform that a client RADIUS Authentication failure has occurred.
  - RADIUS Server No Response—This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
  - WEP Decrypt Error—Notification sent when the controller detects a WEP decrypting error.
  - Rogue AP—Whenever a rogue access point is detected this trap will be sent with its MAC Address; When a rogue access point that was detected earlier and it no longer exists this trap is sent.
SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated.

**Note** When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

- Multiple Users—Two users login with the same login ID.
- Auto RF Profile Traps
  - Load Profile—Notification sent when Load Profile state changes between PASS and FAIL.
  - Noise Profile—Notification sent when Noise Profile state changes between PASS and FAIL.
  - Interference Profile—Notification sent when Interference Profile state changes between PASS and FAIL.
  - Coverage Profile—Notification sent when Coverage Profile state changes between PASS and FAIL.
- Auto RF Update Traps
  - Channel Update—Notification sent when access point dynamic channel algorithm is updated.
  - Tx Power Update—Notification sent when access point dynamic transmit power algorithm is updated.
- Mesh Traps
  - Child Excluded Parent—Notification sent when a defined number of failed association to the controller occurs through a parent mesh node.
  - Notification sent when child mesh node exceeds threshold limit of number of discovery response timeouts. The child mesh node will not try to associate excluded parent mesh node for the interval defined. The child mesh node will remember the excluded parent MAC address and when it joins the network it will inform the controller.
  - Parent Change—Notification is sent by the agent when a child mesh node changes its parent. The child mesh node remembers its previous parent and it will inform the controller about the change of its parent when it joins back the network.
  - Child Moved—Notification sent when a parent mesh node loses connection with its child mesh node.
  - Excessive Parent Change—Notification sent when child mesh node changes its parent frequently. Each mesh node keeps count of number of parent changes in fixed time. If it exceeds the defined threshold then child mesh node informs the controller.
  - Excessive Children—Notification sent when the child count exceeds for a RAP and MAP.
  - Poor SNR—Notification sent when child mesh node detects lower SNR on backhaul link. For the other trap, a notification is sent to clear a notification when child mesh node detects SNR on backhaul link is higher than the object defined by 'clMeshSNRThresholdAbate'.
  - Console Login—Notification is sent by the agent when login on MAP console is successful or failure after three attempts.
  - Default Bridge Group Name—Notification sent when MAP mesh node joins parent using 'default' bridge group name.
The remaining traps do not have trap controls. These are traps, which are not generated too frequently and thus do not require any trap control. Thus, any other trap generated by the Controller cannot be turned off.

In all of the above cases, the controller functions solely as a forwarding device.


**Guidelines and Limitations**

- Starting in release 7.0.116.0, the regular local mode or FlexConnect mode access point has been extended with a subset of Wireless Intrusion Prevention System (wIPS) capabilities. This feature enables you to deploy your access points to provide protection without needing a separate overlay network.
- wIPS ELM is not supported on 1130 and 1240 access points.

**Additional References**

For more information on the Cisco Adaptive wIPS, see the *Cisco Wireless Control System Configuration Guide, Release 7.0.172.0* and the *Cisco 3300 Series Mobility Services Engine Configuration Guide, Release 7.0.201.0*.

**Configuring wIPS on an Access Point (GUI)**

**Step 1** Choose **Wireless > Access Points > All APs > access point name**.

**Step 2** Set the **AP Mode** parameter. To configure an access point for wIPS, you must choose one of the following modes from the AP Mode drop-down list:
- Local
- FlexConnect
- Monitor

**Step 3** Set the AP Sub Mode to wIPS by choosing **wIPS** from the AP Sub Mode drop-down list.

**Step 4** Click **Apply**.
Configuring wIPS on an Access Point (CLI)

Step 1
Configure an access point for monitor mode by entering this command:
```
config ap mode {monitor | local | flexconnect} Cisco_AP
```

Note
To configure an access point for wIPS, the access point must be in monitor, local, or flexconnect modes.

Step 2
Enter Y when you see the message that the access point will be rebooted if you want to continue.

Step 3
Save your changes by entering this command:
```
save config
```

Step 4
Disable the access point radio by entering this command:
```
config {802.11a | 802.11b} disable Cisco_AP
```

Step 5
Configure the wIPS submode on the access point by entering this command:
```
config ap mode ap_mode submode wips Cisco_AP
```

Note
To disable wIPS on the access point, enter the `config ap mode ap_mode submode none Cisco_AP` command.

Step 6
Enable wIPS optimized channel scanning for the access point by entering this command:
```
config ap monitor-mode wips-optimized Cisco_AP
```

The access point scans each channel for 250 milliseconds. It derives the list of channels to be scanned from the monitor configuration. You can choose one of these options:

* **All**—All channels supported by the access point’s radio
* **Country**—Only the channels supported by the access point’s country of operation
* **DCA**—Only the channel set used by the dynamic channel assignment (DCA) algorithm, which by default includes all of the nonoverlapping channels allowed in the access point’s country of operation

The 802.11a or 802.11b Monitor Channels text box in the output of the `show advanced {802.11a | 802.11b} monitor` command shows the monitor configuration channel set:

```
Default 802.11b AP monitoring
802.11b Monitor Mode.......................... enable
802.11b Monitor Channels.................... Country channels
802.11b AP Coverage Interval............... 180 seconds
802.11b AP Load Interval.................... 60 seconds
802.11b AP Noise Interval................... 180 seconds
802.11b AP Signal Strength Interval....... 60 seconds
```

Step 7
Reenable the access point radio by entering this command:
```
config {802.11a | 802.11b} enable Cisco_AP
```

Step 8
Save your changes by entering this command:
```
save config
```
Viewing wIPS Information (CLI)

You can also view the access point submode from the controller GUI. To do so, choose Wireless > Access Points > All APs > the access point name > the Advanced tab. The AP Sub Mode text box shows wIPS if the access point is in monitor mode and the wIPS submode is configured on the access point or None if the access point is not in monitor mode or the access point is in monitor mode but the wIPS submode is not configured.

- See the wIPS submode on the access point by entering this command:
  
  ```
  show ap config general Cisco_AP
  ```

  Information similar to the following appears:

  ```
  Cisco AP Identifier.............................. 3
  Cisco AP Name.................................... AP1131:46f2.98ac
  ...
  AP Mode ......................................... Monitor
  Public Safety ................................... Disabled  Disabled
  AP SubMode ...................................... WIPS
  ...
  ```

- See the wIPS optimized channel scanning configuration on the access point by entering this command:

  ```
  show ap monitor-mode summary
  ```

  Information similar to the following appears:

  ```
  AP Name      Ethernet MAC         Status      Scanning Channel List
  ------------------ -------------------- ----------  ------------------------
  AP1131:46f2.98ac    00:16:46:f2:98:ac     wIPS       1, 6, NA, NA
  ```

- See the wIPS configuration forwarded by WCS to the controller by entering this command:

  ```
  show wps wips summary
  ```

  Information similar to the following appears:

  ```
  Policy Name.............. Default
  Policy Version.......... 3
  ```

- See the current state of wIPS operation on the controller by entering this command:

  ```
  show wps wips statistics
  ```

  Information similar to the following appears:

  ```
  Policy Assignment Requests............ 1
  Policy Assignment Responses........... 1
  Policy Update Requests............... 0
  Policy Update Responses.............. 0
  Policy Delete Requests............... 0
  Policy Delete Responses.............. 0
  Alarm Updates......................... 13572
  Device Updates......................... 8376
  Device Update Requests............... 0
  Device Update Responses.............. 0
  Forensic Updates...................... 1001
  Invalid WIPS Payloads............... 0
  Invalid Messages Received........... 0
  NMSP Transmitted Packets............. 22950
  ```
Configuring Wi-Fi Direct Client Policy

This section contains the following topics:

- Information About Wi-Fi Direct Client Policy, page 7-129
- Guidelines and Limitations, page 7-129
- Configuring Wi-Fi Direct Client Policy (GUI), page 7-129
- Configuring Wi-Fi Direct Client Policy (CLI), page 7-130
- Monitoring and Troubleshooting Wi-Fi Direct Client Policy (CLI), page 7-130

Information About Wi-Fi Direct Client Policy

Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices can associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently. You can use the controller to configure the Wi-Fi Direct Client Policy, on a per WLAN basis, where you can allow or disallow association of Wi-Fi devices with infrastructure WLANs or disable Wi-Fi Direct Client Policy altogether for WLANs.

Guidelines and Limitations

Wi-Fi Direct Client Policy is applicable to WLANs that have APs in local mode only.

Configuring Wi-Fi Direct Client Policy (GUI)

Step 1  Choose WLANs to open the WLANs page.

Step 2  Click the WLAN ID of the WLAN for which you want to configure the Wi-Fi Direct Client Policy. The WLANs > Edit page appears.

Step 3  Click the Advanced tab.

Step 4  From the Wi-Fi Direct Clients Policy drop-down list, choose one of the following options:

- **Disabled**—Disables the Wi-Fi Direct Client Policy for the WLAN and deauthenticates all Wi-Fi Direct clients.
- **Allow**—Allows Wi-Fi Direct clients to associate with the WLAN.
- **Not-Allow**—Disallows the Wi-Fi Direct clients from associating with the WLAN.

Step 5  Click Apply to commit your configuration.
Configuring Wi-Fi Direct Client Policy (CLI)

Step 1
To configure the Wi-Fi Direct Client Policy on WLANs, enter this command:

```
config wlan wifidirect {allow | disable | not-allow} wlan-id
```

The syntax of the command is as follows:
- **allow**—Allows Wi-Fi Direct clients to associate with the WLAN.
- **disable**—Disables the Wi-Fi Direct Client Policy for the WLAN and deauthenticates all Wi-Fi Direct clients.
- **not-allow**—Disallows the Wi-Fi Direct clients from associating with the WLAN.
- **wlan-id**—WLAN identifier.

Step 2
Save your configuration by entering this command:
```
save config
```

Monitoring and Troubleshooting Wi-Fi Direct Client Policy (CLI)

To monitor and troubleshoot the Wi-Fi Direct Client Policy, enter these commands:
- **show wlan wifidirect wlan-id**—Displays the status of Wi-Fi Direct Client Policy on the WLAN.
- **show client wifiDirect-stats**—Displays the total number of clients associated and number of clients rejected if Wi-Fi Direct Client Policy is enabled.

Configuring Web Auth Proxy

This section contains the following topics:
- **Information About Web Auth Proxy**, page 7-130
- **Configuring Web Auth Proxy (GUI)**, page 7-131
- **Configuring Web Auth Proxy (CLI)**, page 7-132

Information About Web Auth Proxy

This feature enables clients that have a manual web proxy enabled in the browser to facilitate authentication with the controller. If the user's browser is configured with manual proxy settings with a configured port number as 8080 or 3128 and if the client requests any URL, the controller responds with a web page prompting the user to change the Internet proxy settings to automatically detect the proxy settings so that the browser's manual proxy settings information does not get lost. After enabling this settings, the user can get access to the network through the web authentication policy. This functionality is given for port 8080 and 3128 because these are the most commonly used ports for the web proxy server.
Note
Webauth proxy redirect ports are not blocked via CPU ACL. If a CPU ACL is configured to block the port 8080, 3128, and one random port as part of webauth proxy configuration, then those ports are not blocked because the webauth rules take higher precedence than the CPU ACL rules, until the client is in webauth_req state.

A web browser has three types of Internet settings that can be configured by the user:

- Auto detect
- System Proxy
- Manual

In a manual proxy server configuration, the browser uses a proxy server's IP address and a port. If this configuration is enabled on the browser, the wireless client communicates with the destination proxy server's IP on the configured port. In a Web-Auth scenario, the controller does not listen to such proxy ports and the client would not be able to establish a TCP connection with the controller. In effect, the user is unable to get any login page to authentication and get access to the network.

When a wireless client enters a web authenticated WLAN network, it tries to access a URL. If a manual proxy configuration is configured on the client's browser, all web traffic going out from the client will be destined to the proxy IP and port configured on the browser.

- A TCP connection is established between the client and the proxy server IP address that the controller proxies for.
- The client processes the DHCP response and obtains a JavaScript file from the controller. The script disables all proxy configurations on the client for that session.

Note
For external clients, the controller sends the login page as is (with or without JavaScript).

- Any requests that are bypass the proxy configuration. The controller can then perform web-redirection, login, and authentication.
- When the client goes out of the network, and then back into its own network, a DHCP refresh occurs and the client continues to use the old proxy configuration configured on the browser.
- If the external DHCP server is used with webauth proxy, then DHCP option 252 must be configured on the DHCP server for that scope. The value of option 252 will have the format http://<virtual ip>/proxy.js. No extra configuration is needed for internal DHCP servers.

Note
When you configure FIPS mode with secure web authentication, we recommend that you use Mozilla Firefox as your browser.

Configuring Web Auth Proxy (GUI)

Step 1
Choose Controller > General to open the Controller > General page.

Step 2
From the WebAuth Proxy Redirection Mode, select Enabled.

Step 3
In the WebAuth Proxy Redirection Port text box, enter the port number of the web auth proxy.
This text box consists of the port numbers on which the controller listens to for web authentication proxy redirection. By default, the three ports 80, 8080, and 3128 are assumed. If you configured the web authentication redirection port to any port other than these values, you must specify that value.

**Step 4** Click **Apply**.

### Configuring Web Auth Proxy (CLI)

- Enable web auth proxy redirection by entering the `config network web-auth proxy-redirect {enable | disable}` command.

- Configure the secure web (https) authentication for clients by entering the `config network web-auth secureweb {enable | disable}` command.

  The default secure web (https) authentication for clients is enabled.

**Note** If you configure to disallow secure web (https) authentication for clients using the `config network web-auth secureweb disable` command, then you must reboot the Cisco WLC to implement the change.

- Set the web auth port number by entering the `config network web-auth port port-number` command.

  This parameter specifies the port numbers on which the controller listens to for web authentication proxy redirection. By default, the three ports 80, 8080, and 3128 are assumed. If you configured the web authentication redirection port to any port other than these values, you must specify that value.

- To see the current status of the web auth proxy configuration, enter the `show network summary` or the `show running-config` command.

### Detecting Active Exploits

The controller supports three active exploit alarms that serve as notifications of potential threats. They are enabled by default and therefore require no configuration on the controller.

- **ASLEAP detection**—The controller raises a trap event if an attacker launches a LEAP crack tool. The trap message is visible in the controller’s trap log.

- **Fake access point detection**—The controller tweaks the fake access point detection logic to avoid false access point alarms in high-density access point environments.

- **Honeypot access point detection**—The controller raises a trap event if a rogue access point is using managed SSIDs (WLANs configured on the controller). The trap message is visible in the controller’s trap log.
Working with WLANs

This chapter contains the following sections:

- Information About WLANs, page 8-1
- Guidelines and Limitations, page 8-1
- Creating WLANs, page 8-3
- Searching WLANs, page 8-6
- Configuring WLANs, page 8-8

Information About WLANs

The Cisco UWN solution can control up to 512 WLANs for lightweight access points. Each WLAN has a separate WLAN ID (1 through 512), a separate profile name, and a WLAN SSID. All controllers publish up to 16 WLANs to each connected access point, but you can create up to 512 WLANs and then selectively publish these WLANs (using access point groups) to different access points to better manage your wireless network.

You can configure WLANs with different Service Set Identifiers (SSIDs) or with the same SSID. An SSID identifies the specific wireless network that you want the controller to access.

Guidelines and Limitations

- All OfficeExtend access points should be in the same access point group, and that 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.

- You can associate up to 16 WLANs with each access point group and assign specific access points to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point does not advertise disabled WLANs in its access point group or WLANs that belong to another group. See the “Creating Access Point Groups (GUI)” section on page 8-60 for more information on access point groups.

- We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers properly route VLAN traffic.

The controller uses different attributes to differentiate between WLANs with the same SSID.

- WLANs with the same SSID and same L2 Policy cannot be created if the WLAN ID < 17.
Guidelines and Limitations

- Two WLANs with ids greater than 17 having the same SSID and same L2 policy is allowed provided WLANS are added in different AP groups.

  **Note** This requirement ensures that clients never detect the SSID present on the same access point radio.

When creating a WLAN with the same SSID, follow these guidelines and requirements:
- You must create a unique profile name for each WLAN.
- When multiple WLANs with the same SSID get assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between them.

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in beacon and probe responses. The available Layer 2 security policies are as follows:
- None (open WLAN)
- Static WEP or 802.1X
  
  **Note** Because static WEP and 802.1X are both advertised by the same bit in beacon and probe responses, they cannot be differentiated by clients. Therefore, they cannot both be used by multiple WLANs with the same SSID.

- CKIP
- WPA/WPA2

  **Note** Although WPA and WPA2 cannot be used by multiple WLANs with the same SSID, you can configure two WLANs with the same SSID with WPA/TKIP with PSK and WPA (Wi-Fi Protected Access) /TKIP (Temporal Key Integrity Protocol) with 802.1X, respectively, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X, respectively.

- If you configured your WLAN with EAP Passthrough and if you downgrade to an earlier controller version, you might encounter XML validation errors during the downgrade process. This problem is because EAP Passthrough is not supported in earlier releases. The configuration will default to the default security settings (WPA2/802.1X).

  **Caution** Some clients might not be able to connect to WLANs properly if they detect the same SSID with multiple security policies. Use this feature with care.

  **Note** The OEAP 600 Series access point supports a maximum of two WLANs and one remote LAN. If you have configured more than two WLANs and one remote LAN, you can assign the 600 Series access point to an AP group. The support for two WLANs and one remote LAN still applies to the AP Group. If the 600 Series OEAP is in the default group, the WLAN or remote LAN IDs must be lower than 8.

  Cisco Flex 7500 Series Controller does not support the 802.1x security variants on a centrally switched WLAN. For example, the following configurations are not allowed on a centrally switched WLAN:
   - WPA1/WPA2 with 802.1x AKM
• WPA1/WPA2 with CCKM
• Dynamic-WEP
• Conditional webauth
• Splash WEB page redirect
• If you want to configure your WLAN in any of the above combinations, the WLAN must be configured to use local switching.

Creating WLANs

This section contains the following topics:
• Creating and Removing WLANs (GUI), page 8-3
• Enabling and Disabling WLANs (GUI), page 8-4
• Creating and Deleting WLANs (CLI), page 8-4
• Viewing WLANs (CLI), page 8-5
• Enabling and Disabling WLANs (CLI), page 8-5

Creating and Removing WLANs (GUI)

Step 1  Choose WLANs to open the WLANs page.

This page lists all of the WLANs currently configured on the controller. For each WLAN, you can see its WLAN ID, profile name, type, SSID, status, and security policies.

The total number of WLANs appears in the upper right-hand corner of the page. If the list of WLANs spans multiple pages, you can access these pages by clicking the page number links.

Note  If you want to delete a WLAN, hover your cursor over the blue drop-down arrow for that WLAN and choose Remove, or select the check box to the left of the WLAN, choose Remove Selected from the drop-down list, and click Go. A message appears asking you to confirm your decision. If you proceed, the WLAN is removed from any access point group to which it is assigned and from the access point’s radio.

Step 2  Create a new WLAN by choosing Create New from the drop-down list and clicking Go. The WLANs > New page appears.

Note  When you upgrade to controller software release 5.2 or later releases, the controller creates the default-group access point group and automatically populates it with the first 16 WLANs (WLANs with IDs 1 through 16, or fewer if 16 WLANs are not configured). This default group cannot be modified (you cannot add WLANs to it or delete WLANs from it). It is dynamically updated whenever the first 16 WLANs are added or deleted. If an access point does not belong to an access point group, it is assigned to the default group and uses the WLANs in that group. If an access point joins the controller with an undefined access point group name, the access point keeps its group name but uses the WLANs in the default-group access point group.

Step 3  From the Type drop-down list, choose WLAN to create a WLAN.
Creating WLANs

Note If you want to create a guest LAN for wired guest users, choose Guest LAN and follow the instructions in the “Configuring Wired Guest Access” section on page 12-28.

Step 4 In the Profile Name text box, enter up to 32 alphanumeric characters for the profile name to be assigned to this WLAN. The profile name must be unique.

Step 5 In the WLAN SSID text box, enter up to 32 alphanumeric characters for the SSID to be assigned to this WLAN.

Step 6 From the WLAN ID drop-down list, choose the ID number for this WLAN.

Note If the Cisco OEAP 600 is in the default group, the WLAN/Remote LAN IDs need to be set as lower than ID 8.

Step 7 Click Apply to commit your changes. The WLANs > Edit page appears.

Note You can also open the WLANs > Edit page from the WLANs page by clicking the ID number of the WLAN that you want to edit.

Step 8 Use the parameters on the General, Security, QoS, and Advanced tabs to configure this WLAN. See the sections in the rest of this chapter for instructions on configuring specific features for WLANs.

Step 9 On the General tab, select the Status check box to enable this WLAN. Be sure to leave it unselected until you have finished making configuration changes to the WLAN.

Step 10 Click Apply to commit your changes.

Step 11 Click Save Configuration to save your changes.

Enabling and Disabling WLANs (GUI)

Step 1 Choose WLANs to open the WLANs page.

This page lists all of the WLANs currently configured on the controller.

Step 2 Enable or disable WLANs from the WLANs page by selecting the check boxes to the left of the WLANs that you want to enable or disable, choosing Enable Selected or Disable Selected from the drop-down list, and clicking Go.

Step 3 Click Apply.

Creating and Deleting WLANs (CLI)

- Create a new WLAN by entering this command:

  ```bash
  config wlan create wlan_id {profile_name | foreign_ap} ssid
  ```
Chapter 8  Working with WLANs

Creating WLANs

Note
If you do not specify an ssid, the profile_name parameter is used for both the profile name and the SSID.

Note
When WLAN 1 is created in the configuration wizard, it is created in enabled mode. Disable it until you have finished configuring it. When you create a new WLAN using the config wlan create command, it is created in disabled mode. Leave it disabled until you have finished configuring it.

Note
If you want to create a guest LAN for wired guest users, follow the instructions in the “Configuring Wired Guest Access” section on page 12-28.

• Delete a WLAN by entering this command:
  config wlan delete {wlan_id | foreign_ap}

Note
An error message appears if you try to delete a WLAN that is assigned to an access point group. If you proceed, the WLAN is removed from the access point group and from the access point’s radio.

Viewing WLANs (CLI)

• View the list of existing WLANs and to see whether they are enabled or disabled by entering this command:
  show wlan summary

Enabling and Disabling WLANs (CLI)

• Enable a WLAN (for example, after you have finished making configuration changes to the WLAN) by entering this command:
  config wlan enable {wlan_id | foreign_ap | all}

Note
If the command fails, an error message appears (for example, “Request failed for wlan 10 - Static WEP key size does not match 802.1X WEP key size”).

• Disable a WLAN (for example, before making any modifications to a WLAN) by entering this command:
  config wlan disable {wlan_id | foreign_ap | all}

where
  • wlan_id is a WLAN ID between 1 and 512.
  • foreign_ap is a third-party access point.
  • all is all WLANs.
Note

If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.

Searching WLANs

This section contains the following topics:

- Searching WLANs (GUI), page 8-6
- Setting the Client Count per WLAN, page 8-6

Searching WLANs (GUI)

Step 1
To search for WLANs using the controller GUI, follow these steps:

Step 2
On the WLANs page, click Change Filter. The Search WLANs dialog box appears.

Step 3
Perform one of the following:

- To search for WLANs based on profile name, select the Profile Name check box and enter the desired profile name in the edit box.
- To search for WLANs based on SSID, select the SSID check box and enter the desired SSID in the edit box.
- To search for WLANs based on their status, select the Status check box and choose Enabled or Disabled from the drop-down list.

Step 4
Click Find. Only the WLANs that match your search criteria appear on the WLANs page, and the Current Filter field at the top of the page specifies the search criteria used to generate the list (for example, None, Profile Name:user1, SSID:test1, Status: disabled).

Note
To clear any configured search criteria and display the entire list of WLANs, click Clear Filter.

Setting the Client Count per WLAN

This section contains the following topics:

- Information About Setting Client Count per WLAN, page 8-7
- Guidelines and Limitations, page 8-7
- Configuring Client Count per WLAN (GUI), page 8-7
- Configuring Maximum Number of Clients per WLAN (CLI), page 8-7
Information About Setting Client Count per WLAN

You can set a limit to the number of clients that can connect to a WLAN, which is useful in scenarios where you have a limited number of clients that can connect to a controller. For example, consider a scenario where the controller can serve up to 256 clients on a WLAN and these clients can be shared between enterprise users (employees) and guest users. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure per WLAN depends on the platform that you are using.

Guidelines and Limitations

- The maximum number of clients per WLAN feature is not supported when you use FlexConnect local authentication.
- The maximum number of clients per WLAN feature is supported only for access points that are in connected mode.

Configuring Client Count per WLAN (GUI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose WLANs to open the WLANs page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the ID number of the WLAN for which you want to limit the number of clients. The WLANs &gt; Edit page appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the Advanced tab, enter the Maximum Allowed Clients text box. See Table 8-1 for the maximum number of clients supported per platform.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Apply to commit your changes.</td>
</tr>
</tbody>
</table>

Configuring Maximum Number of Clients per WLAN (CLI)

| Step 1 | Determine the WLAN ID for which you want to configure the maximum clients by entering this command: show wlan summary |
| Step 2 | Configure the maximum number of clients per WLAN by entering this command: config wlan max-associated-clients max-clients wlanid |
|        | See Table 8-1 for the maximum number of clients supported per platform. |

Configuring Maximum Number of Clients per AP Radio Per WLAN (GUI)

| Step 1 | Choose WLANs to open the WLANs page. |
| Step 2 | Click the ID number of the WLAN for which you want to limit the number of clients. The WLANs > Edit page appears. |
Chapter 8 Working with WLANs

Configuring WLANs

Step 3 On the Advanced tab, enter the maximum allowed clients per access point radio in the Maximum Allowed Clients Per AP Radio text box. You can configure up to 200 clients.

Step 4 Click Apply to commit your changes.

Configuring Maximum Number of Clients per AP Radio Per WLAN (CLI)

Step 1 Determine the WLAN ID for which you want to configure the maximum clients per radio by entering this command:

```
show wlan summary
```

Obtain the WLAN ID from the list.

Step 2 Configure the maximum number of clients per WLAN by entering this command:

```
config wlan max-radio-clients client_count
```

You can configure up to 200 clients.

Step 3 To view the configured maximum associated clients, use the show 802.11a command.

Configuring WLANs

This section contains the following topics:
- Configuring DHCP, page 8-9
- Configuring MAC Filtering for WLANs, page 8-16
- Configuring Local MAC Filters, page 8-16
- Configuring a Timeout for Disabled Clients, page 8-17
- Assigning WLANs to Interfaces, page 8-18
- Configuring the DTIM Period, page 8-18
- Configuring Peer-to-Peer Blocking, page 8-20
- Configuring Layer 2 Security, page 8-23
- Configuring a WLAN for Both Static and Dynamic WEP, page 8-24
- Configuring WPA1 +WPA2, page 8-26
- Configuring CKIP, page 8-29
- Configuring Session Timeouts, page 8-32
- Configuring Layer 3 Security Using Web Authentication, page 8-33
- Configuring Layer 3 Security Using Web Authentication, page 8-33
- Configuring a Fallback Policy with MAC Filtering and Web Authentication, page 8-36
- Assigning a QoS Profile to a WLAN, page 8-38
- Configuring QoS Enhanced BSS, page 8-40
- Configuring Media Session Snooping and Reporting, page 8-43
Configuring DHCP

You can configure WLANs to use the same or different Dynamic Host Configuration Protocol (DHCP) servers or no DHCP server. Two types of DHCP servers are available: internal and external.

This section contains the following topics:
- Internal DHCP Server, page 8-9
- External DHCP Servers, page 8-10
- DHCP Assignment, page 8-10
- Configuring DHCP, page 8-11
- Configuring DHCP Scopes, page 8-13

Internal DHCP Server

The controllers contain an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server. The wireless network generally contains 10 access points or fewer, with the access points on the same IP subnet as the controller. The internal server provides DHCP addresses to wireless clients, direct-connect access points, and DHCP requests that are relayed from access points. Only lightweight access points are supported. When you want to use the internal DHCP server, you must set the management interface IP address of the controller as the DHCP server IP address.

DHCP option 43 is not supported on the internal server. Therefore, the access point must use an alternative method to locate the management interface IP address of the controller, such as local subnet broadcast, DNS, or priming.
Configuring WLANs

Note
See Chapter 9, “Controlling Lightweight Access Points,” or the Controller Deployment Guide at this URL for more information on how access points find controllers:


An internal DHCP server pool only serves the wireless clients of that controller, not clients of other controllers. Also, internal DHCP server can only serve wireless clients and not wired clients. Wired guest clients are always on a Layer 2 network connected to a local or foreign controller.

Note
The DHCP required state can cause traffic to not be forwarded properly if a client is deauthenticated or removed. To overcome this problem, ensure that the DHCP required state is always disabled.

Note
The controller does not support internal DHCPv6 servers. However, clients can learn the IP addresses that are assigned by an external DHCPv6 server.

External DHCP Servers

The operating system is designed to appear as a DHCP Relay to the network and as a DHCP server to clients with industry-standard external DHCP servers that support DHCP Relay, which means that each controller appears as a DHCP Relay agent to the DHCP server and as a DHCP server at the virtual IP address to wireless clients.

Because the controller captures the client IP address obtained from a DHCP server, it maintains the same IP address for that client during intra-controller, inter-controller, and inter-subnet client roaming.

DHCP Assignment

You can configure DHCP on a per-interface or per-WLAN basis. The preferred method is to use the primary DHCP server address assigned to a particular interface.

You can assign DHCP servers for individual interfaces. The management interface, AP-manager interface, and dynamic interfaces can be configured for a primary and secondary DHCP server, and the service-port interface can be configured to enable or disable DHCP servers.

Note
See Chapter 11, “Managing Controller Software and Configurations,” for information on configuring the controller’s interfaces.

You can also define a DHCP server on a WLAN. This server will override the DHCP server address on the interface assigned to the WLAN.

Security Considerations

For enhanced security, we recommend that you require all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, all WLANs can be configured with a DHCP Addr. Assignment Required setting, which disallows client static IP addresses. If DHCP Addr. Assignment
Required is selected, clients must obtain an IP address via DHCP. Any client with a static IP address is not allowed on the network. The controller monitors DHCP traffic because it acts as a DHCP proxy for the clients.

---

**Note**

WLANs that support management over wireless must allow management (device-servicing) clients to obtain an IP address from a DHCP server. See the “Using Management Over Wireless” section on page 7-51 for instructions on configuring management over wireless.

---

If slightly less security is tolerable, you can create WLANs with DHCP Addr. Assignment Required disabled. Clients then have the option of using a static IP address or obtaining an IP address from a designated DHCP server.

---

**Note**

DHCP Addr. Assignment Required is not supported for wired guest LANs.

---

You are also allowed to create separate WLANs with DHCP Addr. Assignment Required being disabled. This is applicable only if DHCP proxy is enabled for the controller. It is not necessary to define the primary/secondary DHCP server. These WLANs drop all DHCP requests and force clients to use a static IP address. These WLANs do not support management over wireless connections.

---

**Note**


---

**Note**

If you want to specify a static IP address for an access point rather than having one assigned automatically by a DHCP server, see the “Configuring a Static IP Address on a Lightweight Access Point” section on page 9-48 for more information.

---

**Guidelines and Limitations**

The controller internal DHCP server does not support Cisco Aironet 600 Series OfficeExtend Access Point.

---

**Configuring DHCP**

This section contains the following topics:

- Configuring DHCP (GUI), page 8-11
- Configuring DHCP (CLI), page 8-12
- Debugging DHCP (CLI), page 8-13

---

**Configuring DHCP (GUI)**

To configure a primary DHCP server for a management, AP-manager, or dynamic interface, see Chapter 4, “Configuring Ports and Interfaces.”

When you want to use the internal DHCP server, you must set the management interface IP address of the controller as the DHCP server IP address.
Step 1 Choose WLANs to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to assign an interface. The WLANs > Edit (General) page appears.

Step 3 On the General tab, unselect the Status check box and click Apply to disable the WLAN.

Step 4 Click the ID number of the WLAN.

Step 5 On the General tab, choose the interface for which you configured a primary DHCP server to be used with this WLAN from the Interface drop-down list.

Step 6 Choose the Advanced tab to open the WLANs > Edit (Advanced) page.

Step 7 If you want to define a DHCP server on the WLAN that will override the DHCP server address on the interface assigned to the WLAN, select the DHCP Server Override check box and enter the IP address of the desired DHCP server in the DHCP Server IP Addr text box. The default value for the check box is disabled.

Note The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override.

Note DHCP Server override is applicable only for the default group.

Note If a WLAN has the DHCP server override option enabled and the controller has DHCP proxy enabled, any interface mapped to the WLAN must have a DHCP server IP address or the WLAN must be configured with a DHCP server IP address.

Step 8 If you want to require all clients to obtain their IP addresses from a DHCP server, select the DHCP Addr. Assignment Required check box. When this feature is enabled, any client with a static IP address is not allowed on the network. The default value is disabled.

Note DHCP Addr. Assignment Required is not supported for wired guest LANs.

Step 9 Click Apply to commit your changes.

Step 10 On the General tab, select the Status check box and click Apply to reenable the WLAN.

Step 11 Click Save Configuration to save your changes.

Configuring DHCP (CLI)

To configure a primary DHCP server for a management, AP-manager, or dynamic interface, see Chapter 4, “Configuring Ports and Interfaces.”

Step 1 Disable the WLAN by entering this command:

```
cfg wlan disable wlan_id
```
Step 2  Specify the interface for which you configured a primary DHCP server to be used with this WLAN by entering this command:

```config wlan interface wlan_id interface_name```

Step 3  If you want to define a DHCP server on the WLAN that will override the DHCP server address on the interface assigned to the WLAN, enter this command:

```config wlan dhcp_server wlan_id dhcp_server_ip_address```

Note  The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override. If you enable the override, you can use the `show wlan` command to verify that the DHCP server has been assigned to the WLAN.

Note  If a WLAN has the DHCP server override option enabled and the controller has DHCP proxy enabled, any interface mapped to the WLAN must have a DHCP server IP address or the WLAN must be configured with a DHCP server IP address.

Step 4  Reenable the WLAN by entering this command:

```config wlan enable wlan_id```

**Debugging DHCP (CLI)**

- `debug dhcp packet {enable | disable}`—Enables or disables debugging of DHCP packets.
- `debug dhcp message {enable | disable}`—Enables or disables debugging of DHCP error messages.
- `debug dhcp service-port {enable | disable}`—Enables or disables debugging of DHCP packets on the service port.

**Configuring DHCP Scopes**

Controllers have built-in DHCP relay agents. However, when you desire network segments that do not have a separate DHCP server, the controllers can have built-in DHCP scopes that assign IP addresses and subnet masks to wireless clients. Typically, one controller can have one or more DHCP scopes that each provide a range of IP addresses.

DHCP scopes are needed for internal DHCP to work. Once DHCP is defined on the controller, you can then point the primary DHCP server IP address on the management, AP-manager, and dynamic interfaces to the controller’s management interface.

You can configure up to 16 DHCP scopes using the controller GUI or CLI.

This section contains the following topics:

- Configuring DHCP Scopes (GUI), page 8-14
- Configuring DHCP Scopes (CLI), page 8-15
Configuring DHCP Scopes (GUI)

Step 1  Choose Controller > Internal DHCP Server > DHCP Scope to open the DHCP Scopes page. This page lists any DHCP scopes that have already been configured.

Note  If you ever want to delete an existing DHCP scope, hover your cursor over the blue drop-down arrow for that scope and choose Remove.

Step 2  Click New to add a new DHCP scope. The DHCP Scope > New page appears.

Step 3  In the Scope Name text box, enter a name for the new DHCP scope.

Step 4  Click Apply. When the DHCP Scopes page reappears, click the name of the new scope. The DHCP Scope > Edit page appears.

Step 5  In the Pool Start Address text box, enter the starting IP address in the range assigned to the clients.

Note  This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 6  In the Pool End Address text box, enter the ending IP address in the range assigned to the clients.

Note  This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 7  In the Network text box, enter the network served by this DHCP scope. This IP address is used by the management interface with Netmask applied, as configured on the Interfaces page.

Step 8  In the Netmask text box, enter the subnet mask assigned to all wireless clients.

Step 9  In the Lease Time text box, enter the amount of time (from 0 to 65536 seconds) that an IP address is granted to a client.

Step 10  In the Default Routers text box, enter the IP address of the optional router connecting the controllers. Each router must include a DHCP forwarding agent, which allows a single controller to serve the clients of multiple controllers.

Step 11  In the DNS Domain Name text box, enter the optional domain name system (DNS) domain name of this DHCP scope for use with one or more DNS servers.

Step 12  In the DNS Servers text box, enter the IP address of the optional DNS server. Each DNS server must be able to update a client’s DNS entry to match the IP address assigned by this DHCP scope.

Step 13  In the Netbios Name Servers text box, enter the IP address of the optional Microsoft Network Basic Input Output System (NetBIOS) name server, such as the Internet Naming Service (WINS) server.

Step 14  From the Status drop-down list, choose Enabled to enable this DHCP scope or choose Disabled to disable it.

Step 15  Click Apply to commit your changes.

Step 16  Click Save Configuration to save your changes.
Step 17  Choose **DHCP Allocated Leases** to see the remaining lease time for wireless clients. The DHCP Allocated Lease page appears, showing the MAC address, IP address, and remaining lease time for the wireless clients.

### Configuring DHCP Scopes (CLI)

#### Step 1
Create a new DHCP scope by entering this command:

```
config dhcp create-scope scope
```

**Note**  If you ever want to delete a DHCP scope, enter this command: `config dhcp delete-scope scope`.

#### Step 2
Specify the starting and ending IP address in the range assigned to the clients by entering this command:

```
config dhcp address-pool scope start end
```

**Note**  This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

#### Step 3
Specify the network served by this DHCP scope (the IP address used by the management interface with the Netmask applied) and the subnet mask assigned to all wireless clients by entering this command:

```
config dhcp network scope network netmask
```

#### Step 4
Specify the amount of time (from 0 to 65536 seconds) that an IP address is granted to a client by entering this command:

```
config dhcp lease scope lease_duration
```

#### Step 5
Specify the IP address of the optional router connecting the controllers by entering this command:

```
config dhcp default-router scope router_1 [router_2] [router_3]
```

Each router must include a DHCP forwarding agent, which allows a single controller to serve the clients of multiple controllers.

#### Step 6
Specify the optional domain name system (DNS) domain name of this DHCP scope for use with one or more DNS servers by entering this command:

```
config dhcp domain scope domain
```

#### Step 7
Specify the IP address of the optional DNS server(s) by entering this command:

```
config dhcp dns-servers scope dns1 [dns2] [dns3]
```

Each DNS server must be able to update a client’s DNS entry to match the IP address assigned by this DHCP scope

#### Step 8
Specify the IP address of the optional Microsoft Network Basic Input Output System (NetBIOS) name server, such as the Internet Naming Service (WINS) server by entering this command:

```
config dhcp netbios-name-server scope wins1 [wins2] [wins3]
```

#### Step 9
Enable or disable this DHCP scope by entering this command:

```
config dhcp {enable | disable} scope
```

#### Step 10
Save your changes by entering this command:
save config

**Step 11**

See the list of configured DHCP scopes by entering this command:

```
show dhcp summary
```

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Scope Name</th>
<th>Enabled</th>
<th>Address Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope 1</td>
<td>No</td>
<td>0.0.0.0 -&gt; 0.0.0.0</td>
</tr>
<tr>
<td>Scope 2</td>
<td>No</td>
<td>0.0.0.0 -&gt; 0.0.0.0</td>
</tr>
</tbody>
</table>

**Step 12**

Display the DHCP information for a particular scope by entering this command:

```
show dhcp scope
```

Information similar to the following appears:

```
Enabled....................................... No
Lease Time.................................... 0
Pool Start.................................... 0.0.0.0
Pool End...................................... 0.0.0.0
Network....................................... 0.0.0.0
Netmask....................................... 0.0.0.0
Default Routers............................... 0.0.0.0 0.0.0.0 0.0.0.0
DNS Domain....................................
DNS........................................... 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers....................... 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

---

**Configuring MAC Filtering for WLANs**

When you use MAC filtering for client or administrator authorization, you need to enable it at the WLAN level first. If you plan to use local MAC address filtering for any WLAN, use the commands in this section to configure MAC filtering for a WLAN.

Use these commands to enable MAC filtering on a WLAN:

- Enable MAC filtering by entering the `config wlan mac-filtering enable wlan_id` command.
- Verify that you have MAC filtering enabled for the WLAN by entering the `show wlan` command.

When you enable MAC filtering, only the MAC addresses that you add to the WLAN are allowed to join the WLAN. MAC addresses that have not been added are not allowed to join the WLAN.

---

**Configuring Local MAC Filters**

This section contains the following topics:

- Information About Local MAC Filters, page 8-17
- Guidelines and Limitations, page 8-17
- Configuring Local MAC Filters (CLI), page 8-17
- Configuring a Timeout for Disabled Clients, page 8-17
- Configuring a Timeout for Disabled Clients (CLI), page 8-17
Information About Local MAC Filters

Controllers have built-in MAC filtering capability, similar to that provided by a RADIUS authorization server. You can configure a MAC filter using the GUI or CLI.

Configuring Local MAC Filters (CLI)

- Create a MAC filter entry on the controller by entering the `config macfilter add mac_addr wlan_id [interface_name] [description] [IP_addr]` command.

  The following parameters are optional:
  - `mac_addr`—MAC address of the client.
  - `wlan_id`—WLAN id on which the client is associating.
  - `interface_name`—The name of the interface. This interface name is used to override the interface configured to the WLAN.
  - `description`—A brief description of the interface in double quotes (for example, “Interface1”).
  - `IP_addr`—The IP address which is used for a passive client with the MAC address specified by the `mac_addr` value above.

- Assign an IP address to an existing MAC filter entry, if one was not assigned in the `config macfilter add` command by entering the `config macfilter ip-address mac_addr IP_addr` command.

- Verify that MAC addresses are assigned to the WLAN by entering the `show macfilter` command.

Note

If MAC filtering is configured, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local MAC filtering is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured.

Guidelines and Limitations

You must have AAA enabled on the WLAN to override the interface name.

Configuring a Timeout for Disabled Clients

You can configure a timeout for disabled clients. Clients who fail to authenticate three times when attempting to associate are automatically disabled from further association attempts. After the timeout period expires, the client is allowed to retry authentication until it associates or fails authentication and is excluded again. Use these commands to configure a timeout for disabled clients.

Configuring a Timeout for Disabled Clients (CLI)

- Configure the timeout for disabled clients by entering the `config wlan exclusionlist wlan_id timeout` command. Enter a timeout from 1 to 65535 seconds, or enter 0 to permanently disable the client.

- Verify the current timeout by entering the `show wlan` command.
Assigning WLANs to Interfaces

Use these commands to assign a WLAN to an interface:

- Assign a WLAN to an interface by entering this command:
  ```plaintext
  config wlan interface {wlan_id | foreignAp} interface_id
  ```
  - Use the `interface_id` option to assign the WLAN to a specific interface.
  - Use the `foreignAp` option to use a third-party access point.
- Verify the interface assignment status by entering the `show wlan summary` command.

Configuring the DTIM Period

This section contains the following topics:

- Information About the DTIM Period, page 8-18
- Guidelines and Limitations, page 8-19
- Configuring the DTIM Period, page 8-19

Information About the DTIM Period

In 802.11a/n and 802.11b/g/n networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Typically, the DTIM value is set to 1 (transmit broadcast and multicast frames after every beacon) or 2 (transmit after every other beacon). For instance, if the beacon period of the 802.11a/n or 802.11b/g/n network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames 5 times per second. Either of these settings may be suitable for applications, including VoIP, that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (transmit broadcast and multicast frames after every 255th beacon) if all 802.11a/n or 802.11b/g/n clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently, resulting in a longer battery life. For instance, if the beacon period is 100 ms and the DTIM value is set to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds, allowing the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, resulting in a longer battery life.

Note

A beacon period, which is specified in milliseconds on the controller, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. On Cisco’s 802.11n access points, this value is rounded to the nearest multiple of 17 TUs. Because of this, a configured beacon period of 100 ms, for example, will result in an actual beacon period of 104 ms.
Many applications cannot tolerate a long time between broadcast and multicast messages, which results in poor protocol and application performance. We recommend a low DTIM value for 802.11a/n and 802.11b/g/n networks that support such clients.

In controller software release 5.0 or later releases, you can configure the DTIM period for the 802.11a/n and 802.11b/g/n radio networks on specific WLANs. In previous software releases, the DTIM period was configured per radio network only, not per WLAN. The benefit of this change is that now you can configure a different DTIM period for each WLAN. For example, you might want to set different DTIM values for voice and data WLANs.

**Guidelines and Limitations**

When you upgrade the controller software to release 5.0 or later releases, the DTIM period that was configured for a radio network is copied to all of the existing WLANs on the controller.

**Configuring the DTIM Period**

This section contains the following topics:

- Configuring the DTIM Period (GUI), page 8-19
- Configuring the DTIM Period (CLI), page 8-19

**Configuring the DTIM Period (GUI)**

Step 1  Choose **WLANs** to open the WLANs page.

Step 2  Click the ID number of the WLAN for which you want to configure the DTIM period.

Step 3  Unselect the **Status** check box to disable the WLAN.

Step 4  Click **Apply** to commit your changes.

Step 5  Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 6  Under DTIM Period, enter a value between 1 and 255 (inclusive) in the 802.11a/n and 802.11b/g/n text boxes. The default value is 1 (transmit broadcast and multicast frames after every beacon).

Step 7  Click **Apply** to commit your changes.

Step 8  Choose the **General** tab to open the WLANs > Edit (General) page.

Step 9  Select the **Status** check box to reenable the WLAN.

Step 10  Click **Save Configuration** to save your changes.

**Configuring the DTIM Period (CLI)**

Step 1  Disable the WLAN by entering this command:

```
config wlan disable wlan_id
```

Step 2  Configure the DTIM period for either the 802.11a/n or 802.11b/g/n radio network on a specific WLAN by entering this command:

```
config wlan dtim {802.11a | 802.11b} dtim wlan_id
```
where dtim is a value between 1 and 255 (inclusive). The default value is 1 (transmit broadcast and multicast frames after every beacon).

**Step 3**  Reenable the WLAN by entering this command:

```
config wlan enable wlan_id
```

**Step 4**  Save your changes by entering this command:

```
save config
```

**Step 5**  Verify the DTIM period by entering this command:

```
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier.......................... 1
Profile Name................................. employee1
Network Name (SSID)......................... employee
Status...................................... Enabled

DTIM period for 802.11a radio............ 1
DTIM period for 802.11b radio............ 1
Local EAP Authentication................. Disabled
```

### Configuring Peer-to-Peer Blocking

This section contains the following topics:

- Information About Peer-to-Peer Blocking, page 8-20
- Guidelines and Limitations, page 8-21
- Configuring Peer-to-Peer Blocking, page 8-22

#### Information About Peer-to-Peer Blocking

In controller software releases prior to 4.2, peer-to-peer blocking is applied globally to all clients on all WLANs and causes traffic between two clients on the same VLAN to be transferred to the upstream VLAN rather than being bridged by the controller. This behavior usually results in traffic being dropped at the upstream switch because switches do not forward packets out the same port on which they are received.

In controller software release 4.2 or later releases, peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. In software release 4.2 or later releases, you also have more control over how traffic is directed. For example, you can choose to have traffic bridged locally within the controller, dropped by the controller, or forwarded to the upstream VLAN. Figure 8-1 shows each option.
In controller release 7.2 and later releases, peer-to-peer blocking is supported for clients associated with local switching WLAN. Per WLAN, peer-to-peer configuration is pushed by the controller to FlexConnect AP.

**Guidelines and Limitations**

- In controller software releases prior to 4.2, the controller forwards Address Resolution Protocol (ARP) requests upstream (just like all other traffic). In controller software release 4.2 or later releases, ARP requests are directed according to the behavior set for peer-to-peer blocking.
- Peer-to-peer blocking does not apply to multicast traffic.
- If you upgrade to controller software release 4.2 or later releases from a previous release that supports global peer-to-peer blocking, each WLAN is configured with the peer-to-peer blocking action of forwarding traffic to the upstream VLAN.
- In FlexConnect, solution peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all FlexConnect APs that broadcast the SSID.
- Unified solution for central switching clients supports peer-to-peer upstream-forward. However, this is not supported in the FlexConnect solution. This is treated as peer-to-peer drop and client packets are dropped.
- Unified solution for central switching clients supports peer-to-peer blocking for clients associated with different APs. However, this solution targets only clients connected to the same AP. FlexConnect ACLs can be used as a workaround for this limitation.
Configuring Peer-to-Peer Blocking

This section contains the following topics:

- Configuring Peer-to-Peer Blocking (GUI), page 8-22
- Configuring Peer-to-Peer Blocking (CLI), page 8-22

Configuring Peer-to-Peer Blocking (GUI)

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose WLANs to open the WLANs page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the ID number of the WLAN for which you want to configure peer-to-peer blocking.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the Advanced tab to open the WLANs &gt; Edit (Advanced) page.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose one of the following options from the P2P Blocking drop-down list:</td>
</tr>
<tr>
<td></td>
<td>Disabled—Disables peer-to-peer blocking and bridges traffic locally within the controller whenever possible. This is the default value.</td>
</tr>
<tr>
<td></td>
<td>Note Traffic is never bridged across VLANs in the controller.</td>
</tr>
<tr>
<td></td>
<td>Drop—Causes the controller to discard the packets.</td>
</tr>
<tr>
<td></td>
<td>Forward-UpStream—Causes the packets to be forwarded on the upstream VLAN. The device above the controller decides what action to take regarding the packets.</td>
</tr>
<tr>
<td></td>
<td>Note To enable peer-to-peer blocking on a WLAN configured for FlexConnect local switching, select Drop from the P2P Blocking drop-down list and select the FlexConnect Local Switching check box.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Apply to commit your changes.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Save Configuration to save your changes.</td>
</tr>
</tbody>
</table>

Configuring Peer-to-Peer Blocking (CLI)

| Step 1 | Configure a WLAN for peer-to-peer blocking by entering this command: config wlan peer-blocking {disable | drop | forward-upstream} wlan_id |
| Note   | See the description of each parameter in the “Configuring Peer-to-Peer Blocking (GUI)” section above. |
| Step 2 | Save your changes by entering this command: save config |
| Step 3 | See the status of peer-to-peer blocking for a WLAN by entering this command: show wlan wlan_id |
|        | Information similar to the following appears:
Configuring Layer 2 Security

This section contains the following topics:

- Configuring Static WEP Keys (CLI), page 8-23
- Configuring Dynamic 802.1X Keys and Authorization (CLI), page 8-23

Configuring Static WEP Keys (CLI)

Controllers can control static WEP keys across access points. Use these commands to configure static WEP for WLANs:

- Disable the 802.1X encryption by entering this command:
  
  ```
  config wlan security 802.1X disable wlan_id
  ```

- Configure 40/64-bit or 104/128-bit WEP keys by entering this command:
  
  ```
  config wlan security static-wep-key encryption wlan_id {40 | 104} {hex | ascii} key key_index
  ```

  - Use the **40** or **104** option to specify 40/64-bit or 104/128-bit encryption. The default setting is 104/128.
  - Use the **hex** or **ascii** option to specify the character format for the WEP key.
  - Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F) or five printable ASCII characters for 40-bit/64-bit WEP keys or enter 26 hexadecimal or 13 ASCII characters for 104-bit/128-bit keys.
  - Enter a key index (sometimes called a **key slot**). The default value is 0, which corresponds to a key index of 1; the valid values are 0 to 3 (key index of 1 to 4).

Configuring Dynamic 802.1X Keys and Authorization (CLI)

Controllers can control 802.1X dynamic WEP keys using Extensible Authentication Protocol (EAP) across access points and support 802.1X dynamic key settings for WLANs.

Note

To use LEAP with lightweight access points and wireless clients, make sure to choose **Cisco-Aironet** as the RADIUS server type when configuring the CiscoSecure Access Control Server (ACS).

- Check the security settings of each WLAN by entering this command:
  
  ```
  show wlan wlan_id
  ```
The default security setting for new WLANs is 802.1X with dynamic keys enabled. To maintain robust Layer 2 security, leave 802.1X configured on your WLANs.

- Disable or enable the 802.1X authentication by entering this command:
  ```
  config wlan security 802.1X {enable | disable} wlan_id
  ```

  After you enable 802.1X authentication, the controller sends EAP authentication packets between the wireless client and the authentication server. This command allows all EAP-type packets to be sent to and from the controller.

- Change the 802.1X encryption level for a WLAN by entering this command:
  ```
  config wlan security 802.1X encryption wlan_id [0 | 40 | 104]
  ```

  - Use the `0` option to specify no 802.1X encryption.
  - Use the `40` option to specify 40/64-bit encryption.
  - Use the `104` option to specify 104/128-bit encryption. (This is the default encryption setting.)

### Configuring a WLAN for Both Static and Dynamic WEP

This section contains the following topics:

- Information About WLAN for Both Static and Dynamic WEP, page 8-24
- WPA1 and WPA2, page 8-24
- Guidelines and Limitations, page 8-25

### Information About WLAN for Both Static and Dynamic WEP

You can configure up to four WLANs to support static WEP keys, and you can also configure dynamic WEP on any of these static-WEP WLANs. Follow these guidelines when configuring a WLAN for both static and dynamic WEP:

- The static WEP key and the dynamic WEP key must be the same length.
- When you configure both static and dynamic WEP as the Layer 2 security policy, no other security policies can be specified. That is, you cannot configure web authentication. However, when you configure either static or dynamic WEP as the Layer 2 security policy, you can configure web authentication.

### WPA1 and WPA2

Wi-Fi Protected Access (WPA or WPA1) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA1 is compatible with the IEEE 802.11i standard but was implemented prior to the standard’s ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard.

By default, WPA1 uses Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Both WPA1 and WPA2 use 802.1X for authenticated key management by default. However, these options are also available:
• **802.1X**—The standard for wireless LAN security, as defined by IEEE, is called 802.1X for 802.11, or simply 802.1X. An access point that supports 802.1X acts as the interface between a wireless client and an authentication server, such as a RADIUS server, to which the access point communicates over the wired network. If 802.1X is selected, only 802.1X clients are supported.

• **PSK**—When you choose PSK (also known as WPA preshared key or WPA passphrase), you need to configure a preshared key (or a passphrase). This key is used as the pairwise master key (PMK) between the clients and the authentication server.

• **CCKM**—Cisco Centralized Key Management (CCKM) uses a fast rekeying technique that enables clients to roam from one access point to another without going through the controller, typically in under 150 milliseconds (ms). CCKM reduces the time required by the client to mutually authenticate with the new access point and derive a new session key during reassociation. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications such as wireless Voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions. CCKM is a CCXv4-compliant feature. If CCKM is selected, only CCKM clients are supported.

When CCKM is enabled, the behavior of access points differs from the controller’s for fast roaming in the following ways:

- If an association request sent by a client has CCKM enabled in a Robust Secure Network Information Element (RSN IE) but CCKM IE is not encoded and only PMKID is encoded in RSN IE, then the controller does not do a full authentication. Instead, the controller validates the PMKID and does a four-way handshake.

- If an association request sent by a client has CCKM enabled in RSN IE but CCKM IE is not encoded and only PMKID is encoded in RSN IE, then AP does a full authentication. The access point does not use PMKID sent with the association request when CCKM is enabled in RSN IE.

• **802.1X+CCKM**—During normal operation, 802.1X-enabled clients mutually authenticate with a new access point by performing a complete 802.1X authentication, including communication with the main RADIUS server. However, when you configure your WLAN for 802.1X and CCKM fast secure roaming, CCKM-enabled clients securely roam from one access point to another without the need to reauthenticate to the RADIUS server. 802.1X+CCKM is considered optional CCKM because both CCKM and non-CCKM clients are supported when this option is selected.

On a single WLAN, you can allow WPA1, WPA2, and 802.1X/PSK/CCKM/802.1X+CCKM clients to join. All of the access points on such a WLAN advertise WPA1, WPA2, and 802.1X/PSK/CCKM/802.1X+CCKM information elements in their beacons and probe responses. When you enable WPA1 and/or WPA2, you can also enable one or two ciphers, or cryptographic algorithms, designed to protect data traffic. Specifically, you can enable AES and/or TKIP data encryption for WPA1 and/or WPA2. TKIP is the default value for WPA1, and AES is the default value for WPA2.

---

**Guidelines and Limitations**

- The OEAP 600 series does not support fast roaming for clients. Dual mode voice clients will experience reduced call quality when they roam between the two spectrums on OEAP602 access point. We recommend that you configure voice devices to only connect on one band, either 2.4 GHz or 5.0 GHz.
• The 4.2 or later release of controller software supports CCX versions 1 through 5. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to limit client functionality. Clients must support CCXv4 or v5 in order to use CCKM. See the “Configuring Cisco Client Extensions” section on page 8-57 for more information on CCX.

**Configuring WPA1 + WPA2**

This section contains the following topics:

- Configuring WPA1+WPA2 (GUI), page 8-26
- Configuring WPA1+WPA2 (CLI), page 8-27

**Configuring WPA1+WPA2 (GUI)**

**Step 1** Choose WLANs to open the WLANs page.

**Step 2** Click the ID number of the desired WLAN to open the WLANs > Edit page.

**Step 3** Choose the **Security** and **Layer 2** tabs to open the WLANs > Edit (Security > Layer 2) page.

**Step 4** Choose WPA+WPA2 from the Layer 2 Security drop-down list.

**Step 5** Under WPA+WPA2 Parameters, select the **WPA Policy** check box to enable WPA1, select the **WPA2 Policy** check box to enable WPA2, or select both check boxes to enable both WPA1 and WPA2.

**Note** The default value is disabled for both WPA1 and WPA2. If you leave both WPA1 and WPA2 disabled, the access points advertise in their beacons and probe responses information elements only for the authentication key management method that you choose in **Step 7**.

**Step 6** Select the **AES** check box to enable AES data encryption or the **TKIP** check box to enable TKIP data encryption for WPA1, WPA2, or both. The default values are TKIP for WPA1 and AES for WPA2.

**Step 7** Choose one of the following key management methods from the Auth Key Mgmt drop-down list: 802.1X, CCKM, PSK, or 802.1X+CCKM.

**Note** Cisco OEAP 600 does not support CCKM. You must choose either 802.1X or PSK.

**Note** For Cisco OEAP 600, the TKIP and AES security encryption settings must be identical for WPA and WPA2.

**Step 8** If you chose PSK in **Step 7**, choose **ASCII** or **HEX** from the PSK Format drop-down list and then enter a preshared key in the blank text box. WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
Note: The PSK parameter is a set-only parameter. The value set for the PSK key is not visible to the user for security reasons. For example, if you selected HEX as the key format when setting the PSK key, and later when you view the parameters of this WLAN, the value shown is the default value. The default is ASCII.

Step 9: Click **Apply** to commit your changes.
Step 10: Click **Save Configuration** to save your changes.

### Configuring WPA1+WPA2 (CLI)

**Step 1** Disable the WLAN by entering this command:
```plaintext
config wlan disable wlan_id
```

**Step 2** Enable or disable WPA for the WLAN by entering this command:
```plaintext
config wlan security wpa {enable | disable} wlan_id
```

**Step 3** Enable or disable WPA1 for the WLAN by entering this command:
```plaintext
config wlan security wpa wpa1 {enable | disable} wlan_id
```

**Step 4** Enable or disable WPA2 for the WLAN by entering this command:
```plaintext
config wlan security wpa wpa2 {enable | disable} wlan_id
```

**Step 5** Enable or disable AES or TKIP data encryption for WPA1 or WPA2 by entering one of these commands:
```
- config wlan security wpa wpa1 ciphers {aes | tkip} {enable | disable} wlan_id
- config wlan security wpa wpa2 ciphers {aes | tkip} {enable | disable} wlan_id
```

The default values are TKIP for WPA1 and AES for WPA2.

**Step 6** Enable or disable 802.1X, PSK, or CCKM authenticated key management by entering this command:
```plaintext
config wlan security wpa akm {802.1X | psk | cckm} {enable | disable} wlan_id
```

The default value is 802.1X.

**Step 7** If you enabled PSK in **Step 6**, enter this command to specify a preshared key:
```plaintext
config wlan security wpa akm psk set-key {ascii | hex} psk-key wlan_id
```

WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

**Step 8** If you enabled WPA2 with 802.1X authenticated key management or WPA1 or WPA2 with CCKM authenticated key management, the PMK cache lifetime timer is used to trigger reauthentication with the client when necessary. The timer is based on the timeout value received from the AAA server or the WLAN session timeout setting. To see the amount of time remaining before the timer expires, enter this command:
```
show pmk-cache all
```

Information similar to the following appears:

<table>
<thead>
<tr>
<th>PMK-CCKM Cache</th>
<th>Type</th>
<th>Station</th>
<th>Entry</th>
<th>Lifetime</th>
<th>VLAN Override</th>
<th>IP Override</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
If you enabled WPA2 with 80.1X authenticated key management, the controller supports opportunistic PMKID caching but not sticky (or non-opportunistic) PMKID caching. In sticky PMKID caching, the client stores multiple PMKIDs. This approach is not practical because it requires full authentication for each new access point and is not guaranteed to work in all conditions. In contrast, opportunistic PMKID caching stores only one PMKID per client and is not subject to the limitations of sticky PMK caching.

**Step 9**
Enable the WLAN by entering this command:
```
config wlan enable wlan_id
```

**Step 10**
Save your settings by entering this command:
```
save config
```

## Configuring Sticky PMKID Caching

This section contains:
- Information About Sticky PMKID Caching
- Guidelines and Limitations
- Configuring Sticky PMKID Caching (CLI)

### Information About Sticky PMKID Caching

Beginning in Release 7.2 and later releases, the controller supports Sticky PMKID Caching (SKC). With sticky PMKID caching, the client receives and stores a different PMKID for every AP it associates with. The APs also maintain a database of the PMKID issued to the client.

In SKC the client stores each Pairwise Master Key (PMK) identifier (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has the PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs. For SKC, PMKSA is a per AP cache that the client stores and PMKSA is precalculated based on the BSSID of the new AP.

### Guidelines and Limitations

- The controller supports SKC for up to eight APs per client. If a client roams to more than 8 APs per session, the old APs are removed to store the newly cached entries when the client roams. We recommend that you do not use SKC for large scale deployments.
- SKC does not work across controllers in a mobility group.
- SKC works only on WPA2-enabled WLANs.
- SKC works only on local mode APs.

### Configuring Sticky PMKID Caching (CLI)

**Step 1**
Disable the WLAN by entering this command:
config wlan disable wlan_id

Step 2
Enable Sticky PMKIDCaching by entering this command:
config wlan security wpa wpa2 cache sticky enable wlan_id

By default, Sticky PMKID Caching (SKC) is disabled and Opportunistic PMKID caching (OKC) is enabled.

Note
SKC works only on WPA2 enabled WLANs.

You can check if SKC is enabled by entering this command:
show wlan wlan_id

Information similar to the following appears:

WLAN Identifier.......................... 2
Profile Name.............................. new
Network Name (SSID)...................... new
Status...................................... Disabled
MAC Filtering............................. Disabled
Security
802.11 Authentication.................. Open System
Static WEP Keys......................... Disabled
802.1X.................................... Disabled
Wi-Fi Protected Access (WPA/WPA2)..... Enabled
WPA (SSN IE)............................ Disabled
WPA2 (RSN IE).......................... Enabled
TKIP Cipher............................. Disabled
AES Cipher............................. Enabled
Auth Key Management
802.1x.................................... Disabled
PSK...................................... Enabled
CCM........................................ Disabled
FT(802.11r).............................. Disabled
FT-PSK(802.11r)......................... Disabled
SKC Cache Support...................... Enabled
FT Reassociation Timeout.............. 20
FT Over-The-Air mode................... Enabled
FT Over-The-Ds mode.................... Enabled
CCM tcf Tolerance........................ 1000
Wi-Fi Direct policy configured........ Disabled
EAP-Passthrough......................... Disabled

Step 3
Enable the WLAN by entering this command:
config wlan enable wlan_id

Step 4
Save your settings by entering this command:
save config

Configuring CKIP

This section contains the following topics:
- Information About CKIP, page 8-30
- Configuring CKIP, page 8-30
Information About CKIP

Cisco Key Integrity Protocol (CKIP) is a Cisco-proprietary security protocol for encrypting 802.11 media. CKIP improves 802.11 security in infrastructure mode using key permutation, a message integrity check (MIC), and a message sequence number. Software release 4.0 or later releases support CKIP with a static key. For this feature to operate correctly, you must enable Aironet information elements (IEs) for the WLAN.

A lightweight access point advertises support for CKIP in beacon and probe response packets by adding an Aironet IE and setting one or both of the CKIP negotiation bits (key permutation and multi-modular hash message integrity check [MMH MIC]). Key permutation is a data encryption technique that uses the basic encryption key and the current initialization vector (IV) to create a new key. MMH MIC prevents bit-flip attacks on encrypted packets by using a hash function to compute message integrity code.

The CKIP settings specified in a WLAN are mandatory for any client attempting to associate. If the WLAN is configured for both CKIP key permutation and MMH MIC, the client must support both. If the WLAN is configured for only one of these features, the client must support only the CKIP feature. CKIP requires that 5-byte and 13-byte encryption keys be expanded to 16-byte keys. The algorithm to perform key expansion occurs at the access point. The key is appended to itself repeatedly until the length reaches 16 bytes. All lightweight access points support CKIP.

Configuring CKIP

This section contains the following topics:

- Configuring CKIP (GUI), page 8-30
- Configuring CKIP (CLI), page 8-31

Configuring CKIP (GUI)

Step 1  Choose WLANs to open the WLANs page.
Step 2  Click the ID number of the desired WLAN to open the WLANs > Edit page.
Step 3  Choose the Advanced tab.
Step 4  Select the Aironet IE check box to enable Aironet IEs for this WLAN and click Apply.
Step 5  Choose the General tab.
Step 6  Unselect the Status check box, if selected, to disable this WLAN and click Apply.
Step 7  Choose the Security and Layer 2 tabs to open the WLANs > Edit (Security > Layer 2) page.
Figure 8-2 WLANs > Edit (Security > Layer 2) Page

![Cisco Wireless LAN Controller Configuration Guide](image)

Step 8 Choose CKIP from the Layer 2 Security drop-down list.

Step 9 Under CKIP Parameters, choose the length of the CKIP encryption key from the Key Size drop-down list. The range is Not Set, 40 bits, or 104 bits and the default is Not Set.

Step 10 Choose the number to be assigned to this key from the Key Index drop-down list. You can configure up to four keys.

Step 11 From the Key Format drop-down list, choose ASCII or HEX and then enter an encryption key in the Encryption Key text box. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.

Step 12 Select the MMH Mode check box to enable MMH MIC data protection for this WLAN. The default value is disabled (or unselected).

Step 13 Select the Key Permutation check box to enable this form of CKIP data protection. The default value is disabled (or unselected).

Step 14 Click Apply to commit your changes.

Step 15 Choose the General tab.

Step 16 Select the Status check box to enable this WLAN.

Step 17 Click Apply to commit your changes.

Step 18 Click Save Configuration to save your changes.

---

### Configuring CKIP (CLI)

**Step 1** Disable the WLAN by entering this command:

```bash
config wlan disable wlan_id
```

**Step 2** Enable Aironet IEs for this WLAN by entering this command:

```bash
config wlan ccx aironet-ie enable wlan_id
```

**Step 3** Enable or disable CKIP for the WLAN by entering this command:

```bash
config wlan security ckip {enable | disable} wlan_id
```
Chapter 8 Working with WLANs

Configuring WLANs

Step 4 Specify a CKIP encryption key for the WLAN by entering this command:
```
config wlan security ckip akm psk set-key wlan_id {40 | 104} {hex | ascii} key key_index
```

Step 5 Enable or disable CKIP MMH MIC for the WLAN by entering this command:
```
config wlan security ckip mmh-mic {enable | disable} wlan_id
```

Step 6 Enable or disable CKIP key permutation for the WLAN by entering this command:
```
config wlan security ckip kp {enable | disable} wlan_id
```

Step 7 Enable the WLAN by entering this command:
```
config wlan enable wlan_id
```

Step 8 Save your settings by entering this command:
```
save config
```

Configuring Session Timeouts

The session timeout is the maximum time for a client session to remain active before requiring reauthorization. This section contains the following topics:

- Configuring a Session Timeout (GUI), page 8-32
- Configuring a Session Timeout (CLI), page 8-32

Configuring a Session Timeout (GUI)

Step 1 Choose WLANs to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to assign a session timeout.

Step 3 When the WLANs > Edit page appears, choose the Advanced tab. The WLANs > Edit (Advanced) page appears.

Step 4 Select the Enable Session Timeout check box to configure a session timeout for this WLAN. Otherwise, unselect the check box. The default value is selected.

In the Session Timeout text box, enter a value between 300 and 86400 seconds to specify the duration of the client session. The default value is 1800 seconds for the following Layer 2 security types: 802.1X, Static WEP+802.1X, WPA+WPA2 with 802.1X, CCKM, or 802.1X+CCKM authentication key management and 0 seconds for all other Layer 2 security types (Open WLAN/CKIP/Static WEP). A value of 0 is equivalent to no timeout.

Step 5 Click Apply to commit your changes.

Step 6 Click Save Configuration to save your changes.

Configuring a Session Timeout (CLI)

Step 1 Configure a session timeout for wireless clients on a WLAN by entering this command:
```
config wlan session-timeout wlan_id timeout
```
The default value is 1800 seconds for the following Layer 2 security types: 802.1X, Static WEP+802.1X, WPA+WPA2 with 802.1X, CCKM, or 802.1X+CCKM authentication key management and 0 seconds for all other Layer 2 security types (Open WLAN/CKIP/Static WEP). A value of 0 is equivalent to no timeout.

**Step 2** Save your changes by entering this command:

```
save config
```

**Step 3** See the current session timeout value for a WLAN by entering this command:

```
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier................................. 9
Profile Name..................................... test12
Network Name (SSID)............................ test12
...                                      
Number of Active Clients..................... 0
Exclusionlist Timeout......................... 60 seconds
Session Timeout............................... 1800 seconds
...                                      
```

### Configuring Layer 3 Security Using Web Authentication

This section contains the following topics:

- Information About Web Authentication, page 8-33
- Guidelines and Limitations, page 8-33
- Configuring Web Authentication, page 8-34

### Information About Web Authentication

WLANs can use web authentication only if VPN passthrough is not enabled on the controller. Web authentication is simple to set up and use and can be used with SSL to improve the overall security of the WLAN.

### Guidelines and Limitations

- Web authentication is supported only with these Layer 2 security policies: open authentication, open authentication+WEP, and WPA-PSK. It is not supported for use with 802.1X.
- To initiate HTTP/HTTPS web authentication redirection, always use only HTTP URL and not HTTPS URL.
- If the CPU ACLs are configured to block HTTP / HTTPS traffic, after the successful web login authentication, there could be a failure in the redirection page.
- Before enabling web authentication, make sure that all proxy servers are configured for ports other than port 53.
When you enable web authentication for a WLAN, a message appears indicating that the controller forwards DNS traffic to and from wireless clients prior to authentication. We recommend that you have a firewall or intrusion detection system (IDS) behind your guest VLAN to regulate DNS traffic and to prevent and detect any DNS tunneling attacks.

If the web authentication is enabled on the WLAN and you also have the CPU ACL rules, the client-based web authentication rules take higher precedence as long as the client is unauthenticated (in the webAuth_Reqd state). Once the client goes to the RUN state, the CPU ACL rules get applied. Therefore, if the CPU ACL rules are enabled in the controller, an allow rule for the virtual interface IP is required (in any direction) with the following conditions:

- When the CPU ACL does not have an allow ACL rule for both directions.
- When an allow ALL rule exists, but also a DENY rule for port 443 or 80 of higher precedence.

The allow rule for the virtual IP should be for TCP protocol and port 80 (if secureweb is disabled) or port 443 (if secureweb is enabled). This process is required to allow client’s access to the virtual interface IP address, post successful authentication when the CPU ACL rules are in place.

When clients connect to a WebAuth SSID and a preauthorization ACL configured to allow VPN users, the clients will get disconnected from the SSID every few minutes. Webauth SSIDs must not connect without authenticating on the web page.

Special characters are not supported in the username field for web-authentication.

You can select the following identity stores to authenticate web-auth user, under WLANs > Security > AAA servers > Authentication priority order for web-auth user section:

- Local
- RADIUS
- LDAP

If multiple identity stores are selected, then the controller checks each identity store in the list, in the order specified, from top to bottom, until authentication for the user succeeds. The authentication fails, if the controller reaches the end of the list and user remains un-authenticated in any of the identity stores.

For more information on using web authentication, see Chapter 12, “Managing User Accounts.”

**Configuring Web Authentication**

This section contains the following topics:

- Configuring the Web Authentication (GUI), page 8-34
- Configuring the Web Authentication (CLI), page 8-35

**Configuring the Web Authentication (GUI)**

**Step 1** Choose WLANs to open the WLANs page.

**Step 2** Click the ID number of the WLAN for which you want to configure web authentication. The WLANs > Edit page appears.

**Step 3** Choose the Security and Layer 3 tabs to open the WLANs > Edit (Security > Layer 3) page.

**Step 4** Select the Web Policy check box.

**Step 5** Make sure that the Authentication option is selected.

**Step 6** Click Apply to commit your changes.
Step 7  
Click **Save Configuration** to save your settings.

## Configuring the Web Authentication (CLI)

**Step 1**  
Enable or disable web authentication on a particular WLAN by entering this command:

```
config wlan security web-auth {enable | disable} wlan_id
```

**Step 2**  
Release the guest user IP address when the web authentication policy timer expires and prevent the guest user from acquiring an IP address for 3 minutes by entering this command:

```
config wlan webauth-exclude wlan_id {enable | disable}
```

The default value is disabled. This command is applicable when you configure the internal DHCP scope on the controller. By default, when the web authentication timer expires for a guest user, the user can immediately reassociate to the same IP address before another guest user can acquire it. If there are many guest users or limited IP addresses in the DHCP pool, some guest users might not be able to acquire an IP address.

When you enable this feature on the guest WLAN, the guest user’s IP address is released when the web authentication policy timer expires and the guest user is excluded from acquiring an IP address for 3 minutes. The IP address is available for another guest user to use. After 3 minutes, the excluded guest user can reassociate and acquire an IP address, if available.

**Step 3**  
See the status of web authentication by entering this command:

```
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier...................... 1
Profile Name.......................... cj
Network Name (SSID).................. cj
Status................................ Disabled
MAC Filtering......................... Disabled
Broadcast SSID........................ Enabled
AAA Policy Override.................. Disabled
Network Admission Control
NAC-State.............................. Disabled
Quarantine VLAN...................... 0
Number of Active Clients............. 0
Exclusionlist Timeout............... 60 seconds
Session Timeout...................... 1800 seconds
CHD per WLAN......................... Enabled
Webauth DHCP exclusion.............. Disabled
Interface.................. management
WLAN ACL............................. unconfigured
DHCP Server......................... Default
DHCP Address Assignment Required.. Disabled
...  
Web Based Authentication............ Disabled
Web-Passthrough...................... Disabled
...  
```
### Configuring Captive Bypassing

#### Information about Captive Bypassing

WISPr is a draft protocol that enables users to roam between different wireless service providers. Some devices (for example, Apple iOS devices) have a mechanism using which they can determine if the device is connected to Internet, based on an HTTP WISPr request made to a designated URL. This mechanism is used to allow users to launch the web browser if they need to provide credentials to access Internet, and the actual authentication is done in the background every time the device connects to a new SSID.

This HTTP request triggers a webauth interception in the controller as any other page requests are performed by a wireless client. This interception leads to a webauth process, which will be completed normally. If the webauth is being used with any of the controller splash page features (URL provided by a configured RADIUS server), the splash page may never be displayed because the WISPr requests are made at very short intervals, and as soon as one of the queries is able to reach the designated server, any web redirection or splash page display process that is performed in the background is aborted, and the device processes the page request, thus breaking the splash page functionality.

For example, Apple introduced an iOS feature to facilitate network access when captive portals are present. This feature detects the presence of captive portal by sending a web request upon connecting to a wireless network, and directs the request to http://www.apple.com/library/test/success.html. If a response is received, then the internet access is assumed to be available and no further interaction is required. If no response is received, then the internet access is assumed to be blocked by captive portal and Apple’s Captive Network Assistant (CNA) auto-launches the pseudo browser to request portal login in a controlled window.

The CNA may break when redirecting to an ISE captive portal.

Cisco Wireless Lan Controller 7.2 prevents this pseudo browser from popping up. You can now configure the controller to bypass WISPr detection process, so the webauth interception is only done when a user requests a webpage leading to splash page load in user context, without the WISPr detection being performed in the background.

#### Configuring Captive Bypassing

**Configuring Captive Bypassing (CLI)**

- `config network web-auth captive-bypass {enable | disable}`—Enables or disables the controller to support bypass of captive portals at the network level.
- `show network summary`—Displays the status for the WISPr protocol detection feature.

#### Configuring a Fallback Policy with MAC Filtering and Web Authentication

This section contains the following topics:

- Information About Fallback Policy with MAC Filtering and Web Authentication, page 8-37
- Configuring a Fallback Policy with MAC Filtering and Web Authentication, page 8-37
Information About Fallback Policy with MAC Filtering and Web Authentication

You can configure a fallback policy mechanism that combines Layer 2 and Layer 3 security. In a scenario where you have both MAC filtering and web authentication implemented, when a client tries to connect to a WLAN using the MAC filter (RADIUS server), if the client fails the authentication, you can configure the authentication to fall back to web authentication. When a client passes the MAC filter authentication, the web authentication is skipped and the client is connected to the WLAN. With this feature, you can avoid disassociations based on only a MAC filter authentication failure.

Configuring a Fallback Policy with MAC Filtering and Web Authentication

This section contains the following topics:
- Configuring a Fallback Policy with MAC Filtering and Web Authentication (GUI), page 8-37
- Configuring a Fallback Policy with MAC Filtering and Web Authentication (CLI), page 8-38

Configuring a Fallback Policy with MAC Filtering and Web Authentication (GUI)

Note
Before configuring a fallback policy, you must have MAC filtering enabled. To know more about how to enable MAC filtering, see the “Configuring MAC Filtering for WLANs” section on page 8-16.

Step 1
Choose WLANs to open the WLANs page.

Step 2
Click the ID number of the WLAN for which you want to configure the fallback policy for web authentication. The WLANs > Edit page appears.

Step 3
Choose the Security and Layer 3 tabs to open the WLANs > Edit (Security > Layer 3) page.

Step 4
From the Layer 3 Security drop-down list, choose None.

Step 5
Select the Web Policy check box.

Note
The controller forwards DNS traffic to and from wireless clients prior to authentication.

The following options are displayed:
- Authentication
- Passthrough
- Conditional Web Redirect
- Splash Page Web Redirect
- On MAC Filter Failure

Step 6
Click On MAC Filter Failure.

Step 7
Click Apply to commit your changes.

Step 8
Click Save Configuration to save your settings.
Configuring a Fallback Policy with MAC Filtering and Web Authentication (CLI)

**Note**  
Before configuring a fallback policy, you must have MAC filtering enabled. To know more about how to enable MAC filtering, see the “Configuring MAC Filtering for WLANs” section on page 8-16.

### Step 1

Enable or disable web authentication on a particular WLAN by entering this command:

```
config wlan security web-auth on-macfilter-failure wlan-id
```

### Step 2

See the web authentication status by entering this command:

```
show wlan wlan-id
```

FT Over-The-Ds mode.............................. Enabled

ACL............................................. Unconfigured

Web Authentication server precedence:

1............................................... local
2............................................... radius
3............................................... ldap

Assigning a QoS Profile to a WLAN

This section contains the following topics:

- Information About QoS Profiles, page 8-38
- Assigning QoS Profiles, page 8-39

**Information About QoS Profiles**

Cisco UWN solution WLANs support four levels of QoS: Platinum/Voice, Gold/Video, Silver/Best Effort (default), and Bronze/Background. You can configure the voice traffic WLAN to use Platinum QoS, assign the low-bandwidth WLAN to use Bronze QoS, and assign all other traffic between the remaining QoS levels.

The WLAN QoS level defines a specific 802.11e user priority (UP) for over-the-air traffic. This UP is used to derive the over-the-wire priorities for non-WMM traffic, and it also acts as the ceiling when managing WMM traffic with various levels of priorities. The access point uses this QoS-profile-specific UP in accordance with the values in Table 8-1 to derive the IP DSCP value that is visible on the wired LAN.

<table>
<thead>
<tr>
<th>AVVID Traffic Type</th>
<th>AVVID IP DSCP</th>
<th>QoS Profile</th>
<th>AVVID 802.1p</th>
<th>IEEE 802.11e UP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network control</td>
<td>56 (CS7)</td>
<td>Platinum</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Inter-network control</td>
<td>48 (CS6)</td>
<td>Platinum</td>
<td>6</td>
<td>7</td>
</tr>
</tbody>
</table>

(CAPWAP control, 802.11 management)
### Assigning QoS Profiles

This section contains the following topics:
- Assigning a QoS Profile to a WLAN (GUI), page 8-39
- Assigning a QoS Profile to a WLAN (CLI), page 8-40

#### Assigning a QoS Profile to a WLAN (GUI)

If you have not already done so, configure one or more QoS profiles using the instructions in the “Configuring QoS Profiles (GUI)” section on page 4-66.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose WLANs to open the WLANs page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the ID number of the WLAN to which you want to assign a QoS profile.</td>
</tr>
<tr>
<td>Step 3</td>
<td>When the WLANs &gt; Edit page appears, choose the QoS tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the Quality of Service (QoS) drop-down list, choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Platinum (voice)</td>
</tr>
<tr>
<td></td>
<td>• Gold (video)</td>
</tr>
<tr>
<td></td>
<td>• Silver (best effort)</td>
</tr>
<tr>
<td></td>
<td>• Bronze (background)</td>
</tr>
<tr>
<td>Note</td>
<td>Silver (best effort) is the default value.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Apply to commit your changes.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Save Configuration to save your changes.</td>
</tr>
</tbody>
</table>

---

**Table 8-1 Access Point QoS Translation Values (continued)**

<table>
<thead>
<tr>
<th>AVVID Traffic Type</th>
<th>AVVID IP DSCP</th>
<th>QoS Profile</th>
<th>AVVID 802.1p</th>
<th>IEEE 802.11e UP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>46 (EF)</td>
<td>Platinum</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Interactive video</td>
<td>34 (AF41)</td>
<td>Gold</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Mission critical</td>
<td>26 (AF31)</td>
<td>Gold</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Transactional</td>
<td>18 (AF21)</td>
<td>Silver</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Bulk data</td>
<td>10 (AF11)</td>
<td>Bronze</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Best effort</td>
<td>0 (BE)</td>
<td>Silver</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Scavenger</td>
<td>2</td>
<td>Bronze</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

---

**Note**

The IEEE 802.11e UP 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.
Assigning a QoS Profile to a WLAN (CLI)

If you have not already done so, configure one or more QoS profiles using the instructions in the “Configuring QoS Profiles (CLI)” section on page 4-68.

Step 1
Assign a QoS profile to a WLAN by entering this command:
```
cfg wlan qos wlan_id {bronze | silver | gold | platinum}
```
Silver is the default value.

Step 2
Save your changes by entering this command:
```
save config
```

Step 3
Verify that you have properly assigned the QoS profile to the WLAN by entering this command:
```
show wlan wlan_id
```
Information similar to the following appears:

<table>
<thead>
<tr>
<th>WLAN Identifier</th>
<th>Profile Name</th>
<th>Network Name (SSID)</th>
<th>Status</th>
<th>MAC Filtering</th>
<th>Broadcast SSID</th>
<th>AAA Policy Override</th>
<th>Number of Active Clients</th>
<th>Exclusionlist</th>
<th>Session Timeout</th>
<th>Interface</th>
<th>WLAN ACL</th>
<th>DHCP Server</th>
<th>DHCP Address Assignment Required</th>
<th>Quality of Service</th>
<th>WMM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>test</td>
<td>test</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>0</td>
<td>Disabled</td>
<td>0</td>
<td>management</td>
<td>unconfigured</td>
<td>1.100.163.24</td>
<td>Disabled</td>
<td>Silver (best effort)</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Configuring QoS Enhanced BSS

This section contains the following topics:

- Information About QoS Enhanced BSS, page 8-40
- Guidelines and Limitations, page 8-41
- Configuring QBSS, page 8-42

Information About QoS Enhanced BSS

The QoS Enhanced Basis Service Set (QBSS) information element (IE) enables the access points to communicate their channel usage to wireless devices. Because access points with high channel usage might not be able to handle real-time traffic effectively, the 7921 or 7920 phone uses the QBSS value to determine if they should associate to another access point. You can enable QBSS in these two modes:

- Wi-Fi Multimedia (WMM) mode, which supports devices that meet the 802.11E QBSS standard (such as Cisco 7921 IP Phones)
• 7920 support mode, which supports Cisco 7920 IP Phones on your 802.11b/g network

The 7920 support mode has two options:

- Support for 7920 phones that require call admission control (CAC) to be configured on and advertised by the client device (these are typically older 7920 phones)
- Support for 7920 phones that require CAC to be configured on and advertised by the access point (these are typically newer 7920 phones)

When access point-controlled CAC is enabled, the access point sends out a Cisco proprietary CAC Information Element (IE) and does not send out the standard QBSS IE.

Guidelines and Limitations

• The OEAP 600 Series access points do not support CAC.
• QBSS is disabled by default.
• 7920 phones are non-WMM phones with limited CAC functionality. The phones look at the channel utilization of the access point to which they are associated and compare that to a threshold that is beaconed by the access point. If the channel utilization is less than the threshold, the 7920 places a call. In contrast, 7921 phones are full-fledged WMM phones that use traffic specifications (TSPECs) to gain access to the voice queue before placing a phone call. The 7921 phones work well with load-based CAC, which uses the percentage of the channel set aside for voice and tries to limit the calls accordingly.

Because 7921 phones support WMM and 7920 phones do not, capacity and voice quality problems can arise if you do not properly configure both phones when they are used in a mixed environment. To enable both 7921 and 7920 phones to co-exist on the same network, make sure that load-based CAC and 7920 AP CAC are both enabled on the controller and the WMM Policy is set to Allowed. These settings become particularly important if you have many more 7920 users than 7921 users.

Additional Guidelines for Using Cisco 7921 and 7920 Wireless IP Phones

Follow these guidelines to use Cisco 7921 and 7920 Wireless IP Phones with controllers:

• Aggressive load balancing must be disabled for each controller. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.
• The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the `config 802.11b dtpc enable` command. The DTPC IE is a beacon and probe information element that allows the access point to broadcast information on its transmit power. The 7921 or 7920 phone uses this information to automatically adjust its transmit power to the same level as the access point to which it is associated. In this manner, both devices are transmitting at the same level.
• Both the 7921 and 7920 phones and the controllers support Cisco Centralized Key Management (CCKM) fast roaming.
• When configuring WEP, there is a difference in nomenclature for the controller and the 7921 or 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7921 or 7920.
• For standalone 7921 phones, load-based CAC must be enabled, and the WMM Policy must be set to Required on the WLAN.
• The controller supports traffic classification (TCLAS) coming from 7921 phones using firmware version 1.1.1. This feature ensures proper classification of voice streams to the 7921 phones.
• When using a 7921 phone with the 802.11a radio of a 1242 series access point, set the 24-Mbps data rate to Supported and choose a lower Mandatory data rate (such as 12 Mbps). Otherwise, the phone might experience poor voice quality.
See Chapter 4, “Configuring Controller Settings,” for more information and configuration instructions for load-based CAC.

Configuring QBSS

This section contains the following topics:

- Configuring QBSS (GUI), page 8-42
- Configuring QBSS (CLI), page 8-42

Configuring QBSS (GUI)

**Step 1** Choose **WLANs** to open the WLANs page.

**Step 2** Click the ID number of the WLAN for which you want to configure WMM mode.

**Step 3** When the WLANs > Edit page appears, choose the **QoS** tab to open the WLANs > Edit (Qos) page.

**Step 4** From the WMM Policy drop-down list, choose one of the following options, depending on whether you want to enable WMM mode for 7921 phones and other devices that meet the WMM standard:

- **Disabled**—Disables WMM on the WLAN. This is the default value.
- **Allowed**—Allows client devices to use WMM on the WLAN.
- **Required**—Requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

**Step 5** Select the **7920 AP CAC** check box if you want to enable 7920 support mode for phones that require access point-controlled CAC. The default value is unselected.

**Step 6** Select the **7920 Client CAC** check box if you want to enable 7920 support mode for phones that require client-controlled CAC. The default value is unselected.

**Note** You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

**Step 7** Click **Apply** to commit your changes.

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

Configuring QBSS (CLI)

**Step 1** Determine the ID number of the WLAN to which you want to add QBSS support by entering this command:

```
show wlan summary
```

**Step 2** Disable the WLAN by entering this command:

```
config wlan disable wlan_id
```

**Step 3** Configure WMM mode for 7921 phones and other devices that meet the WMM standard by entering this command:

```
config wlan wmm {disabled | allowed | required} wlan_id
```

where
Chapter 8      Working with WLANs

Configuring Captive Bypassing

- **disabled** disables WMM mode on the WLAN.
- **allowed** allows client devices to use WMM on the WLAN.
- **required** requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

**Step 4** Enable or disable 7920 support mode for phones that require client-controlled CAC by entering this command:

```
config wlan 7920-support client-cac-limit {enable | disable} wlan_id
```

**Note** You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

**Step 5** Enable or disable 7920 support mode for phones that require access point-controlled CAC by entering this command:

```
config wlan 7920-support ap-cac-limit {enable | disable} wlan_id
```

**Step 6** Reenable the WLAN by entering this command:

```
config wlan enable wlan_id
```

**Step 7** Save your changes by entering this command:

```
save config
```

**Step 8** Verify that the WLAN is enabled and the Dot11-Phone Mode (7920) text box is configured for compact mode by entering this command:

```
show wlan wlan_id
```

---

**Configuring Media Session Snooping and Reporting**

This section contains the following topics:

- **Information About Media Session Snooping and Reporting**, page 8-43
- **Guidelines and Limitations**, page 8-44
- **Configuring Media Session Snooping**, page 8-44

**Information About Media Session Snooping and Reporting**

This feature enables access points to detect the establishment, termination, and failure of Session Initiation Protocol (SIP) voice calls and then report them to the controller and WCS. VoIP snooping and reporting can be enabled or disabled for each WLAN.

When VoIP MSA snooping is enabled, the access point radios that advertise this WLAN look for SIP voice packets that comply with SIP RFC 3261. They do not look for non-RFC 3261-compliant SIP voice packets or Skinny Call Control Protocol (SCCP) voice packets. Any SIP packets destined to or originating from port number 5060 (the standard SIP signaling port) are considered for further inspection. The access points track when Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, are already on an active call, or are in the process of ending a call. Upstream packet classification for both client types occurs at the access point. Downstream packet classification occurs at the controller for WMM clients and at the access point for non-WMM clients. The access points notify the controller and WCS of any major call events, such as call establishment, termination, and failure.
The controller provides detailed information for VoIP MSA calls. For failed calls, the controller generates a trap log with a timestamp and the reason for failure (in the GUI) and an error code (in the CLI) to aid in troubleshooting. For successful calls, the controller shows the number and duration of calls for usage tracking purposes. WCS displays failed VoIP call information in the Events page.

Guidelines and Limitations

Controller software release 6.0 or later releases support Voice over IP (VoIP) Media Session Aware (MSA) snooping and reporting.

Configuring Media Session Snooping

This section contains the following topics:

- Configuring Media Session Snooping (GUI), page 8-44
- Configuring Media Session Snooping (CLI), page 8-44

Configuring Media Session Snooping (GUI)

Step 1 Choose WLANs to open the WLANs page.
Step 2 Click the ID number of the WLAN for which you want to configure media session snooping.
Step 3 On the WLANs > Edit page, click the Advanced tab.
Step 4 Under Voice, select the Media Session Snooping check box to enable media session snooping or unselect it to disable this feature. The default value is unselected.
Step 5 Click Apply to commit your changes.
Step 6 Click Save Configuration to save your changes.
Step 7 See the VoIP statistics for your access point radios as follows:
   a. Choose Monitor > Access Points > Radios > 802.11a/n or 802.11b/g/n to open the 802.11a/n (or 802.11b/g/n) Radios page.
   b. Scroll to the right and click the Detail link for the access point for which you want to view VoIP statistics. The Radio > Statistics page appears.

   The VoIP Stats section shows the cumulative number and length of voice calls for this access point radio. Entries are added automatically when voice calls are successfully placed and deleted when the access point disassociates from the controller.

Step 8 Choose Management > SNMP > Trap Logs to see the traps generated for failed calls. The Trap Logs page appears.

   For example, log 0 shows that a call failed. The log provides the date and time of the call, a description of the failure, and the reason why the failure occurred.

Configuring Media Session Snooping (CLI)

Step 1 Enable or disable VoIP snooping for a particular WLAN by entering this command:

   config wlan call-snoop {enable | disable} wlan_id

Step 2 Save your changes by entering this command:
save config

Step 3
See the status of media session snooping on a particular WLAN by entering this command:

```
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier................................. 1
Profile Name...................................... wpa2-psk
Network Name (SSID)........................... wpa2-psk
Status........................................... Enabled
...
FlexConnect Local Switching.................. Disabled
FlexConnect Learn IP Address............... Enabled
Infrastructure MFP protection............. Enabled (Global Infrastructure MFP Disabled)
Client MFP........................................ Optional
Tkip MIC Countermeasure Hold-down Timer... 60
Call Snooping.................................. Enabled
```

Step 4
See the call information for an MSA client when media session snooping is enabled and the call is active by entering this command:

```
show call-control client callInfo client_MAC_address
```

Information similar to the following appears:

```
Uplink IP/port.................................. 192.11.1.71 / 23870
Downlink IP/port.............................. 192.12.1.47 / 2070
UP.................................................. 6
Calling Party..................................... sip:1054
Called Party...................................... sip:1000
Call ID........................................... 58635b00-850161b7-14853-1501a8
Number of calls for given client is......... 1
```

Step 5
See the metrics for successful calls or the traps generated for failed calls by entering this command:

```
show call-control ap {802.11a | 802.11b} Cisco_AP {metrics | traps}
```

Information similar to the following appears when you enter `show call-control ap {802.11a | 802.11b} Cisco_AP metrics`:

```
Total Call Duration in Seconds.................. 120
Number of Calls.................................. 10
```

Information similar to the following appears when you enter `show call-control ap {802.11a | 802.11b} Cisco_AP traps`:

```
Number of traps sent in one min................ 2
Last SIP error code.............................. 404
Last sent trap timestamp...................... Jun 20 10:05:06
```

To aid in troubleshooting, the output of this command shows an error code for any failed calls. Table 8-2 explains the possible error codes for failed calls.

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Integer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>unknown</td>
<td>Unknown error.</td>
</tr>
<tr>
<td>400</td>
<td>badRequest</td>
<td>The request could not be understood because of malformed syntax.</td>
</tr>
<tr>
<td>401</td>
<td>unauthorized</td>
<td>The request requires user authentication.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Integer</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>402</td>
<td>paymentRequired</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td>403</td>
<td>forbidden</td>
<td>The server understood the request but refuses to fulfill it.</td>
</tr>
<tr>
<td>404</td>
<td>notFound</td>
<td>The server has information that the user does not exist at the domain specified in the Request-URI.</td>
</tr>
<tr>
<td>405</td>
<td>methodNotAllowed</td>
<td>The method specified in the Request-Line is understood but not allowed for the address identified by the Request-URI.</td>
</tr>
<tr>
<td>406</td>
<td>notAcceptable</td>
<td>The resource identified by the request is only capable of generating response entities with content characteristics that are not acceptable according to the Accept header text box sent in the request.</td>
</tr>
<tr>
<td>407</td>
<td>proxyAuthenticationRequired</td>
<td>The client must first authenticate with the proxy.</td>
</tr>
<tr>
<td>408</td>
<td>requestTimeout</td>
<td>The server could not produce a response within a suitable amount of time, if it could not determine the location of the user in time.</td>
</tr>
<tr>
<td>409</td>
<td>conflict</td>
<td>The request could not be completed due to a conflict with the current state of the resource.</td>
</tr>
<tr>
<td>410</td>
<td>gone</td>
<td>The requested resource is no longer available at the server, and no forwarding address is known.</td>
</tr>
<tr>
<td>411</td>
<td>lengthRequired</td>
<td>The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.</td>
</tr>
<tr>
<td>413</td>
<td>requestEntityTooLarge</td>
<td>The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.</td>
</tr>
<tr>
<td>414</td>
<td>requestURITooLarge</td>
<td>The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.</td>
</tr>
<tr>
<td>415</td>
<td>unsupportedMediaType</td>
<td>The server is refusing to service the request because the message body of the request is in a format not supported by the server for the requested method.</td>
</tr>
<tr>
<td>420</td>
<td>badExtension</td>
<td>The server did not understand the protocol extension specified in a Proxy-Require or Require header text box.</td>
</tr>
<tr>
<td>480</td>
<td>temporarilyNotAvailable</td>
<td>The callee’s end system was contacted successfully, but the callee is currently unavailable.</td>
</tr>
<tr>
<td>481</td>
<td>callLegDoesNotExist</td>
<td>The UAS received a request that does not match any existing dialog or transaction.</td>
</tr>
<tr>
<td>482</td>
<td>loopDetected</td>
<td>The server has detected a loop.</td>
</tr>
<tr>
<td>483</td>
<td>tooManyHops</td>
<td>The server received a request that contains a Max-Forwards header text box with the value zero.</td>
</tr>
</tbody>
</table>
Configuring Captive Bypassing

If you experience any problems with media session snooping, enter the `debug call-control {all | event} {enable | disable}` command to debug all media session snooping messages or events.

### Table 8-2 Error Codes for Failed VoIP Calls (continued)

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Integer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>484</td>
<td>addressIncomplete</td>
<td>The server received a request with a Request-URI that was incomplete.</td>
</tr>
<tr>
<td>485</td>
<td>ambiguous</td>
<td>The Request-URI was ambiguous.</td>
</tr>
<tr>
<td>486</td>
<td>busy</td>
<td>The end system of the callee was contacted successfully, but the callee is currently not willing or able to take additional calls at this end system.</td>
</tr>
<tr>
<td>500</td>
<td>internalServerError</td>
<td>The server encountered an unexpected condition that prevented it from fulfilling the request.</td>
</tr>
<tr>
<td>501</td>
<td>notImplemented</td>
<td>The server does not support the functionality required to fulfill the request.</td>
</tr>
<tr>
<td>502</td>
<td>badGateway</td>
<td>The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.</td>
</tr>
<tr>
<td>503</td>
<td>serviceUnavailable</td>
<td>The server is temporarily unable to process the request because of a temporary overloading or maintenance of the server.</td>
</tr>
<tr>
<td>504</td>
<td>serverTimeout</td>
<td>The server did not receive a timely response from an external server it accessed in attempting to process the request.</td>
</tr>
<tr>
<td>505</td>
<td>versionNotSupported</td>
<td>The server does not support or refuses to support the SIP protocol version that was used in the request.</td>
</tr>
<tr>
<td>600</td>
<td>busyEverywhere</td>
<td>The callee’s end system was contacted successfully, but the callee is busy or does not want to take the call at this time.</td>
</tr>
<tr>
<td>603</td>
<td>decline</td>
<td>The callee’s machine was contacted successfully, but the user does not want to or cannot participate.</td>
</tr>
<tr>
<td>604</td>
<td>doesNotExistAnywhere</td>
<td>The server has information that the user indicated in the Request-URI does not exist anywhere.</td>
</tr>
<tr>
<td>606</td>
<td>notAcceptable</td>
<td>The user’s agent was contacted successfully, but some aspects of the session description (such as the requested media, bandwidth, or addressing style) were not acceptable.</td>
</tr>
</tbody>
</table>

### Configuring Key Telephone System-Based CAC

This section contains the following topics:
Key Telephone System (KTS) based CAC is a protocol that is used in NEC MH240 wireless IP telephones. You can configure the controller to support CAC on KTS-based SIP clients, to process bandwidth request message from such clients, to allocate the required bandwidth on the AP radio, and to handle other messages that are part of the protocol.

When a call is initiated, the KTS-based CAC client sends a Bandwidth Request message to which the controller responds with a Bandwidth Confirm message indicating whether the bandwidth is allocated or not. The call is allowed only if the bandwidth is available. If the client roams from one AP to another, the client sends another Bandwidth Request message to the controller.

Bandwidth allocation depends on the median time calculated using the data rate from the Bandwidth Request message and the packetization interval. For KTS-based CAC clients, the G.711 codec with 20 milliseconds as the packetization interval is used to compute the medium time.

The controller releases the bandwidth after it receives the bandwidth release message from the client. When the client roams to another AP, the controller releases the bandwidth on the previous AP and allocates bandwidth on the new AP, in both intracontroller and intercontroller roaming scenarios. The controller releases the bandwidth if the client is dissociated or if there is inactivity for 120 seconds. The controller does not inform the client when the bandwidth is released for the client due to inactivity or dissociation of the client.

Guidelines and Limitations

- The controller ignores the SSID Capability Check Request message from the clients.
- Preferred call is not supported for KTS CAC clients.
- Reason code 17 is not supported in intercontroller roaming scenarios.
- To make the KTS-based CAC feature functional, ensure that you do the following:
  - Enable WMM on the WLAN
  - Enable ACM at the radio level
  - Enable processing of TSPEC inactivity timeout at the radio level

Configuring KTS-based CAC (GUI)

This section contains the following topics:

- Configuring KTS-based CAC (GUI), page 8-48
- Configuring KTS-based CAC (CLI), page 8-49

Configuring KTS-based CAC (CLI)

Prerequisites

To enable KTS-based CAC for a WLAN, ensure that you do the following:
• Set the QoS profile for the WLAN to Platinum (see the “Assigning QoS Profiles” section on page 8-39).
• Set the WLAN in disabled state (see the “Enabling and Disabling WLANs (GUI)” section on page 8-4).
• Set the FlexConnect Local Switching in disabled state for the WLAN (On the WLANs > Edit page, click the Advanced tab and unselect the FlexConnect Local Switching check box).

---

**Step 1** Choose WLANs to open the WLANs page.
**Step 2** Click the ID number of the WLAN for which you want to configure the KTS-based CAC policy.
**Step 3** On the WLANs > Edit page, click the Advanced tab.
**Step 4** Under Voice, select or unselect the KTS based CAC Policy check box to enable or disable KTS-based CAC for the WLAN.
**Step 5** Click Apply to commit your changes.

---

### Configuring KTS-based CAC (CLI)

**Prerequisites**
To enable KTS-based CAC for a WLAN, ensure that you do the following:

- Configure the QoS profile for the WLAN to Platinum by entering the following command:
  ```
  config wlan qos wlan-id platinum
  ```
- Disable the WLAN by entering the following command:
  ```
  config wlan disable wlan-id
  ```
- Disable FlexConnect Local Switching for the WLAN by entering the following command:
  ```
  config wlan flexconnect local-switching wlan-id disable
  ```

**Step 1** Enable KTS-based CAC for a WLAN by entering this command:
  ```
  config wlan kts-cac enable wlan-id
  ```

**Step 2** Enable the KTS-based CAC feature by doing the following:
  a. Enable WMM on the WLAN by entering this command:
     ```
     config wlan wmm allow wlan-id
     ```
  b. Enable ACM at the radio level by entering this command:
     ```
     config 802.11a cac voice acm enable
     ```
  c. Enable processing of the TSPEC inactivity timeout at the radio level by entering this command:
     ```
     config 802.11a cac voice tspec-inactivity-timeout enable
     ```

**Related Commands**

- See whether the client supports KTS-based CAC by entering the following command:
  ```
  show client detail client-mac-address
  ```
Information similar to the following appears:

Client MAC Address............................... 00:60:b9:0d:ef:26
Client Username ................................. N/A
AP MAC Address................................... 58:bc:27:93:79:90

QoS Level............................................ Platinum
802.1P Priority Tag.............................. disabled
KTS CAC Capability............................... Yes
WMM Support....................................... Enabled
Power Save........................................ ON

- Troubleshoot issues with KTS-based CAC by entering the following command:
  `debug cac kts enable`
- Troubleshoot other issues related to CAC, by entering the following commands:
  - `debug cac event enable`
  - `debug call-control all enable`

### Configuring Reanchoring of Roaming Voice Clients

This section contains the following topics:

- **Information About Reanchoring of Roaming Voice Clients**, page 8-50
- **Guidelines and Limitations**, page 8-50
- **Configuring Reanchoring of Roaming Voice Clients**, page 8-50

#### Information About Reanchoring of Roaming Voice Clients

You can allow voice clients to get anchored on the best suited and nearest available controller, which is useful when intercontroller roaming occurs. By using this feature, you can avoid the use of tunnels to carry traffic between the foreign controller and the anchor controller and remove unnecessary traffic from the network.

The ongoing call during roaming is not affected and can continue without any problem. The traffic passes through proper tunnels that are established between the foreign controller and the anchor controller. Disassociation occurs only after the call ends, and then the client then gets reassociated to a new controller.

#### Guidelines and Limitations

- The ongoing data session might be affected due to disassociation and then reassociation.
- This feature is supported for TSPEC-based calls and non-TSPEC SIP-based calls only when you enable the admission control.
- You can reanchor roaming of voice clients for each WLAN.
- This feature is not recommended for use on Cisco 792x phones.

#### Configuring Reanchoring of Roaming Voice Clients

This section contains the following topics:
Chapter 8  Working with WLANs

Configuring Captive Bypassing

- Configuring Reanchoring of Roaming Voice Clients (GUI), page 8-51
- Configuring Reanchoring of Roaming Voice Clients (CLI), page 8-51

Configuring Reanchoring of Roaming Voice Clients (GUI)

**Step 1**  Choose WLANs to open the WLANs page.

**Step 2**  Click the ID number of the WLAN for which you want to configure reanchoring of roaming voice clients.

**Step 3**  When the WLANs > Edit page appears, choose the Advanced tab to open the WLANs > Edit (Advanced) page.

**Step 4**  In the Voice area select the Re-anchor Roamed Clients check box.

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

**Step 6**  Click Save Configuration to save your changes.

Configuring Reanchoring of Roaming Voice Clients (CLI)

**Step 1**  Enable or disable reanchoring of roaming voice clients for a particular WLAN by entering this command:

```
config wlan roamed-voice-client re-anchor {enable | disable} wlan_id
```

**Step 2**  Save your changes by entering this command:

```
save config
```

**Step 3**  See the status of reanchoring roaming voice client on a particular WLAN by entering this command:

```
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier.......................... 1
Profile Name............................... wpa2-psk
Network Name (SSID)....................... wpa2-psk
Status...................................... Enabled
...
Call Snooping.............................. Enabled
Roamed Call Re-Anchor Policy............. Enabled
Band Select............................... Disabled
Load Balancing........................... Disabled
```

**Step 4**  Save your changes by entering this command:

```
save config
```

Configuring Seamless IPv6 Mobility

This section contains the following topics:

- Information About IPv6 Mobility, page 8-52
- Guidelines and Limitations, page 8-52
**Information About IPv6 Mobility**

Internet Protocol version 6 (IPv6) is the next-generation network layer Internet protocol intended to replace version 4 (IPv4) in the TCP/IP suite of protocols. This new version increases the Internet global address space to accommodate users and applications that require unique global IP addresses. IPv6 incorporates 128-bit source and destination addresses, which provide significantly more addresses than the 32-bit IPv4 addresses.

To support IPv6 clients across controllers, ICMPv6 messages must be dealt with specially to ensure the IPv6 client remains on the same Layer 3 network. The controllers keep track of IPv6 clients by intercepting the ICMPv6 messages to provide seamless mobility and protect the network from network attacks. The NDP (Neighbor Discovery Packets) packets are converted from multicast to unicast and delivered individually per client. This unique solution ensures that Neighbor Discovery and Router Advertisement packets are not leaked across VLANs. Clients can receive specific Neighbor Discovery and Router Advertisement packets ensuring correct IPv6 addressing and avoids unnecessary multicast traffic.

The configuration for IPv6 mobility is the same as IPv4 mobility and requires no separate software on the client side to achieve seamless roaming. The controllers must be part of the same mobility group. Both IPv4 and IPv6 client mobility are enabled by default.

**Guidelines and Limitations**

- Up to 16 client addresses can be tracked per client.
- Clients must support IPv6 with either static stateless auto configuration (such as Windows XP clients) or stateful DHCPv6 IP addressing (such as Windows Vista clients).

>**Note** Currently, DHCPv6 is supported for use only with Windows Vista clients. For these clients, you must manually renew the DHCPv6 IP address after the client changes VLANs.

>**Note** The dynamic VLAN function for IPv6 is not supported on the controller software releases 6.0 and 7.0.

- To allow stateful DHCPv6 IP addressing to operate properly, you must have a switch or router that supports the DHCP for IPv6 feature (such as the Catalyst 3750 switch) that is configured to act like a DHCPv6 server, or you need a dedicated server such as a Windows 2008 server with a built-in DHCPv6 server.

>**Note** To load the SDM IPv6 template in the Catalyst 3750 switch, enter the `sdm prefer dual-ipv4-and-v6 default` command and then reset the switch. For more information, see *Catalyst 3750 Switch Configuration Guide for Cisco IOS Release 12.2(46)SE*.

To support the seamless IPv6 Mobility, you might need to configure the following:

- Configuring RA Guard for IPv6 Clients, page 8-53
- Configuring RA Throttling for IPv6 Clients, page 8-53
- Configuring IPv6 Neighbor Discovery Caching, page 8-55
Configuring RA Guard for IPv6 Clients

This section contains the following topics:
- Information About RA Guard, page 8-53
- Configuring RA Guard (GUI), page 8-53
- Configuring RA Guard (CLI), page 8-53

Information About RA Guard

IPv6 clients configure IPv6 addresses and populate their router tables based on IPv6 Router Advertisement (RA) packets. The RA guard feature is similar to the RA guard feature of wired networks. RA guard increases the security of the IPv6 network by dropping the unwanted or rogue RA packets that come from wireless clients. If this feature is not configured, malicious IPv6 clients could announce themselves as the router for the network often with high priority, which would take higher precedence over legitimate IPv6 routers.

RA guard occurs at the controller. You can configure the controller to drop RA messages at the access point or at the controller. By default, RA guard is configured at the access point and also enabled in the controller. All IPv6 RA messages are dropped, which protects other wireless clients and upstream wired network from malicious IPv6 clients.

Configuring RA Guard (GUI)

Step 1 Choose Controller > IPv6 > RA Guard to open the IPv6 RA Guard page. By default, the IPv6 RA Guard on AP is enabled.

Step 2 From the drop-down list, select Disable if you want to disable RA guard. The controller also displays the clients that have been identified as sending RA packets.

Step 3 Click Apply to commit your changes.

Step 4 Click Save Configuration to save your changes.

Configuring RA Guard (CLI)

- config ipv6 ra-guard ap {enable | disable}

Configuring RA Throttling for IPv6 Clients

This section contains the following topics:
- Information about RA Throttling, page 8-54
- Configuring RA Throttling (GUI), page 8-54
- Configuring RA Throttle Policy (CLI), page 8-54
Information about RA Throttling

RA throttling allows the controller to enforce limits to RA packets headed toward the wireless network. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. If a client sends an RS packet, an RA is sent back to the client. This RA is allowed through the controller and unicast to the client. This process ensures that the new clients or roaming clients are not affected by the RA throttling.

Configuring RA Throttling (GUI)

Step 1 Choose **Controller > IPv6 > RA Throttle Policy** page. By default the IPv6 RA Throttle Policy is enabled.

Step 2 Unselect the check box to disable RA throttle policy.

Step 3 Configure the following parameters:

- **Throttle period**—The period of time for throttling. RA throttling takes place only after the Max Through limit is reached for the VLAN or the Allow At-Most value is reached for a particular router. The range is from 10 seconds to 86400 seconds. The default is 600 seconds.

- **Max Through**—The maximum number of RA packets on a VLAN that can be sent before throttling takes place. The No Limit option allows an unlimited number of RA packets through with no throttling. The range is from 0 to 256 RA packets. The default is 10 RA packets.

- **Interval Option**—Allows the controller to act differently based on the RFC 3775 value set in IPv6 RA packets.
  - **Passthrough**—Allows any RA messages with the RFC3775 interval option to go through without throttling.
  - **Ignore**—Causes the RA throttle to treat packets with the interval option as a regular RA and subject to throttling if in effect.
  - **Throttle**—Causes the RA packets with the interval option to always be subject to rate limiting.

- **Allow At-least**—The minimum number of RA packets per router that can be sent as multicast before throttling takes place. The range is from 0 to 32 RA packets.

- **Allow At-most**—The maximum number of RA packets per router that can be sent as multicast before throttling takes place. The No Limit option allows an unlimited number of RA packets through the router. The range is from 0 to 256 RA packets.

**Note** When RA throttling occurs, only the first IPv6 capable router is allowed through. For networks that have multiple IPv6 prefixes being served by different routers, you should disable RA throttling.

Step 4 Click **Apply** to commit your changes.

Step 5 Click **Save Configuration** to save your changes.

Configuring RA Throttle Policy (CLI)

- `config ipv6 neighbor-binding ra-throttle { allow at-least at-least-value | enable | disable | interval-option { ignore | passthrough | throttle } | max-through { max-through-value | no-limit } }`
Configuring IPv6 Neighbor Discovery Caching

This section contains the following topics:

- Information About IPv6 Neighbor Discovery, page 8-55
- Configuring Neighbor Binding Timers (GUI), page 8-55
- Configure Neighbor Binding Timers (CLI), page 8-55

Information About IPv6 Neighbor Discovery

IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes. Neighbor Discovery replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4.

IPv6 Neighbor Discovery inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery packets that do not comply are dropped. The neighbor binding table in the controller tracks each IPv6 address and its associated MAC address. Clients are expired from the table according to Neighbor Binding timers.

Configuring Neighbor Binding Timers (GUI)

**Step 1** Choose Controller > IPv6 > Neighbor Binding Timers page.

**Step 2** Configure the following Timers:

- **Down–Lifetime**—Specifies how long IPv6 cache entries are kept if the interface goes down. The range is from 0 to 86400 seconds.
- **Reachable–Lifetime**—Specifies how long IPv6 addresses are active. The range is from 0 to 86400 seconds.
- **Stale–Lifetime**—Specifies how long to keep IPv6 addresses in the cache. The range is from 0 to 86400 seconds.

**Note** It is recommended that you configure Reachable-lifetime as 3600 sec and Stale-Lifetime as 300 sec for optimal performance.

**Step 3** Click Apply to commit your changes.

**Step 4** Click Save Configuration to save your changes.

Configure Neighbor Binding Timers (CLI)

```
config ipv6 neighbor-binding timers {down-lifetime | reachable-lifetime | stale-lifetime} {enable | disable}
```
8-56

Cisco Wireless LAN Controller Configuration Guide

Chapter 8 Working with WLANs

Configuring Unknown Address NS Multicast Forwarding

The IPv6 addresses of wireless clients are cached by the controller. If the controller receives an NS multicast looking for an IPv6 address, which belongs to any of the wireless clients of the controller, the controller acts as the proxy and replies with the NA. If the controller does not have the IPv6 address of a wireless client, the controller would not respond with NA and would drop the NS packet. To resolve this issue, an NS Multicast Forwarding knob is provided. If this knob is enabled, the controller gets the NS packet for the IPv6 address that it does not have (cache miss), forwards the NS packet to the wireless side. This packet reaches the intended wireless client and the client replies with NA.

This cache miss scenario occurs rarely, and only very few clients which do not implement complete IPv6 stack may not advertise their IPv6 address during NDP.

Configuring NS Multicast Forwarding (CLI)

- Enter the following command to enable or disable NS multicast forwarding:

  ```
  config ipv6 ns-mcast-fwd {enable | disable}
  ```

  By default, NS multicast forwarding is disabled.

  When the NS multicast forwarding is enabled, the controller sends an NS multicast packet to all the wireless and wired clients. When the NS multicast forwarding is disabled, the controller sends an NS multicast packet to the wired side.

- Enter the following command to view the status of the NS multicast forwarding:

  ```
  show ipv6 summary
  ```

  Information similar to the following appears:

  ```
  Reachable-lifetime value.................... 86400
  Stale-lifetime value........................ 86400
  Down-lifetime value......................... 86400
  RA Throttling............................... Enabled
  RA Throttling allow at-least................. 2
  RA Throttling allow at-most................. no-limit
  RA Throttling max-through................... 10
  RA Throttling throttle-period.............. 12
  RA Throttling interval-option............. ignore
  NS Multicast CacheMiss Forwarding........... Disabled
  ```

- Enter the following command to view the NS multicast forwarding statistics:

  ```
  show ipv6 neighbor-binding counters
  ```

  Information similar to the following appears:

  ```
  ..............
  Cache Miss Statistics:

  Multicast NS Forward[1]
  Multicast NS Dropped[3]
  ```

  **Note**

  The Multicast NS Forward parameter is incremented when the knob is enabled. The Multicast NS Dropped parameter is incremented when the knob is disabled.
Configuring Cisco Client Extensions

This section contains the following topics;

- Information About Cisco Client Extensions, page 8-57
- Guidelines and Limitations, page 8-57
- Configuring CCX Aironet IEs, page 8-57

Information About Cisco Client Extensions

Cisco Client Extensions (CCX) software is licensed to manufacturers and vendors of third-party client devices. The CCX code resident on these clients enables them to communicate wirelessly with Cisco access points and to support Cisco features that other client devices do not, including those features related to increased security, enhanced performance, fast roaming, and superior power management.

Guidelines and Limitations

- The 4.2 or later releases of controller software support CCX versions 1 through 5, which enables controllers and their access points to communicate wirelessly with third-party client devices that support CCX. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. However, you can configure a specific CCX feature per WLAN. This feature is Aironet information elements (IEs).

- If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

- CCX is not supported on Cisco OEAP 600 access points and all elements related to CCX are not supported.

- Cisco OEAP 600 do not support Cisco Aeronet IEs.

- With the 7.2 release, a new version of CCX, which is called CCX Lite is available. For more information about CCX Lite, see http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html.

Configuring CCX Aironet IEs

This section contains the following topics;

- Configuring CCX Aironet IEs (GUI), page 8-57
- Viewing a Client’s CCX Version (GUI), page 8-58
- Configure CCX Aironet IEs (CLI), page 8-58
- Viewing a Client’s CCX Version (CLI), page 8-58

Configuring CCX Aironet IEs (GUI)

Step 1 Choose WLANs to open the WLANs page.
Step 2  Click the ID number of the desired WLAN to open the WLANs > Edit page.
Step 3  Choose the Advanced tab to open the WLANs > Edit (Advanced tab) page.
Step 4  Select the Aironet IE check box if you want to enable support for Aironet IEs for this WLAN. Otherwise, unselect this check box. The default value is enabled (or selected).
Step 5  Click Apply to commit your changes.
Step 6  Click Save Configuration to save your changes.

Viewing a Client's CCX Version (GUI)

A client device sends its CCX version in association request packets to the access point. The controller then stores the client's CCX version in its database and uses it to limit the features for this client. For example, if a client supports CCX version 2, the controller does not allow the client to use CCX version 4 features.

Step 1  Choose Monitor > Clients to open the Clients page.
Step 2  Click the MAC address of the desired client device to open the Clients > Detail page.
The CCX Version text box shows the CCX version supported by this client device. Not Supported appears if the client does not support CCX.
Step 3  Click Back to return to the previous screen.
Step 4  Repeat this procedure to view the CCX version supported by any other client devices.

Configure CCX Aironet IEs (CLI)

```
config wlan ccx aironet-ie {enable | disable} wlan_id
```

Note  The default value is enabled.

Viewing a Client's CCX Version (CLI)

See the CCX version supported by a particular client device using the controller CLI by entering this command:

```
show client detail client_mac
```

Configuring AP Groups

This section contains the following topics:

- Information About Access Point Groups, page 8-59
- Guidelines and Limitations, page 8-59
- Configuring Access Point Groups, page 8-60
Information About Access Point Groups

After you create up to 512 WLANs on the controller, you can selectively publish them (using access point groups) to different access points to better manage your wireless network. In a typical deployment, all users on a WLAN are mapped to a single interface on the controller. Therefore, all users associated with that WLAN are on the same subnet or VLAN. However, you can choose to distribute the load among several interfaces or to a group of users based on specific criteria such as individual departments (such as Marketing) by creating access point groups. Additionally, these access point groups can be configured in separate VLANs to simplify network administration.

In the example, three configured dynamic interfaces are mapped to three different VLANs (VLAN 61, VLAN 62, and VLAN 63). Three access point groups are defined, and each is a member of a different VLAN, but all are members of the same SSID. A client within the wireless SSID is assigned an IP address from the VLAN subnet on which its access point is a member. For example, any user that associates with an access point that is a member of access point group VLAN 61 is assigned an IP address from that subnet.

In the example, the controller internally treats roaming between access points as a Layer 3 roaming event. In this way, WLAN clients maintain their original IP addresses.

After all access points have joined the controller, you can create access point groups and assign up to 16 WLANs to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point does not advertise disabled WLANs in its access point group or WLANs that belong to another group.

Guidelines and Limitations

- The required access control list (ACL) must be defined on the router that serves the VLAN or subnet.
- Multicast traffic is supported with access point group VLANs. However, if the client roams from one access point to another, the client might stop receiving multicast traffic, unless IGMP snooping is enabled.
- The OEAP 600 Series access point supports a maximum of two WLANs and one remote LAN. If you have configured more than two WLANs and one remote LAN, you can assign the 600 Series access point to an AP group. The support for two WLANs and one remote LAN still applies to the AP group. If the 600 Series OEAP is in the default group, the WLAN/remote LAN ids must be lower than 8.
- 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 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.

Note

A controller with OfficeExtend access points in an access point group publishes up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID.

- You can create up to 300 access point groups for Cisco 4400 Series Controllers, Cisco WiSM, and 3750G wireless LAN controller switch; and up to 500 access point groups for Cisco 5500 Series Controllers.
Configuring Captive Bypassing

- All OfficeExtend access points should be in the same access point group, and that 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.
- If you clear the configuration on the controller, all of the access point groups disappear except for the default access point group “default-group,” which is created automatically.

Configuring Access Point Groups

**Step 1** Configure the appropriate dynamic interfaces and map them to the desired VLANs.

For example, to implement the network in Figure 7-23, create dynamic interfaces for VLANs 61, 62, and 63 on the controller. See Chapter 4, “Configuring Ports and Interfaces,” for information on how to configure dynamic interfaces.

**Step 2** Create the access point groups. See the “Creating Access Point Groups (GUI)” section on page 8-60.

**Step 3** Create a RF profile. See the “Creating an RF Profile (GUI)” section on page 8-65.

**Step 4** Assign access points to the appropriate access point groups. See the “Creating Access Point Groups (GUI)” section on page 8-60.

**Step 5** Apply the RF profile on the AP Groups. See the “Applying RF Profile to AP Groups (GUI)” section on page 8-65.

Creating Access Point Groups (GUI)

**Step 1** Choose WLANs > Advanced > AP Groups to open the AP Groups page.

This page lists all the access point groups currently created on the controller. By default, all access points belong to the default access point group “default-group,” unless you assign them to other access point groups.

**Note** When you upgrade to controller software release 5.2 or later releases, the controller creates the default-group access point group and automatically populates it with the first 16 WLANs (WLANs with IDs 1 through 16, or fewer if 16 WLANs are not configured). This default group cannot be modified (you cannot add WLANs to it or delete WLANs from it). It is dynamically updated whenever the first 16 WLANs are added or deleted. If an access point does not belong to an access point group, it is assigned to the default group and uses the WLANs in that group. If an access point joins the controller with an undefined access point group name, the access point keeps its group name but uses the WLANs in the default-group access point group.

**Step 2** Click Add Group to create a new access point group. The Add New AP Group section appears at the top of the page.

**Step 3** In the AP Group Name text box, enter the group’s name.

**Step 4** In the Description text box, enter the group’s description.

**Step 5** Click Add. The newly created access point group appears in the list of access point groups on the AP Groups page.
Note: If you ever want to delete this group, hover your cursor over the blue drop-down arrow for the group and choose Remove. An error message appears if you try to delete an access point group that is used by at least one access point. Before deleting an access point group in controller software release 6.0 or later releases, move all access points in the group to another group. The access points are not moved to the default-group access point group as in previous releases.

Step 6: Click the name of the group to edit this new group. The AP Groups > Edit (General) page appears.

Step 7: Change the description of this access point group by entering the new text in the AP Group Description text box and click Apply.

Step 8: Choose the WLANs tab to open the AP Groups > Edit (WLANs) page. This page lists the WLANs that are currently assigned to this access point group.

Step 9: Click Add New to assign a WLAN to this access point group. The Add New section appears at the top of the page.

Step 10: From the WLAN SSID drop-down list, choose the SSID of the WLAN.

Step 11: From the Interface Name drop-down list, choose the interface to which you want to map the access point group. Choose the quarantine VLAN if you plan to enable network admission control (NAC) out-of-band support.

Note: The interface name in the default-group access point group matches the WLAN interface.

Step 12: Select the NAC State check box to enable NAC out-of-band support for this access point group. To disable NAC out-of-band support, leave the check box unselected, which is the default value. See the “Configuring NAC Out-of-Band Integration” section on page 8-70 for more information on NAC.

Step 13: Click Add to add this WLAN to the access point group. This WLAN appears in the list of WLANs that are assigned to this access point group.

Note: If you ever want to remove this WLAN from the access point group, hover your cursor over the blue drop-down arrow for the WLAN and choose Remove.

Step 14: Repeat Step 9 through Step 13 to add any additional WLANs to this access point group.

Step 15: Choose the APs tab to assign access points to this access point group. The AP Groups > Edit (APs) page lists the access points that are currently assigned to this group as well as any access points that are available to be added to the group. If an access point is not currently assigned to a group, its group name appears as “default-group”.

Step 16: Select the check box to the left of the access point name and click Add APs to add an access point to this access point group. The access point now appears in the list of access points currently in this access point group.

Note: To select all of the available access points at once, select the AP Name check box. All of the access points are then selected.
### Configuring Captive Bypassing

Note If you ever want to remove an access point from the group, select the check box to the left of the access point name and click Remove APs. To select all of the access points at once, select the AP Name check box. All of the access points are then removed from this group.

Note If you ever want to change the access point group to which an access point belongs, choose Wireless > Access Points > All APs > ap_name > Advanced tab, choose the name of another access point group from the AP Group Name drop-down list, and click Apply.

**Step 17** Click Save Configuration to save your changes.

### Creating Access Point Groups (CLI)

**Step 1** Create an access point group by entering this command:

```
config wlan apgroup add group_name
```

Note To delete an access point group, enter the `config wlan apgroup delete group_name` command. An error message appears if you try to delete an access point group that is used by at least one access point. Before deleting an access point group in controller software release 6.0 or later releases, move all access points in the group to another group. The access points are not moved to the default-group access point group as in previous releases. To see the access points in a group, enter the `show wlan apgroups` command. To move the access points to another group, enter the `config ap group-name group_name Cisco_AP` command.

**Step 2** Add a description to an access point group by entering this command:

```
config wlan apgroup description group_name description
```

**Step 3** Assign a WLAN to an access point group by entering this command:

```
config wlan apgroup interface-mapping add group_name wlan_id interface_name
```

Note To remove a WLAN from an access point group, enter the `config wlan apgroup interface-mapping delete group_name wlan_id` command.

**Step 4** Enable or disable NAC out-of-band support for this access point group by entering this command:

```
config wlan apgroup nac {enable | disable} group_name wlan_id
```

**Step 5** Configure a WLAN radio policy on the access point group by entering this command:

```
config wlan apgroup wlan-radio-policy apgroup_name wlan_id {802.11a-only | 802.11bg | 802.11g-only | all}
```

**Step 6** Assign an access point to an access point group by entering this command:

```
config ap group-name group_name Cisco_AP
```
**Note**

To remove an access point from an access point group, reenter this command and assign the access point to another group.

**Step 7**

Save your changes by entering this command:

```
save config
```

**Viewing Access Point Groups (CLI)**

To view information about or to troubleshoot access point groups, use these commands:

- See a list of all access point groups on the controller by entering this command:

  ```
  show wlan apgroups
  ```

  Information similar to the following appears:

  ```
  Site Name................................. AP2
  Site Description........................ Access Point 2
  WLAN ID       Interface       Network Admission Control
  --------       -----------        --------------------------
  1     management     Disabled
  2     management     Disabled
  3     management     Disabled
  4     management     Disabled
  9     management     Disabled
  10    management     Disabled
  11    management     Disabled
  12    management     Disabled
  13    management     Disabled
  14    management     Disabled
  15    management     Disabled
  16    management     Disabled
  18    management     Disabled
  ```

- See the BSSIDs for each WLAN assigned to an access point group by entering this command:

  ```
  show ap wlan {802.11a | 802.11b} Cisco_AP
  ```

  Information similar to the following appears:

  ```
  Site Name................................. AP3
  Site Description........................ Access Point 3
  WLAN ID       Interface       BSSID
  --------       -----------        -------------------
  10    management   00:14:1b:58:14:df
  ```

- See the number of WLANs enabled for an access point group by entering this command:

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

  Information similar to the following appears:

  ```
  Cisco AP Identifier.............................. 166
  ```
Configuring RF Profiles

This section contains the following topics:

- Information About RF Profiles, page 8-64
- Guidelines and Limitations, page 8-64
- Configuring RF Profiles, page 8-65

Information About RF Profiles

RF profiles allow you to tune groups of APs that share a common coverage zone together and selectively change how RRM operates the APs within that coverage zone.

For example, a university might deploy a high density of APs, in an area with a high number of users. This situation requires that you manipulate both data rates and power to address the cell density while managing the co-channel interference. In adjacent areas, normal coverage is provided and such manipulation would result in a loss of coverage.

Using RF profiles and AP groups allow you to optimize the RF settings for AP groups that operate in different environments or coverage zones. RF profiles are created for 802.11b/g/n or 802.11a/n radios. RF profiles are applied to all APs that belong to an AP group, where all APs in that group will have the same profile settings.

The RF profile gives you control over the data rates and power (TPC) values.

The application of an RF profile does not change the AP’s status in RRM. It is still in global configuration mode controlled by RRM.

An AP that has a custom power setting applied for AP power is not in global configuration mode, an RF profile has no effect on this AP. For RF profiling to work, all APs must have their channel and power managed by RRM.

Guidelines and Limitations

Once you create an AP group and apply RF profiles or modify an existing AP group, the new settings are in effect and the following rules apply:

- The same RF profile must be applied and present on every controller of the AP group or the action will fail for that controller.
• Once you assign an RF profile to an AP group you cannot make changes to that RF profile. You must
change the AP group RF profile settings to none in order to change the RF profile and then add it
back to the AP group. You can also work around this restriction by disabling the network that will
be affected by the changes that you will be making, either for 802.11a or 802.11b.
• You can assign the same RF profile to more than one AP group.
• Within the AP group, changing the assignment of an RF profile on either band causes the AP to
reboot.
• You cannot delete an RF profile that is applied to an AP group.
• You cannot delete an AP group that has APs assigned to it.

Configuring RF Profiles

This section contains the following topics:
• Creating an RF Profile (GUI), page 8-65
• Applying RF Profile to AP Groups (GUI), page 8-65

Creating an RF Profile (GUI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Wireless &gt; RF Profiles to open the RF profiles page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click New to create a new RF profile.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the RF Profile Name and choose the radio band.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Apply to configure the customizations of power and data rate parameters.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure the Maximum and Minimum Power Level Assignment, that is the maximum and minimum power that the APs in this RF profile are allowed to use. The range is from -10 dBm to 30 dBm.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Configure a custom TPC power threshold for either Version1 or Version 2 of TPC. The range is from –80 dBm to –50 dBm.</td>
</tr>
</tbody>
</table>

Note Only one TPC version can be operable for RRM on a controller. Version 1 and Version 2 are not interoperable within the same RF profile. If you select a threshold value for TPCv2 and it is not in the chosen TPC algorithm for the RF profile, this value will be ignored.

| Step 7 | Configure the data rates to be applied to the APs of this RF profile. |
| Step 8 | Click Apply to commit your changes. |
| Step 9 | Click Save Configuration to save your changes. |

Applying RF Profile to AP Groups (GUI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose WLAN &gt; Advanced &gt; AP Groups to open the AP Groups page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click AP Group Name to open a configuration dialog box.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the RF Profile tab to configure the RF Profile details. You can choose an RF profile for each band (802.11a/802.11b) or you can choose one or none to apply to this group.</td>
</tr>
</tbody>
</table>
Configuring Captive Bypassing

Note
Until you choose the APs and add them to the new group, no configurations are applied. You can save the new configuration as is, but no profiles are applied. Once you have chose the APs in to the AP group, the process of moving the APs into the new group reboots the APs and the configurations for the RF profiles will be applied to the APs of the AP group.

Step 4
Click the APs tab and choose the APs to add to the AP group.

Step 5
Click the Add APs to add the selected APs to the AP group. A warning message is displayed indicating that the AP group reboot and the APs rejoin the controller.

Note
The APs cannot belong to two AP groups at once.

Step 6
Click OK. The APs are added to the AP group.

Configuring Web Redirect with 802.1X Authentication

This section contains the following sections:

- Information About Web Redirect with 802.1X Authentication, page 8-66
- Configuring Web Redirect, page 8-67

Information About Web Redirect with 802.1X Authentication

You can configure a WLAN to redirect a user to a particular web page after 802.1X authentication has completed successfully. You can configure the web redirect to give the user partial or full access to the network.

Conditional Web Redirect

If you enable conditional web redirect, the user can be conditionally redirected to a particular web page after 802.1X authentication has completed successfully. You can specify the redirect page and the conditions under which the redirect occurs on your RADIUS server. Conditions might include the user’s password reaching expiration or the user needing to pay his or her bill for continued usage.

If the RADIUS server returns the Cisco AV-pair “url-redirect,” then the user is redirected to the specified URL upon opening a browser. If the server also returns the Cisco AV-pair “url-redirect-acl,” the specified access control list (ACL) is installed as a preauthentication ACL for this client. The client is not considered fully authorized at this point and can only pass traffic allowed by the preauthentication ACL.

After the client completes a particular operation at the specified URL (for example, changing a password or paying a bill), the client must reauthenticate. When the RADIUS server does not return a “url-redirect,” the client is considered fully authorized and allowed to pass traffic.

Note
The conditional web redirect feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security.

After you configure the RADIUS server, you can then configure the conditional web redirect on the controller using either the controller GUI or CLI.
Splash Page Web Redirect

If you enable splash page web redirect, the user is redirected to a particular web page after 802.1X authentication has completed successfully. After the redirect, the user has full access to the network. You can specify the redirect page on your RADIUS server. If the RADIUS server returns the Cisco AV-pair “url-redirect,” then the user is redirected to the specified URL upon opening a browser. The client is considered fully authorized at this point and is allowed to pass traffic, even if the RADIUS server does not return a “url-redirect.”

Note

The splash page web redirect feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security with 802.1x key management. Preshared key management is not supported with any Layer 2 security method.

After you configure the RADIUS server, you can then configure the splash page web redirect on the controller using either the controller GUI or CLI.

Configuring the RADIUS Server (GUI)

Note

This procedure is specific to the CiscoSecure ACS; however, this procedure should be similar to those for other RADIUS servers.

Step 1
From the CiscoSecure ACS main menu, choose Group Setup.

Step 2
Click Edit Settings.

Step 3
From the Jump To drop-down list, choose RADIUS (Cisco IOS/PIX 6.0).

Step 4
Select the [009]cisco-av-pair check box.

Step 5
Enter the following Cisco AV-pairs in the [009]cisco-av-pair edit box to specify the URL to which the user is redirected and, if configuring conditional web redirect, the conditions under which the redirect takes place, respectively:

url-redirect=http://url
url-redirect-acl=acl_name

Configuring Web Redirect

This section contains the following topics:

- Configuring Web Redirect (GUI), page 8-68
- Configuring Web Redirect (CLI), page 8-68
- Disabling Accounting Servers per WLAN (GUI), page 8-69
- Disabling Coverage Hole Detection per WLAN, page 8-69
- Disabling Coverage Hole Detection on a WLAN (GUI), page 8-69
- Disabling Coverage Hole Detection on a WLAN (CLI), page 8-69
Configuring Captive Bypassing

Chapter 8  Working with WLANs

Configuring Web Redirect (GUI)

Step 1  Choose WLANs to open the WLANs page.
Step 2  Click the ID number of the desired WLAN. The WLANs > Edit page appears.
Step 3  Choose the Security and Layer 2 tabs to open the WLANs > Edit (Security > Layer 2) page.
Step 4  From the Layer 2 Security drop-down list, choose 802.1X or WPA+WPA2.
Step 5  Set any additional parameters for 802.1X or WPA+WPA2.
Step 6  Choose the Layer 3 tab to open the WLANs > Edit (Security > Layer 3) page.
Step 7  From the Layer 3 Security drop-down list, choose None.
Step 8  Check the Web Policy check box.
Step 9  Choose one of the following options to enable conditional or splash page web redirect: Conditional Web Redirect or Splash Page Web Redirect. The default value is disabled for both parameters.
Step 10 If the user is to be redirected to a site external to the controller, choose the ACL that was configured on your RADIUS server from the Preauthentication ACL drop-down list.
Step 11 Click Apply to commit your changes.
Step 12 Click Save Configuration to save your changes.

Configuring Web Redirect (CLI)

Step 1  Enable or disable conditional web redirect by entering this command:

```
config wlan security cond-web-redir {enable | disable} wlan_id
```

Step 2  Enable or disable splash page web redirect by entering this command:

```
config wlan security splash-page-web-redir {enable | disable} wlan_id
```

Step 3  Save your settings by entering this command:

```
save config
```

See the status of the web redirect features for a particular WLAN by entering this command:

```
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier................................. 1
Profile Name..................................... test
Network Name (SSID)............................ test
...  
Web Based Authentication....................... Disabled
Web-Passthrough................................. Disabled
Conditional Web Redirect...................... Disabled
Splash-Page Web Redirect...................... Enabled
...  
```
Disabling Accounting Servers per WLAN (GUI)

Note
Disabling accounting servers disables all accounting operations and prevents the controller from falling back to the default RADIUS server for the WLAN.

Step 1 Choose WLANs to open the WLANs page.
Step 2 Click the ID number of the WLAN to be modified. The WLANs > Edit page appears.
Step 3 Choose the Security and AAA Servers tabs to open the WLANs > Edit (Security > AAA Servers) page.
Step 4 Unselect the Enabled check box for the Accounting Servers.
Step 5 Click Apply to commit your changes.
Step 6 Click Save Configuration to save your changes.

Disabling Coverage Hole Detection per WLAN

Note
Coverage hole detection is enabled globally on the controller. See the “Configuring Coverage Hole Detection (GUI)” section on page 13-14 for more information.

Note
In software release 5.2 or later releases, you can disable coverage hole detection on a per-WLAN basis. When you disable coverage hole detection on a WLAN, a coverage hole alert is still sent to the controller, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where guests are connected to your network for short periods of time and are likely to be highly mobile.

Disabling Coverage Hole Detection on a WLAN (GUI)

Step 1 Choose WLANs to open the WLANs page.
Step 2 Click the profile name of the WLAN to be modified. The WLANs > Edit page appears.
Step 3 Choose the Advanced tab to display the WLANs > Edit (Advanced) page.
Step 4 Unselect the Coverage Hole Detection Enabled check box.
Note
OEAP 600 Series Access Points do not support coverage hole detection.
Step 5 Click Apply to commit your changes.
Step 6 Click Save Configuration to save your changes.

Disabling Coverage Hole Detection on a WLAN (CLI)

Step 1 Disable coverage hole detection by entering this command:
config wlan chd wlan_id disable

Note  OEAP 600 Series Access Points do not support Coverage Hole detection.

Step 2  Save your settings by entering this command:
        save config

Step 3  See the coverage hole detection status for a particular WLAN by entering this command:
show wlan wlan_id

Information similar to the following appears:

WLAN Identifier.................................. 2
Profile Name..................................... wlan2
Network Name (SSID).............................. 2

CHD per WLAN.................................. Disabled

Configuring NAC Out-of-Band Integration

This section contains the following topics:
- Information About NAC Out-of-Band Integration, page 8-70
- Guidelines and Limitations, page 8-71
- Configuring NAC Out-of-Band Integration, page 8-72

Information About NAC Out-of-Band Integration

The Cisco NAC Appliance, also known as Cisco Clean Access (CCA), is a network admission control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether machines are compliant with security policies and repairs vulnerabilities before permitting access to the network. The NAC appliance is available in two modes: in-band and out-of-band. Customers can deploy both modes if desired, each geared toward certain types of access (in-band for supporting wireless users and out-of-band for supporting wired users, for example).

To implement the NAC out-of-band feature on the controller, you must enable NAC support on the WLAN or guest LAN and then map this WLAN or guest LAN to an interface that is configured with a quarantine VLAN (untrusted VLAN) and an access VLAN (trusted VLAN). When a client associates and completes Layer 2 authentication, the client obtains an IP address from the access VLAN subnet, but the client state is Quarantine. While deploying the NAC out-of-band feature, be sure that the quarantine VLAN is allowed only between the Layer 2 switch on which the controller is connected and the NAC appliance and that the NAC appliance is configured with a unique quarantine-to-access VLAN mapping. Client traffic passes into the quarantine VLAN, which is trunked to the NAC appliance. After posture validation is completed, the client is prompted to take action for remediation. After cleaning is completed, the NAC appliance updates the controller to change the client state from Quarantine to Access.
the link between the controller and the switch is configured as a trunk, enabling the quarantine VLAN (110) and the access VLAN (10). On the Layer 2 switch, the quarantine traffic is trunked to the NAC appliance while the access VLAN traffic goes directly to the Layer 3 switch. Traffic that reaches the quarantine VLAN on the NAC appliance is mapped to the access VLAN based on a static mapping configuration.

**Guidelines and Limitations**

- In controller software releases prior to 5.1, the controller integrates with the NAC appliance only in in-band mode, where the NAC appliance must remain in the data path. For in-band mode, a NAC appliance is required at each authentication location (such as at each branch or for each controller), and all traffic must traverse the NAC enforcement point. In controller software release 5.1 or later releases, the controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing.
- The NAC appliance supports up to 3500 users, and the controller supports up to 5000 users. Multiple NAC appliances might need to be deployed.
- CCA software release 4.5 or later releases is required for NAC out-of-band integration.
- Because the NAC appliance supports static VLAN mapping, you must configure a unique quarantine VLAN for each interface configured on the controller. For example, you might configure a quarantine VLAN of 110 on controller 1 and a quarantine VLAN of 120 on controller 2. However, if two WLANs or guest LANs use the same distribution system interface, they must use the same quarantine VLAN, provided they have one NAC appliance deployed in the network. The NAC appliance supports unique quarantine-to-access VLAN mapping.
- For posture reassessment based on session expiry, you must configure the session timeout on both the NAC appliance and the WLAN, making sure that the session expiry on the WLAN is greater than that on the NAC appliance.
- When a session timeout is configured on an open WLAN, the timing out of clients in the Quarantine state is determined by the timer on the NAC appliance. Once the session timeout expires for WLANs using web authentication, clients deauthenticate from the controller and must perform posture validation again.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.

**Note** See Chapter 16, “Configuring FlexConnect,” for more information on FlexConnect.

- If you want to enable NAC on an access point group VLAN, you must first enable NAC on the WLAN. Then you can enable or disable NAC on the access point group VLAN. If you ever decide to disable NAC on the WLAN, be sure to disable it on the access point group VLAN as well.
- NAC out-of-band integration is not supported for use with the WLAN AAA override feature.
- All Layer 2 and Layer 3 authentication occurs in the quarantine VLAN. To use external web authentication, you must configure the NAC appliance to allow HTTP traffic to and from external web servers and to allow the redirect URL in the quarantine VLAN.

**Note** See the Cisco NAC appliance configuration guides for configuration instructions:
Configuring NAC Out-of-Band Integration

This section contains the following topics:

- Configuring NAC Out-of-Band Integration (GUI), page 8-72
- Configure NAC Out-of-Band Integration (CLI), page 8-73

Configuring NAC Out-of-Band Integration (GUI)

Step 1
Configure the quarantine VLAN for a dynamic interface as follows:

a. Choose Controller > Interfaces to open the Interfaces page.

b. Click New to create a new dynamic interface.

c. In the Interface Name text box, enter a name for this interface, such as “quarantine.”

d. In the VLAN ID text box, enter a nonzero value for the access VLAN ID, such as “10.”

e. Click Apply to commit your changes. The Interfaces > Edit page appears.

f. Select the Quarantine check box and enter a nonzero value for the quarantine VLAN ID, such as “110.”

Note
We recommend that you configure unique quarantine VLANs throughout your network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in the same subnet, it is mandatory to have the same quarantine VLAN if there is only one NAC appliance in the network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in different subnets, it is mandatory to have different quarantine VLANs if there is only one NAC appliance in the network.

g. Configure any remaining text boxes for this interface, such as the IP address, netmask, and default gateway.

h. Click Apply to save your changes.

Step 2
Configure NAC out-of-band support on a WLAN or guest LAN as follows:

a. Choose WLANs to open the WLANs page.

b. Click the ID number of the desired WLAN or guest LAN. The WLANs > Edit page appears.

c. Choose the Advanced tab to open the WLANs > Edit (Advanced) page.

d. Configure NAC out-of-band support for this WLAN or guest LAN by selecting the NAC State check box. To disable NAC out-of-band support, leave the check box unselected, which is the default value.

e. Click Apply to commit your changes.

Step 3
Configure NAC out-of-band support for a specific access point group as follows:

a. Choose WLANs > Advanced > AP Groups to open the AP Groups page.

b. Click the name of the desired access point group.

c. Choose the WLANs tab to open the AP Groups > Edit (WLANs) page.

d. Click Add New to assign a WLAN to this access point group. The Add New section appears at the top of the page.
e. From the WLAN SSID drop-down list, choose the SSID of the WLAN.

f. From the Interface Name drop-down list, choose the interface to which you want to map the access point group. Choose the quarantine VLAN if you plan to enable NAC out-of-band support.

g. To enable NAC out-of-band support for this access point group, select the **NAC State** check box. To disable NAC out-of-band support, leave the check box unselected, which is the default value.

h. Click **Add** to add this WLAN to the access point group. This WLAN appears in the list of WLANs assigned to this access point group.

**Note**
If you ever want to remove this WLAN from the access point group, hover your cursor over the blue drop-down arrow for the WLAN and choose **Remove**.

**Step 4**
Click **Save Configuration** to save your changes.

**Step 5**
See the current state of the client (Quarantine or Access) as follows:

a. Choose **Monitor > Clients** to open the Clients page.

b. Click the MAC address of the desired client to open the Clients > Detail page. The NAC state appears under the Security Information section.

**Note**
The client state appears as “Invalid” if the client is probing, has not yet associated to a WLAN, or cannot complete Layer 2 authentication.

---

**Configure NAC Out-of-Band Integration (CLI)**

**Step 1**
Configure the quarantine VLAN for a dynamic interface by entering this command:

```
config interface quarantine vlan interface_name vlan_id
```

**Note**
You must configure a unique quarantine VLAN for each interface on the controller.

**Note**
To disable the quarantine VLAN on an interface, enter 0 for the VLAN ID.

**Step 2**
Enable or disable NAC out-of-band support for a WLAN or guest LAN by entering this command:

```
config {wlan | guest-lan} nac {enable | disable} {wlan_id | guest_lan_id}
```

**Step 3**
Enable or disable NAC out-of-band support for a specific access point group by entering this command:

```
config wlan apgroup nac {enable | disable} group_name wlan_id
```

**Step 4**
Save your changes by entering this command:

```
save config
```

**Step 5**
See the configuration of a WLAN or guest LAN, including the NAC state by entering this command:

```
show {wlan wlan_id | guest-lan guest_lan_id}
```

Information similar to the following appears:

```
WLAN Identifier.................................. 1
```
**Configuring Captive Bypassing**

Profile Name..................................... wlan
Network Name (SSID)................................ wlan
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID.................................. Enabled
AAA Policy Override.............................. Disabled

**Network Admission Control**

  NAC-State...................................... Enabled
  Quarantine VLAN............................. 110

...  

**Step 6**  
See the current state of the client (either Quarantine or Access) by entering this command:

```plaintext
show client detailed client_mac
```

Information similar to the following appears:

| Client's NAC state                      | QUARANTINE |

**Note**  
The client state appears as “Invalid” if the client is probing, has not yet associated to a WLAN, or cannot complete Layer 2 authentication.

## Configuring Passive Clients

This section contains the following topics:

- Information About Passive Clients, page 8-74
- Guidelines and Limitations, page 8-75
- Configuring Passive Clients, page 8-75

### Information About Passive Clients

Passive clients are wireless devices, such as scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information when they associate with an access point. As a result, when passive clients are used, the controller never knows the IP address unless they use the DHCP.

Wireless LAN controllers currently act as a proxy for ARP requests. Upon receiving an ARP request, the controller responds with an ARP response instead of passing the request directly to the client. This scenario has two advantages:

- The upstream device that sends out the ARP request to the client will not know where the client is located.
- Power for battery-operated devices such as mobile phones and printers is preserved because they do not have to respond to every ARP requests.

Since the wireless controller does not have any IP related information about passive clients, it cannot respond to any ARP requests. The current behavior does not allow the transfer of ARP requests to passive clients. Any application that tries to access a passive client will fail.

The passive client feature enables the ARP requests and responses to be exchanged between wired and wireless clients. This feature when enabled, allows the controller to pass ARP requests from wired to wireless clients until the desired wireless client gets to the RUN state.
Guidelines and Limitations

- The passive client feature is not supported with the AP groups and FlexConnect centrally switched WLANs.

Configuring Passive Clients

This section contains the following topics:
- Enabling the Passive Client Feature on the Controller (GUI), page 8-76
- Configuring Passive Clients (CLI), page 8-76

Enabling the Multicast-Multicast Mode (GUI)

Step 1
Choose Controller > General to open the General page.

Step 2
Choose one of the following options from the AP Multicast Mode drop-down list:
- Unicast—Configures the controller to use the unicast method to send multicast packets. This is the default value.
- Multicast—Configures the controller to use the multicast method to send multicast packets to a CAPWAP multicast group.

Step 3
Select Multicast from the AP Multicast Mode drop-down list. The Multicast Group Address text box is displayed.

Step 4
In the Multicast Group Address text box, enter the IP address of the multicast group.

Step 5
Click Apply to commit your changes.

Step 6
Click Multicast to enable the global multicast mode.

Enabling the Global Multicast Mode on Controllers (GUI)

Step 1
Choose Controller > Multicast to open the Multicast page.

Note
The Enable IGMP Snooping text box is highlighted only when you enable the Enable Global Multicast mode. The IGMP Timeout (seconds) text box is highlighted only when you enable the Enable IGMP Snooping text box.

Step 2
Select the Enable Global Multicast Mode check box to enable the multicast mode. This step configures the controller to use the multicast method to send multicast packets to a CAPWAP multicast group.

Step 3
Select the Enable IGMP Snooping check box to enable the IGMP snooping. The default value is disabled.

Step 4
In the IGMP Timeout text box to set the IGMP timeout, enter a value between 30 and 7200 seconds.

Step 5
Click Apply to commit your changes.
Enabling the Passive Client Feature on the Controller (GUI)

Step 1  Choose WLANs > WLANs > WLAN ID to open the WLANs > Edit page. By default, the General tab is displayed.

Step 2  Choose the Advanced tab.

Step 3  Select the Passive Client check box to enable the passive client feature.

Step 4  Click Apply to commit your changes.

Configuring Passive Clients (CLI)

Step 1  Enable multicasting on the controller by entering this command:

   config network multicast global enable

   The default value is disabled.

Step 2  Configure the controller to use multicast to send multicast to an access point by entering this command:

   config network multicast mode multicast multicast_group_IP_address

Step 3  Configure passive client on a wireless LAN by entering this command:

   config wlan passive-client {enable | disable} wlan_id

Step 4  Configure a WLAN by entering this command:

   config wlan

Step 5  Save your changes by entering this command:

   save config

Step 6  Display the passive client information on a particular WLAN by entering this command:

   show wlan 2

   Information similar to the following appears:

   WLAN Identifier.......................... 2
   Profile Name............................... passive
   Network Name (SSID)....................... passive
   Status.................................... Enabled
   MAC Filtering............................. Disabled
   Broadcast SSID.......................... Enabled
   AAA Policy Override...................... Disabled
   Network Admission Control
   NAC-State............................... Disabled
   Quarantine VLAN........................ 0
   Number of Active Clients................. 1
   Exclusionlist Timeout.................... 60 seconds
   Session Timeout.......................... 1800 seconds
   CHD per WLAN........................... Enabled
   Webauth DHCP exclusion................ Disabled
   Interface............................... management
   WLAN ACL................................. unconfigured
   DHCP Server............................ Default
   DHCP Address Assignment Required..... Disabled
   --More-- or (q)uit
   Quality of Service....................... Silver (best effort)
   WMM...................................... Allowed
   CCX - AironetIE Support............... Enabled
Step 7 Verify if the passive client is associated correctly with the AP and if the passive client has moved into the DHCP required state at the controller by entering this command:

```
debug client mac_address
```

Step 8 Display the detailed information for a client by entering this command:

```
show client detail mac_address
```

Information similar to the following appears:

```
Client MAC Address............................... 00:0d:28:f4:c0:45
Client Username .................................. N/A
AP MAC Address................................. 00:14:1b:58:19:00
Client State...................................... Associated
Client NAC OOB State............................ Access
Wireless LAN Id.................................. 1
BSSID............................................ 00:14:1b:58:19:00
Connected For .................................. 8 secs
Channel.......................................... 11
IP Address....................................... Unknown

Security Policy Completed...................... No
Policy Manager State............................ DHCP_REQD
Policy Manager Rule Created.................. Yes
ACL Name........................................ none
ACL Applied Status............................ Unavailable
```
### Configuring Captive Bypassing

**Step 9** Check if the client moves into the run state, when a wired client tries to contact the client by entering this command:

```
debug client mac_address
```

**Step 10** Configure and check if the ARP request is forwarded from the wired side to the wireless side by entering this command:

```
debug arp all enable
```

Information similar to the following appears:

```
*dtlArpTask: Apr 15 10:54:26.161: Received dtlArpRequest
  sha: 00:19:06:61:b1:c3 spa: 80.4.1.1
  tha: 00:00:00:00:00:00 tpa: 80.4.0.50
  intf: 1, vlan: 71, node type: 1, mscb: not found, isFromSta: 0
*dtlArpTask: Apr 15 10:54:26.161: dtlArpFindClient:ARP look-up for 80.4.0.50 failed (not a client).

*dtlArpTask: Apr 15 10:54:26.161: Dropping ARP to DS (mscb (nil), port 65535)
  sha 0019.0661.b1c3 spa: 80.4.1.1
  tha 0000:0000:0000 tpa: 80.4.0.50
*dtlArpTask: Apr 15 10:54:26.161: Arp from Wired side to passive client

*dtlArpTask: Apr 15 10:54:27.465: dtlArpBcastRecv: received packet (rxTunType 1, dataLen 122)
```

### Configuring Client Profiling

This section contains the following topics:

- Information About Client Profiling, page 8-78
- Guidelines and Limitations, page 8-78
- Configuring Client Profiling (GUI), page 8-79
- Configuring Client Profiling (CLI), page 8-79

### Information About Client Profiling

When a client tries to associate with a WLAN, it is possible to determine the client type from the information received in the process. The controller acts as the collector of the information and sends the ISE with the required data in an optimal form.

### Guidelines and Limitations

- By default, client profiling will be disabled on all WLANs.
- Client profiling is supported on access points that are in Local mode and FlexConnect mode.
- Profiling is not supported for clients in the following scenarios:
  - Clients associating with FlexConnect mode APs in Standalone mode.
  - Clients associating with FlexConnect mode APs when local authentication is done with local switching is enabled.
- Both DHCP Proxy and DHCP Bridging mode on the controller are supported.
Accounting Server configuration on the WLAN must be pointing at an ISE running 1.1 MnR or later releases. Cisco ACS does not support client profiling.

The type of DHCP server used does not affect client profiling.

If the DHCP_REQUEST packet contains a string that is found in the Profiled Devices list of the ISE, then the client will be profiled automatically.

The client is identified based on the MAC address sent in the Accounting request packet.

Only MAC address should be sent as calling station ID in accounting packets when profiling is enabled.

To enable client profiling, you must enable DHCP required flag and disable local authentication flag.

With profiling enabled for local switching FlexConnect mode APs, only VLAN override is supported as an AAA override attribute.

### Configuring Client Profiling (GUI)

1. Choose **WLANs** to open the WLANs page.
2. Click the WLAN ID. The WLANs > Edit page appears.
3. Click the **Advanced** tab.
4. In the Client Profiling area, to profile clients based on DHCP, select the **DHCP Profiling** check box.
5. Click **Apply**.
6. Click **Save Configuration**.

### Configuring Client Profiling (CLI)

- To enable or disable client profiling for a WLAN based on DHCP, enter this command:
  
  ```
  config wlan profiling radius dhcp {enable | disable} wlan-id
  ```

- To see the status of client profiling on a WLAN, enter this command:
  
  ```
  show wlan wlan-id
  ```

- To enable or disable debugging of client profiling, enter this command:
  
  ```
  debug profiling {enable | disable}
  ```

### Configuring Per-WLAN RADIUS Source Support

This section contains the following topics:

- Information About Per-WLAN RADIUS Source Support, page 8-80
- Guidelines and Limitations, page 8-80
- Configuring Per-WLAN RADIUS Source Support, page 8-80
Information About Per-WLAN RADIUS Source Support

By default, the controller sources all RADIUS traffic from the IP address on its management interface. This means that even if a WLAN has specific RADIUS servers configured instead of the global list, the identity used is the management interface IP address.

If you want to do a per-user WLAN filtering, you can use the callStationID set by RFC 3580 to be in the APMAC:SSID format. You can also extend the filtering on the authentication server to be on a per-WLAN source interface by using the NAS-IP-Address attribute.

When the per-WLAN RADIUS source support is enabled, the controller sources all RADIUS traffic for a particular WLAN using the dynamic interface that is configured. Also, RADIUS attributes are modified accordingly to match the identity. This feature effectively virtualizes the controller on the per-WLAN RADIUS traffic, where each WLAN can have a separate L3 identity. This feature is useful in ACS Network Access Restrictions, Network Access Profiles, and so on.

This feature can be combined with normal RADIUS traffic source, with some WLANs using the management interface and others using the per-WLAN dynamic interface as the address source.

Guidelines and Limitations

- It is up to the authentication server (RADIUS) to implement a proper rule filtering on the new identity because the controller sources traffic only from the selected interface.
- callStationID is always in the APMAC:SSID format to comply with 802.1x over RADIUS RFC. This is also a legacy behavior. Web-auth can use different formats available in the `config radius callStationIDType` command.

If AP groups or AAA override are used, the source interface remains the WLAN interface, and not what is specified on the new AP group or RADIUS profile configuration.

Configuring Per-WLAN RADIUS Source Support

This section contains the following topics:

- Configuring Per-WLAN RADIUS Source Support (CLI), page 8-80
- Monitoring the Status of Per-WLAN RADIUS Source Support (CLI), page 8-81

Configuring Per-WLAN RADIUS Source Support (CLI)

1. Enter the `config wlan disable wlan-id` command to disable the WLAN.
2. Enable or disable the per-WLAN RADIUS source support by entering this command:
   ```
   config wlan radius_server overwrite-interface {enable | disable} wlan-id
   ```

Note: When enabled, the controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on that WLAN.

When disabled, the controller uses the management interface as the identity in the NAS-IP-Address attribute. If the RADIUS server is on a directly connected dynamic interface, the RADIUS traffic will be sourced from that interface. Otherwise, the management IP address is used. In all cases, the NAS-IP-Address attribute remains the management interface, unless the feature is enabled.
**Step 3** Enter the `config wlan enable wlan-id` command to enable the WLAN.

---

**Note**
You can filter requests on the RADIUS server side using CiscoSecure ACS. You can filter (accept or reject) a request depending on the NAS-IP-Address attribute through a Network Access Restrictions rule. The filtering to be used is the CLI/DNIS filtering.

---

**Monitoring the Status of Per-WLAN RADIUS Source Support (CLI)**

To see if the feature is enabled or disabled, enter this command:

```
show wlan wlan-id
```

**Example**

The following example shows that the per-WLAN RADIUS source support is enabled on WLAN 1.

```
show wlan 1
```

Information similar to the following appears:

- WLAN Identifier: 4
- Profile Name: 4400-wpa2
- Network Name (SSID): 4400-wpa2
- Status: Enabled
- MAC Filtering: Disabled
- Broadcast SSID: Enabled
- AAA Policy Override: Disabled
- Network Admission Control
  - Radius Servers
    - Authentication: Global Servers
    - Accounting: Global Servers
  - Overwrite Sending Interface: Enabled
- Local EAP Authentication: Disabled

---

**Configuring Remote LANs**

This section contains the following topics:

- Guidelines and Limitations, page 8-81
- Configuring Remote LANs, page 8-82

**Guidelines and Limitations**

- You must remove all remote LANs from a controller’s configuration before moving to a release that does not support the remote LAN functionality. The remote LAN changes to a WLAN in earlier releases, which could cause an undesirable or unsecured WLAN being broadcast on the wireless network. Remote LAN is only supported in release 7.0.116.0 and later releases.
• Only four clients can connect to an OEAP 600 series access point through a remote LAN port. This number does not affect the fifteen WLAN limit imposed for the controller WLANs. The remote LAN client limit supports connecting a switch or hub to the remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices can connect until one of the devices is idle for more than one minute.

• A Remote LAN can be applied on a dedicated LAN port on an OEAP 600 series access point.

Configuring Remote LANs

This section contains the following topics:

- Configuring a Remote LAN (GUI), page 8-82
- Configuring a Remote LAN (CLI), page 8-83

Configuring a Remote LAN (GUI)

Step 1 Choose WLANs to open the WLANs page.

This page lists all of the WLANs and remote LANs currently configured on the controller. For each WLAN, you can see its WLAN/remote LAN ID, profile name, type, SSID, status, and security policies. The total number of WLANs/remote LANs appears in the upper right-hand corner of the page. If the list of WLANs/remote LANs spans multiple pages, you can access these pages by clicking the page number links.

Note If you want to delete a remote LAN, hover your cursor over the blue drop-down arrow for that WLAN and choose Remove, or select the check box to the left of the row, choose Remove Selected from the drop-down list, and click Go. A message appears asking you to confirm your decision. If you proceed, the remote LAN is removed from any access point group to which it is assigned and from the access point’s radio.

Step 2 From the drop-down list, choose Create New and click Go. The WLANs > New page appears.

Step 3 From the Type drop-down list, choose Remote LAN to create a remote LAN.

Step 4 In the Profile Name text box, enter up to 32 alphanumeric characters for the profile name to be assigned to this Remote WLAN. The profile name must be unique.

Step 5 From the WLAN ID drop-down list, choose the ID number for this WLAN.

Step 6 Click Apply to commit your changes. The WLANs > Edit page appears.

Note You can also open the WLANs > Edit page from the WLANs page by clicking the ID number of the WLAN that you want to edit.

Step 7 Use the parameters on the General, Security, and Advanced tabs to configure this remote LAN. See the sections in the rest of this chapter for instructions on configuring specific features.

Step 8 On the General tab, select the Status check box to enable this remote LAN. Be sure to leave it unselected until you have finished making configuration changes to the remote LAN.
Note
You can also enable or disable remote LANs from the WLANs page by selecting the check boxes to the left of the IDs that you want to enable or disable, choosing Enable Selected or Disable Selected from the drop-down list, and clicking Go.

Step 9
Click Apply to commit your changes.

Step 10
Click Save Configuration to save your changes.

Configuring a Remote LAN (CLI)

- See the current configuration of the remote LAN by entering this command:
  
  \[ \text{show remote-lan remote-lan-id} \]

- Enable or disable remote LAN by entering this command:
  
  \[ \text{config remote-lan \{enable | disable\} remote-lan-id} \]

- Enable or disable 802.1X authentication for remote LAN by entering this command:
  
  \[ \text{config remote-lan security 802.1X \{enable | disable\} remote-lan-id} \]

Note
The encryption on a remote LAN is always “none.”

- Enable or disable local EAP with the controller as an authentication server, by entering this command:
  
  \[ \text{config remote-lan local-auth enable profile-name remote-lan-id} \]

- If you are using an external AAA authentication server, enter this command:
  
  \[ \text{config remote-lan radius_server auth \{add | delete\} remote-lan-id server id} \]
  \[ \text{config remote-lan radius_server auth \{enable | disable\} remote-lan-id} \]
Controlling Lightweight Access Points

This chapter contains these sections:

- Access Point Communication Protocols, page 9-2
- Searching for Access Points, page 9-9
- Searching for Access Point Radios, page 9-14
- Configuring Global Credentials for Access Points, page 9-16
- Configuring Authentication for Access Points, page 9-20
- Configuring Embedded Access Points, page 9-26
- Converting Autonomous Access Points to Lightweight Mode, page 9-28
- Configuring OfficeExtend Access Points, page 9-51
- Using Cisco Workgroup Bridges, page 9-70
- Configuring Backup Controllers, page 9-77
- Configuring Failover Priority for Access Points, page 9-81
- Configuring Country Codes, page 9-87
- Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain, page 9-93
- Using the W56 Band in Japan, page 9-96
- Dynamic Frequency Selection, page 9-96
- Optimizing RFID Tracking on Access Points, page 9-97
- Configuring Probe Request Forwarding, page 9-100
- Retrieving the Unique Device Identifier on Controllers and Access Points, page 9-101
- Performing a Link Test, page 9-102
- Configuring Link Latency, page 9-105
- Configuring the TCP MSS, page 9-108
- Configuring Power over Ethernet, page 9-110
- Configuring Flashing LEDs, page 9-114
- Viewing Clients, page 9-115
- Configuring LED States for Access Points, page 9-120
Access Point Communication Protocols

This section contains the following topics:

- Information About Access Point Communication Protocols, page 9-2
- Guidelines and Limitations, page 9-2
- Configuring Data Encryption, page 9-3
- Viewing CAPWAP Maximum Transmission Unit Information, page 9-6
- Debugging CAPWAP, page 9-7
- Controller Discovery Process, page 9-7
- Verifying that Access Points Join the Controller, page 9-8

Information About Access Point Communication Protocols

Cisco lightweight access points use the IETF standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate with the controller and other lightweight access points on the network.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points. CAPWAP is implemented in controller for these reasons:

- To provide an upgrade path from Cisco products that use LWAPP to next-generation Cisco products that use CAPWAP
- To manage RFID readers and similar devices
- To enable controllers to interoperate with third-party access points in the future

LWAPP-enabled access points can discover and join a CAPWAP controller, and conversion to a CAPWAP controller is seamless. For example, the controller discovery process and the firmware downloading process when using CAPWAP are the same as when using LWAPP. The one exception is for Layer 2 deployments, which are not supported by CAPWAP.

You can deploy CAPWAP controllers and LWAPP controllers on the same network. The CAPWAP-enabled software allows access points to join either a controller running CAPWAP or LWAPP. The only exceptions are that the Cisco Aironet 1040, 1140, 1260, 3500, and 3600 Series Access Points, which support only CAPWAP and join only controllers that run CAPWAP. For example, an 1130 series access point can join a controller running either CAPWAP or LWAPP where an1140 series access point can join only a controller that runs CAPWAP.

Guidelines and Limitations

- If your firewall is currently configured to allow traffic only from access points using LWAPP, you must change the rules of the firewall to allow traffic from access points using CAPWAP.
- Make sure that the CAPWAP UDP ports 5246 and 5247 (similar to the LWAPP UDP ports 12222 and 12223) are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.
- If access control lists (ACLs) are in the control path between the controller and its access points, you need to open new protocol ports to prevent access points from being stranded.
Ensure that the controllers are configured with the correct date and time. If the date and time configured on the controller precedes the creation and installation date of certificates on the access points, the access point fails to join the controller.

**Configuring Data Encryption**

This section contains the following topics:
- Information About Data Encryption, page 9-3
- Guidelines and Limitations, page 9-3
- Upgrading or Downgrading DTLS Images for Cisco 5500 Series Controllers, page 9-4
- Configuring Data Encryption, page 9-4

**Information About Data Encryption**

Cisco 5500 Series Controllers enable you to encrypt CAPWAP control packets (and optionally, CAPWAP data packets) that are sent between the access point and the controller using Datagram Transport Layer Security (DTLS). DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS. CAPWAP control packets are management packets exchanged between a controller and an access point while CAPWAP data packets encapsulate forwarded wireless frames. CAPWAP control and data packets are sent over separate UDP ports: 5246 (control) and 5247 (data). If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.

**Guidelines and Limitations**

- Cisco 1130 and 1240 series access points support DTLS data encryption with software-based encryption, and 1040, 1140, 1250, 1260, 3500, and 3600 series access points support DTLS data encryption with hardware-based encryption.
- DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points. Most access points are deployed in a secure network within a company building, so data encryption is not necessary. In contrast, the traffic between an OfficeExtend access point and the controller travels through an unsecure public network, so data encryption is more important for these access points. When data encryption is enabled, traffic is encrypted at the access point before it is sent to the controller and at the controller before it is sent to the client.
- Encryption limits throughput at both the controller and the access point, and maximum throughput is desired for most enterprise networks.
- In a Cisco unified local wireless network environment, do not enable DTLS on the Cisco 1130 and 1240 access points, as it may result in severe throughput degradation and may render the APs unusable.

See the “Configuring OfficeExtend Access Points” section on page 9-51 for more information on OfficeExtend access points.
- You can use the controller to enable or disable DTLS data encryption for a specific access point or for all access points.
- The availability of data DTLS for the 7.0.116.0 release is as follows:
The Cisco 5500 Series Controller will be available with two licenses options: One that allows data DTLS without any license requirements and another image that requires a license to use data DTLS. See the “Upgrading or Downgrading DTLS Images for Cisco 5500 Series Controllers” section on page 9-4. The images for the DTLS and licensed DTLS images are as follows:

- Licensed DTLS—AS_5500_LDPE_x_x_x_x.aes
- Non licensed DTLS—AS_5500_x_x_x_x.aes

Cisco 2500, WiSM2, WLC2—By default, these platforms do not contain DTLS. To turn on data DTLS, you must install a license. These platforms have a single image with data DTLS turned off. To use data DTLS, you must have a license.

- If your controller does not have a data DTLS license and if the access point associated with the controller has DTLS enabled, the data path will be unencrypted.
- Non-Russian customers using Cisco 5508 Series Controller do not need data DTLS license. However all customers using WISM2 and Cisco 2500 Series Controllers must enable data DTLS.

### Upgrading or Downgrading DTLS Images for Cisco 5500 Series Controllers

**Step 1**
The upgrade operation fails on the first attempt with a warning indicating that the upgrade to a licensed DTLS image is irreversible.

**Caution**
Do not reboot the controller after Step 1.

**Step 2**
On a subsequent attempt, the license is applied and the image is successfully updated.

### Guidelines and Limitations

- You cannot install a regular image (non-Licensed data DTLS) once a licensed data DTLS image is installed.
- You can upgrade from one licensed DTLS image to another licensed DTLS image.
- You can upgrade from a regular image (DTLS) to a licensed DTLS image in a two step process.
- You can use the `show sysinfo` command to verify the LDPE image, before and after the image upgrade.

### Configuring Data Encryption

This section contains the following topics:

- Configuring Data Encryption (GUI), page 9-5
- Configuring Data Encryption (CLI), page 9-5
Chapter 9  Controlling Lightweight Access Points

Configuring Data Encryption (GUI)

Prerequisites
Ensure that the base license is installed on the Cisco 5500 Series Controller. Once the license is installed, you can enable data encryption for the access points. See Chapter 4, “Configuring Controller Settings,” for information on obtaining and installing licenses.

Step 1  Choose Wireless > Access Points > All APs to open the All APs page.
Step 2  Click the name of the access point for which you want to enable data encryption.
Step 3  Choose the Advanced tab to open the All APs > Details for (Advanced) page.

Figure 9-1  All APs > Details for (Advanced) Page

Step 4  Select the Data Encryption check box to enable data encryption for this access point or unselect it to disable this feature. The default value is unselected.

Note Changing the data encryption mode requires the access points to rejoin the controller.

Step 5  Click Apply to commit your changes.
Step 6  Click Save Configuration to save your changes.

Configuring Data Encryption (CLI)

Note In images without a DTLS license, the config or show commands are not available.
### Step 1
Enable or disable data encryption for all access points or a specific access point by entering this command:

```
config ap link-encryption {enable | disable} {all | Cisco_AP}
```

The default value is disabled.

**Note** Changing the data encryption mode requires the access points to rejoin the controller.

### Step 2
When prompted to confirm that you want to disconnect the access point(s) and attached client(s), enter `Y`.

### Step 3
Enter the `save config` command to save your configuration.

### Step 4
See the encryption state of all access points or a specific access point by entering this command:

```
show ap link-encryption {all | Cisco_AP}
```

Information similar to the following appears:

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Encryption</th>
<th>Dnstream Count</th>
<th>Upstream Count</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP1130</td>
<td>En</td>
<td>112</td>
<td>1303</td>
<td>23:49</td>
</tr>
<tr>
<td>AP1140</td>
<td>En</td>
<td>232</td>
<td>2146</td>
<td>23:49</td>
</tr>
</tbody>
</table>

**Note**

- auth err: 198
- replay err: 0

AP1250  En 0 0 Never
AP1240  En 6191 15011 22:13

This command also shows authentication errors, which tracks the number of integrity check failures, and replay errors, which tracks the number of times that the access point receives the same packet.

### Step 5
See a summary of all active DTLS connections by entering this command:

```
show dtls connections
```

Information similar to the following appears:

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Local Port</th>
<th>Peer IP</th>
<th>Peer Port</th>
<th>Ciphersuite</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP1130</td>
<td>Capwap_Ctrl</td>
<td>172.20.225.163</td>
<td>62369</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>AP1250</td>
<td>Capwap_Ctrl</td>
<td>172.20.225.165</td>
<td>19917</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>AP1140</td>
<td>Capwap_Ctrl</td>
<td>172.20.225.165</td>
<td>1904</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>AP1140</td>
<td>Capwap_Data</td>
<td>172.20.225.165</td>
<td>1904</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>AP1130</td>
<td>Capwap_Data</td>
<td>172.20.225.163</td>
<td>62369</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>AP1250</td>
<td>Capwap_Data</td>
<td>172.20.225.166</td>
<td>19917</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
</tbody>
</table>

**Note**

If you experience any problems with DTLS data encryption, enter the `debug dtls {all | event | trace | packet} {enable | disable}` command to debug all DTLS messages, events, traces, or packets.

### Viewing CAPWAP Maximum Transmission Unit Information

See the maximum transmission unit (MTU) for the CAPWAP path on the controller by entering this command:

```
show ap config general Cisco_AP
```

---

---
The MTU specifies the maximum size of any packet (in bytes) in a transmission.

Information similar to the following appears:

Cisco AP Identifier.............................. 9
Cisco AP Name.................................... Maria-1250
Country code..................................... US - United States
Regulatory Domain allowed by Country............. 802.11bg:-A 802.11a:-A
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 00:1f:ca:bd:bc:7c
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.193
IP NetMask....................................... 255.255.255.0
CAPWAP Path MTU............................... 1485

Debugging CAPWAP

Use these CLI commands to obtain CAPWAP debug information:

- `debug capwap events {enable | disable}` — Enables or disables debugging of CAPWAP events.
- `debug capwap errors {enable | disable}` — Enables or disables debugging of CAPWAP errors.
- `debug capwap detail {enable | disable}` — Enables or disables debugging of CAPWAP details.
- `debug capwap info {enable | disable}` — Enables or disables debugging of CAPWAP information.
- `debug capwap packet {enable | disable}` — Enables or disables debugging of CAPWAP packets.
- `debug capwap payload {enable | disable}` — Enables or disables debugging of CAPWAP payloads.
- `debug capwap hexdump {enable | disable}` — Enables or disables debugging of the CAPWAP hexadecimal dump.
- `debug capwap dtls-keepalive {enable | disable}` — Enables or disables debugging of CAPWAP DTLS data keepalive packets.

Controller Discovery Process

In a CAPWAP environment, a lightweight access point discovers a controller by using CAPWAP discovery mechanisms and then sends the controller a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

Guidelines and Limitations

- Upgrade and downgrade paths from LWAPP to CAPWAP or from CAPWAP to LWAPP are supported. An access point with an LWAPP image starts the discovery process in LWAPP. If it finds an LWAPP controller, it starts the LWAPP discovery process to join the controller. If it does not find a LWAPP controller, it starts the discovery in CAPWAP. If the number of times that the discovery process starts with one discovery type (CAPWAP or LWAPP) exceeds the maximum discovery count and the access point does not receive a discovery response, the discovery type changes to the other type. For example, if the access point does not discover the controller in LWAPP, it starts the discovery process in CAPWAP.
• If an access point is in the UP state and its IP address changes, the access point tears down the existing CAPWAP tunnel and rejoins the controller. In previous software releases, the access point notifies the controller, and the session continues with the changed IP address without tearing down the session.

• You must install software release 4.0.155.0 or later releases on the controller before connecting 1100 and 1300 series access points to the controller. The 1120 and 1310 access points were not supported prior to software release 4.0.155.0.

• During the discovery process, the 1040, 1140, 1260, 3500, and 3600 series access points will only query for Cisco CAPWAP Controllers. It will not query for LWAPP controllers. If you want these access points to query for both LWAPP and CAPWAP controllers then you need to update the DNS.

• To configure the IP addresses that the controller sends in its CAPWAP discovery responses, use the `config network ap-discovery nat-ip-only {enable | disable}` command.

• Ensure that the controller is set to the current time. If the controller is set to a time that has already occurred, the access point might not join the controller because its certificate may not be valid for that time.

• Access points must be discovered by a controller before they can become an active part of the network. The lightweight access points support these controller discovery processes:
  - Layer 3 CAPWAP or LWAPP discovery—This feature can be enabled on different subnets from the access point and uses IP addresses and UDP packets rather the MAC addresses used by Layer 2 discovery.
  - Locally stored controller IP address discovery—If the access point was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point’s nonvolatile memory. This process of storing controller IP addresses on an access point for later deployment is called priming the access point.
  - DHCP server discovery—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the “Using DHCP Option 43 and DHCP Option 60” section on page 9-36.
  - DNS discovery—The access point can discover controllers through your domain name server (DNS). You must configure your DNS to return controller IP addresses in response to CISCO-LWAPP-CONTROLLER.localdomain or CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the access point domain name. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-LWAPP-CONTROLLER.localdomain or CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

### Verifying that Access Points Join the Controller

When replacing a controller, ensure that access points join the new controller.

This section contains the following topics:

• Verifying that Access Points Join the Controller (GUI), page 9-9

• Verifying that Access Points Join the Controller (CLI), page 9-9
Verifying that Access Points Join the Controller (GUI)

**Step 1** Configure the new controller as a master controller as follows:
- a. Choose **Controller > Advanced > Master Controller Mode** to open the Master Controller Configuration page.
- b. Select the **Master Controller Mode** check box.
- c. Click **Apply** to commit your changes.
- d. Click **Save Configuration** to save your changes.

**Step 2** (Optional) Flush the ARP and MAC address tables within the network infrastructure.

**Step 3** Restart the access points.

**Step 4** Once all the access points have joined the new controller, configure the controller not to be a master controller by unselecting the **Master Controller Mode** check box on the Master Controller Configuration page.

Verifying that Access Points Join the Controller (CLI)

**Step 1** Configure the new controller as a master controller by entering this command:
```
config network master-base enable
```

**Step 2** (Optional) Flush the ARP and MAC address tables within the network infrastructure.

**Step 3** Restart the access points.

**Step 4** Configure the controller not to be a master controller once all the access points have joined the new controller by entering this command:
```
config network master-base disable
```

Searching for Access Points

This section contains the following topics:
- Information About Searching for Access Points, page 9-9
- Filtering the AP Search (GUI), page 9-10
- Monitoring the Interface Details (GUI), page 9-12

Information About Searching for Access Points

You can search for specific access points in the list of access points on the All APs page. To do so, you create a filter to display only access points that meet certain criteria (such as MAC address, status, access point mode, and certificate type). This feature is especially useful if your list of access points spans multiple pages, preventing you from viewing them all at once.
Filtering the AP Search (GUI)

Step 1  Choose Monitor > Access Point Summary > All APs > Details to open the All APs page.

This page lists all of the access points joined to the controller. For each access point, you can see its name, MAC address, uptime, status, operating mode, certificates, OfficeExtend access point status, and access point submode.

The total number of access points appears in the upper right-hand corner of the page. If the list of access points spans multiple pages, you can access these pages by clicking the page number links. Each page shows up to 20 access points.

Step 2  Click Change Filter to open the Search AP dialog box.

Step 3  Select one or more of the following check boxes to specify the criteria used when displaying access points:

- **MAC Address**—Enter the MAC address of an access point.
  
  **Note**  When you enable the MAC Address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC Address filter is disabled automatically.

- **AP Name**—Enter the name of an access point.
- **AP Model**—Enter the model name of an access point.
- **Operating Status**—Select one or more of the following check boxes to specify the operating status of the access points:
  - **UP**—The access point is up and running.
  - **DOWN**—The access point is not operational.
  - **REG**—The access point is registered to the controller.
  - **DEREG**—The access point is not registered to the controller.
  - **DOWNLOAD**—The controller is downloading its software image to the access point.
- **Port Number**—Enter the controller port number to which the access point is connected.
Searching for Access Points

- **Admin Status**—Choose **Enabled** or **Disabled** to specify whether the access points are enabled or disabled on the controller.

- **AP Mode**—Select one or more of the following options to specify the operating mode of the access points:
  - **Local**—The default option.
  - **FlexConnect**—This mode is used for 1040, 1130, 1140, 1240, 1250, 1260, 3500, 3600, and 800 access points.
  - **REAP**—This mode is the remote edge lightweight access point.
  - **Monitor**—This mode is the monitor-only mode.
  - **Rogue Detector**—This mode monitors the rogue APs on wire. It does not transmit or receive frames over the air or contain rogue APs.
  - **Sniffer**—The access point starts sniffing the air on a given channel. It captures and forwards all the packets from the clients on that channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). It includes information on the time stamp, signal strength, packet size, and so on.
  - **Bridge**—This mode sets the AP mode to “Bridge” if you are connecting a Root AP.
  - **SE-Connect**—This mode allows you to connect to spectrum expert and it allows the access point to perform spectrum intelligence.

**Note** The 600 OEAP series access point uses only local mode.

When an access point in local mode connects to a Cisco Flex 7500 Series Controller, it does not serve clients. The access point details are available in the controller. To enable an access point to serve clients or perform monitoring-related tasks when connected to the Cisco Flex 7500 Series Controller, the access point mode must be in FlexConnect or monitor mode. Use the following command to automatically convert access points to a FlexConnect mode or monitor mode on joining the controller:

```
config ap autoconvert {flexconnect | monitor | disable}
```

All access points that connect to the controller will either be converted to FlexConnect mode or monitor mode depending on the configuration provided.

- **FlexConnect**—This mode is used for 1040, 1130, 1140, 1240, 1250, 1260, 3500, 3600, and 800 access points.
- **REAP**—This mode is the remote edge lightweight access point.
- **Monitor**—This mode is the monitor-only mode.
- **Rogue Detector**—This mode monitors the rogue APs on wire. It does not transmit or receive frames over the air or contain rogue APs.

**Note** Information about rogues that are detected is not shared between controllers. Therefore, we recommend that every controller has its own connected rogue detector AP when rogue detector APs are used.

- **Sniffer**—The access point starts sniffing the air on a given channel. It captures and forwards all the packets from the clients on that channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). It includes information on the time stamp, signal strength, packet size, and so on.

**Note** The Bridge option is displayed only if the AP is bridge capable.

**Note** If the AP mode is set to “Bridge” and the AP is not REAP capable, an error appears.

- **Bridge**—This mode sets the AP mode to “Bridge” if you are connecting a Root AP.
- **SE-Connect**—This mode allows you to connect to spectrum expert and it allows the access point to perform spectrum intelligence.

**Note** The AP3500 and the AP3600 support the spectrum intelligence and AP1260 does not support the spectrum intelligence.
When an access point is configured in SE-Connect mode, the access point reboots and rejoins the controller. Access points that are configured in this mode do not serve the client.

- **Certificate Type**—Select one or more of the following check boxes to specify the types of certificates installed on the access points:
  - MIC—Manufactured-installed certificate
  - SSC—Self-signed certificate
  - LSC—Local significant certificate

  *Note* See the “Authorizing Access Points” section on page 9-30 for more information about these certificate types.

- **Primary S/W Version**—Select this check box to enter the primary software version number
- **Backup S/W Version**—Select this check box to enter the secondary software version number.

**Step 4** Click Apply to commit your changes. Only the access points that match your search criteria appear on the All APs page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1d:e5:54:0e:e6, AP Name: pmsk-ap, Operational Status: UP, Status: Enabled, and so on).

*Note* If you want to remove the filters and display the entire access point list, click Clear Filter.

**Monitoring the Interface Details (GUI)**

**Step 1** Choose Monitor > Summary > All APs. The All APs > Details page appears.

**Step 2** Click the Interfaces tab.
Step 3  Click on the available Interface name. The Interface Details page appears.

Step 4  The Interface Details page displays the following parameter details.

Table 9-1 Interfaces Parameters Details

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Name</td>
<td>Name of the access point.</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Speed of the interference in Mbps.</td>
</tr>
<tr>
<td>RX Bytes</td>
<td>Total number of bytes in the error-free packets received on the interface.</td>
</tr>
<tr>
<td>RX Unicast Packets</td>
<td>Total number of unicast packets received on the interface.</td>
</tr>
<tr>
<td>RX Non-Unicast Packets</td>
<td>Total number of nonunicast or multicast packets received on the interface.</td>
</tr>
<tr>
<td>Input CRC</td>
<td>Total number of CRC error in packets while receiving on the interface.</td>
</tr>
<tr>
<td>Input Errors</td>
<td>Sum of all errors in the packets while receiving on the interface.</td>
</tr>
<tr>
<td>Input Overrun</td>
<td>Number of times the receiver hardware was incapable of handling received data to a hardware buffer because the input rate exceeded the receiver’s capability to handle that data.</td>
</tr>
<tr>
<td>Input Resource</td>
<td>Total number of resource errors in packets received on the interface.</td>
</tr>
<tr>
<td>Runts</td>
<td>Number of packets that are discarded because they are similar to the medium’s minimum packet size.</td>
</tr>
<tr>
<td>Throttle</td>
<td>Total number of times the interface advised a sending NIC that it was overwhelmed by packets being sent and to slow the pace of delivery.</td>
</tr>
<tr>
<td>Output Collision</td>
<td>Total number of packet retransmitted due to an Ethernet collision.</td>
</tr>
<tr>
<td>Output Resource</td>
<td>Resource errors in packets transmitted on the interface.</td>
</tr>
<tr>
<td>Output Errors</td>
<td>Errors that prevented the final transmission of packets out of the interface.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Operational state of the physical ethernet interface on the AP.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Interface’s duplex mode.</td>
</tr>
<tr>
<td>TX Bytes</td>
<td>Number of bytes in the error-free packets transmitted on the interface.</td>
</tr>
</tbody>
</table>
Table 9-1  Interfaces Parameters Details (continued)

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Unicast Packets</td>
<td>Total number of unicast packets transmitted on the interface.</td>
</tr>
<tr>
<td>TX Non-Unicast</td>
<td>Total number of nonunicast or multicast packets transmitted on the interface.</td>
</tr>
<tr>
<td>Packets</td>
<td></td>
</tr>
<tr>
<td>Input Aborts</td>
<td>Total number of packets aborted while receiving on the interface.</td>
</tr>
<tr>
<td>Input Frames</td>
<td>Total number of packets received incorrectly that has a CRC error and a noninteger number of octets on the interface.</td>
</tr>
<tr>
<td>Input Drops</td>
<td>Total number of packets dropped while receiving on the interface because the queue was full.</td>
</tr>
<tr>
<td>Unknown Protocol</td>
<td>Total number of packets discarded on the interface due to an unknown protocol.</td>
</tr>
<tr>
<td>Giants</td>
<td>Number of packets that are discarded because they exceeded the medium’s maximum packet size.</td>
</tr>
<tr>
<td>Interface Resets</td>
<td>Number of times that an interface has been completely reset.</td>
</tr>
<tr>
<td>Output No Buffer</td>
<td>Total number of packets discarded because there was no buffer space.</td>
</tr>
<tr>
<td>Output Underrun</td>
<td>Number of times the transmitter has been running faster than the router can handle.</td>
</tr>
<tr>
<td>Output Total Drops</td>
<td>Total number of packets dropped while transmitting from the interface because the queue was full.</td>
</tr>
</tbody>
</table>

Searching for Access Point Radios

This section contains the following topics:

- Information About Searching for Access Point Radios, page 9-14
- Searching for Access Point Radios (GUI), page 9-14

Information About Searching for Access Point Radios

You can search for specific access point radios in the list of radios on the 802.11a/n Radios page or the 802.11b/g/n Radios page. You can access these pages from the Monitor tab on the menu bar when viewing access point radios or from the Wireless tab on the menu bar when configuring access point radios. To search for specific access point radios, you create a filter to display only radios that meet certain criteria (such as radio MAC address, access point name, or CleanAir status). This feature is especially useful if your list of access point radios spans multiple pages, which prevents you from viewing them all at once.

Searching for Access Point Radios (GUI)

Step 1

Perform either of the following:

- Choose Monitor > Access Points Summary > 802.11a/n (or 802.11b/g/n) Radios > Details to open the 802.11a/n (or 802.11b/g/n) Radios page.
Choose Wireless > Access Points > Radios > 802.11a/n (or 802.11b/g/n) to open the 802.11a/n (or 802.11b/g/n) Radios page.

These pages show all of the 802.11a/n or 802.11b/g/n access point radios that are joined to the controller and their current settings.

The total number of access point radios appears in the upper right-hand corner of the page. If the list of radios spans multiple pages, you can access these pages by clicking the page number links. Each page shows up to 25 access point radios.

Note In a Cisco Unified Wireless Network environment, the 802.11a and 802.11b/g radios should not be differentiated based on their Base Radio MAC addresses, as they may have the same addresses. Instead, the radios should be differentiated based on their physical addresses.

Step 2 Click Change Filter to open the Search AP dialog box.

Step 3 Select one of the following check boxes to specify the criteria used when displaying access point radios:

- **MAC Address**—Base radio MAC address of an access point radio.

Note When you enable the MAC address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC address filter is disabled automatically.

- **AP Name**—Access point name. If you do not know the exact name of the AP, you can specify the name partially by entering one or more successive characters that are part of the AP name.
- **AP Model**—Access point model check box where you select and enter the model of the access point.
- **Operating Status**—Operating status of the access points:
- UP—The access point is up and running.
- DOWN—The access point is not operational.
- REG—The access point is registered to the controller.
- DEREG—The access point is not registered to the controller.
- DOWNLOAD—The controller is downloading its software image to the access point.

• **Admin Status**—Whether the access points are enabled or disabled on the controller.

• **AP Mode**—Options to specify the operating mode of the access points: Local, FlexConnect, REAP, Monitor, Rogue Detector, Sniffer, Bridge, and SE Connect. Depending on the capabilities and support available for the APs, one or more options are displayed.

---

**Note**
The Cisco OEAP 600 Series access point uses Local mode and the settings cannot be altered. The Cisco OEAP 600 Series access point does not support the following AP Modes: Monitor, FlexConnect, Sniffer, Rogue Detector, Bridge, and SE Connect.

---

**Note**
To configure an access point for wIPS, you must set the AP mode to one of the following from the AP Mode drop-down list: Local, FlexConnect, and Monitor.

---

• **Certificate Type**—Check boxes that you can select to specify the types of certificates installed on the access points:
  - MIC—Manufactured-installed certificate
  - SSC—Self-signed certificate
  - LSC—Local significant certificate

• **Primary S/W Version**—Primary controller software version.

• **Secondary S/W Version**—Secondary controller software version.

**Step 4**
Click **Find** to commit your changes. Only the access point radios that match your search criteria appear on the 802.11a/n Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

---

**Note**
If you want to remove the filter and display the entire access point radio list, click **Clear Filter**.

---

# Configuring Global Credentials for Access Points

This section contains the following topics:

- Information About Configuring Global Credentials for Access Points, page 9-17
- Guidelines and Limitations, page 9-17
- Configuring Global Credentials for Access Points, page 9-17
Information About Configuring Global Credentials for Access Points

Cisco IOS access points are shipped from the factory with Cisco as the default enable password. This password allows users to log into the nonprivileged mode and execute show and debug commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the access point’s console port.

Guidelines and Limitations

- In controller software releases prior to 5.0, you can set the access point enable password only for access points that are currently connected to the controller. In controller software release 5.0 or later releases, you can set a global username, password, and enable password that all access points that are currently joined to the controller and any that join in the future inherit as they join the controller. If desired, you can override the global credentials and assign a unique username, password, and enable password for a specific access point.

- Also in controller software release 5.0 or later releases, after an access point joins the controller, the access point enables console port security, and you are prompted for your username and password whenever you log into the access point’s console port. When you log in, you are in nonprivileged mode, and you must enter the enable password in order to use the privileged mode.

- These controller software release 5.0 or later release features are supported on all access points that have been converted to lightweight mode, except the 1100 series. VxWorks access points are not supported.

- The global credentials that you configure on the controller are retained across controller and access point reboots. They are overwritten only if the access point joins a new controller that is configured with a global username and password. If the new controller is not configured with global credentials, the access point retains the global username and password configured for the first controller.

- The controller name in the AP configuration is case sensitive. Therefore, make sure to configure the exact system name on the AP configuration. Failure to do this results in the AP fallback not working.

- You need to keep careful track of the credentials used by the access points. Otherwise, you might not be able to log into an access point’s console port. If you need to return the access points to the default Cisco/Cisco username and password, you must clear the controller’s configuration and the access point’s configuration to return them to factory-default settings. To clear the controller’s configuration, choose Commands > Reset to Factory Default > Reset on the controller GUI, or enter the clear config command on the controller CLI. To clear the access point’s configuration, enter the clear ap config Cisco_AP command on the controller CLI. Entering the command does not clear the static IP address of the access point. Once the access point rejoins a controller, it adopts the default Cisco/Cisco username and password.

Configuring Global Credentials for Access Points

This section contains the following topics:

- Configuring Global Credentials for Access Points (GUI), page 9-18
- Configuring Global Credentials for Access Points (CLI), page 9-19
Configuring Global Credentials for Access Points (GUI)

Step 1  Choose Wireless > Access Points > Global Configuration to open the Global Configuration page.

Step 2  In the Username text box, enter the username that is to be inherited by all access points that join the controller.

Step 3  In the Password text box, enter the password that is to be inherited by all access points that join the controller.

You can set a global username, password, and enable password that all access points inherit as they join the controller including access points that are currently joined to the controller and any that join in the future. You can override the global credentials and assign a unique username, password, and enable password for a specific access point. The following are requirements enforced on the password:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain the management username or the reverse of the username.
- The password should not contain words like Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

Step 4  In the Enable Password text box, enter the enable password that is to be inherited by all access points that join the controller.

Step 5  Click Apply to send the global username, password, and enable password to all access points that are currently joined to the controller or that join the controller in the future.

Step 6  Click Save Configuration to save your changes.

Step 7  (Optional) Override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point as follows:

a. Choose Access Points > All APs to open the All APs page.

b. Click the name of the access point for which you want to override the global credentials.
c. Choose the Credentials tab. The All APs > Details for (Credentials) page appears.

Figure 9-7 All APs > Details for (Credentials) Page

<table>
<thead>
<tr>
<th>Wireless</th>
<th>All APs &gt; Details for AP1140</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Points</td>
<td>General</td>
</tr>
<tr>
<td>Access Points</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced</td>
<td></td>
</tr>
<tr>
<td>Mesh</td>
<td></td>
</tr>
<tr>
<td>RF Profiles</td>
<td></td>
</tr>
<tr>
<td>FlexConnect Groups</td>
<td></td>
</tr>
<tr>
<td>802.11a/n</td>
<td></td>
</tr>
<tr>
<td>802.11b/g/n</td>
<td></td>
</tr>
<tr>
<td>Media Stream</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td></td>
</tr>
<tr>
<td>Timers</td>
<td></td>
</tr>
<tr>
<td>QoS</td>
<td></td>
</tr>
</tbody>
</table>

![Figure 9-7 All APs > Details for (Credentials) Page](image)

- Select the Over-ride Global Credentials check box to prevent this access point from inheriting the global username, password, and enable password from the controller. The default value is unselected.
- In the Username, Password, and Enable Password text boxes, enter the unique username, password, and enable password that you want to assign to this access point.
  
  **Note**  
  The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

- Click Apply to commit your changes.
- Click Save Configuration to save your changes.

  **Note**  
  If you want to force this access point to use the controller’s global credentials, unselect the Over-ride Global Credentials check box.

### Configuring Global Credentials for Access Points (CLI)

**Step 1**  
Configure the global username, password, and enable password for all access points currently joined to the controller as well as any access points that join the controller in the future by entering this command:

```
config ap mgmtuser add username user password password enablesecret enable_password all
```

**Step 2**  
(Optional) Override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point by entering this command:

```
config ap mgmtuser add username user password password enablesecret enable_password Cisco_AP
```
The credentials that you enter in this command are retained across controller and access point reboots and if the access point joins a new controller.

Note: If you want to force this access point to use the controller’s global credentials, enter the `config ap mgmtuser delete Cisco_AP` command. The following message appears after you execute this command: “AP reverted to global username configuration.”

Step 3
Enter the `save config` command to save your changes.

Step 4
Verify that global credentials are configured for all access points that join the controller by entering this command:

`show ap summary`

Information similar to the following appears:

- Number of APs: 1
- Global AP User Name: `globalap`

```
AP Name  Slots  AP Model         Ethernet MAC       Location        Port  Country
-------- ------ ------------------- ------------------ ------------------ ----  -------
FlexConnect   2  AIR-AP1131AG-N-K9 00:13:80:60:48:3e  default location  1     US
```

Note: If global credentials are not configured, the Global AP User Name text box shows “Not Configured.”

To view summary of specific access point you can specify the access point name. You can also use wildcard searches when filtering for access points.

Step 5
See the global credentials configuration for a specific access point by entering this command:

`show ap config general Cisco_AP`

Note: The name of the access point is case sensitive.

Information similar to the following appears:

```
Cisco AP Identifier: 0
Cisco AP Name: FlexConnect

AP User Mode: AUTOMATIC
AP User Name: `globalap`
```

Note: If this access point is configured for global credentials, the AP User Mode text boxes shows “Automatic.” If the global credentials have been overwritten for this access point, the AP User Mode text box shows “Customized.”

## Configuring Authentication for Access Points

This section contains the following topics:
Information About Configuring Authentication for Access Points

You can configure 802.1X authentication between a lightweight access point and a Cisco switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning.

Guidelines and Limitations

- This feature is supported on the following hardware:
  - Cisco Aironet 1040, 1130, 1140, 1240, 1250, 1260, 3500, and 3600 series access points.
  - All controller platforms running in local, flexconnect, monitor, or sniffer mode. Bridge mode is not supported.

  Note
  In flexconnect mode, you can configure local switching with 802.1X authentication if you have configured a local external RADIUS server configured.

  - All Cisco switches that support authentication.

  Note
  See the Release Notes for Cisco wireless LAN controllers and Lightweight Access Points for Release 7.0.155.0 for a list of supported switch hardware and minimum supported software.

- The OEAP 600 Series access points do not support LEAP.
- You can configure global authentication settings that all access points that are currently joined to the controller and any that join in the future. If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.

Prerequisites for Configuring Authentication for Access Points

Step 1
If the access point is new, do the following:

a. Boot the access point with the installed recovery image.

b. If you choose not to follow this suggested flow and instead enable 802.1X authentication on the switch port connected to the access point prior to the access point joining the controller, enter this command:

lwapp ap dot1x username username password password
Chapter 9  Controlling Lightweight Access Points

Configuring Authentication for Access Points

This section contains the following topics:

- Configuring Authentication for Access Points (GUI), page 9-22
- Configuring Authentication for Access Points (CLI), page 9-24

Configuring Authentication for Access Points (GUI)

Step 1  Choose **Wireless > Access Points > Global Configuration** to open the Global Configuration page.
Step 2  Under 802.1x Supplicant Credentials, select the **802.1x Authentication** check box.

Step 3  In the Username text box, enter the username that is to be inherited by all access points that join the controller.

Step 4  In the Password and Confirm Password text boxes, enter the password that is to be inherited by all access points that join the controller.

**Note**  You must enter a strong password in these text boxes. Strong passwords have the following characteristics:
- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.

Step 5  Click **Apply** to send the global authentication username and password to all access points that are currently joined to the controller and to any that join the controller in the future.

Step 6  Click **Save Configuration** to save your changes.

Step 7  If desired, you can choose to override the global authentication settings and assign a unique username and password to a specific access point as follows:

a. Choose **Access Points > All APs** to open the All APs page.

b. Click the name of the access point for which you want to override the authentication settings.

c. Choose the **Credentials** tab to open the All APs > Details for (Credentials) page.
d. Under 802.1x Supplicant Credentials, select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global authentication username and password from the controller. The default value is unselected.

e. In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point.

**Note**
The information that you enter is retained across controller and access point reboots and whenever the access point joins a new controller.

f. Click **Apply** to commit your changes.

g. Click **Save Configuration** to save your changes.

**Note**
If you want to force this access point to use the controller’s global authentication settings, unselect the **Over-ride Global Credentials** check box.

---

### Configuring Authentication for Access Points (CLI)

**Step 1**

Configure the global authentication username and password for all access points currently joined to the controller as well as any access points that join the controller in the future by entering this command:

```
config ap dot1xuser add username userpassword password all
```

**Note**
You must enter a strong password for the `password` parameter. Strong passwords have the following characteristics:
- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.
Step 2  (Optional) Override the global authentication settings and assign a unique username and password to a specific access point. To do so, enter this command:

```
cfg ap dot1xuser add username user password password Cisco_AP
```

**Note**  You must enter a strong password for the `password` parameter. See the note in Step 1 for the characteristics of strong passwords.

The authentication settings that you enter in this command are retained across controller and access point reboots and whenever the access point joins a new controller.

**Note**  If you want to force this access point to use the controller’s global authentication settings, enter the `cfg ap dot1xuser delete Cisco_AP` command. The following message appears after you execute this command: “AP reverted to global username configuration.”

Step 3  Save your changes by entering this command:

```
save config
```

Step 4  (Optional) Disable 802.1X authentication for all access points or for a specific access point by entering this command:

```
cfg ap dot1xuser disable {all | Cisco_AP}
```

**Note**  You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

Step 5  See the authentication settings for all access points that join the controller by entering this command:

```
show ap summary
```

Information similar to the following appears:

```
Number of APs.................................... 1
Global AP User Name.............................. globalap
Global AP Dot1x User Name........................ globalDot1x
```

**Note**  If global authentication settings are not configured, the Global AP Dot1x User Name text box shows “Not Configured.”

To see summary of specific access point you can specify the access point name. You can also use wildcard searches when filtering for access points.

Step 6  See the authentication settings for a specific access point by entering this command:

```
show ap config general Cisco_AP
```

**Note**  The name of the access point is case sensitive.

Information similar to the following appears:

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................. FlexConnect
...
Configuring Embedded Access Points

This section contains the following topics:

- Information About Embedded Access Points, page 9-26
- Guidelines and Limitations, page 9-27
- Additional References, page 9-28

Information About Embedded Access Points

Controller software release 7.0.116.0 or later releases support the embedded access points: AP801 and AP802, which are the integrated access points on the Cisco 880 Series Integrated Services Routers (ISRs). This access points use a Cisco IOS software image that is separate from the router Cisco IOS software image. The access points can operate as autonomous access points configured and managed locally, or they can operate as centrally managed access points that utilize the CAPWAP or LWAPP protocol. The AP801 and AP802 access points are preloaded with both an autonomous Cisco IOS release and a recovery image for the unified mode.
Guidelines and Limitations

- Before you use an AP801 or AP802 Series Lightweight Access Point with controller software release 7.0.116.0 or later releases, you must upgrade the software in the Next Generation Cisco 880 Series Integrated Services Routers (ISRs) to Cisco IOS 151.4.M or later.

- When you want to use the AP801 or AP802 with a controller, you must enable the recovery image for the unified mode on the access point by entering the `service-module wlan-ap 0 bootimage unified` command on the router in privileged EXEC mode.

- If the `service-module wlan-ap 0 bootimage unified` command does not work successfully, make sure that the software license is still eligible.

- After enabling the recovery image, enter the `service-module wlan-ap 0 reload` command on the router to shut down and reboot the access point. After the access point reboots, it discovers the controller, downloads the full CAPWAP or LWAPP software release from the controller, and acts as a lightweight access point.

- To use the CLI commands mentioned above, the router must be running Cisco IOS Release 12.4(20)T or later releases. If you experience any issues, see the “Troubleshooting an Upgrade or Reverting the AP to Autonomous Mode” section in the ISR configuration guide at: http://www.cisco.com/c/en/us/td/docs/routers/access/800/software/configuration/guide/SCG800Guide/SCG800_Guide_BkMap_chapter_01001.html

- To support CAPWAP or LWAPP, the router must be activated with at least the Cisco Advanced IP Services IOS license-grade image. A license is required to upgrade to this Cisco IOS image on the router. For licensing information, see http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

- After the AP801 or AP802 boots up with the recovery image for the unified mode, it requires an IP address to communicate with the controller and to download its unified image and configuration from the controller. The router can provide DHCP server functionality, the DHCP pool to reach the controller, and setup option 43 for the controller IP address in the DHCP pool configuration. Use the following configuration to perform this task:

  ```
  ip dhcp pool pool_name
  network ip_address subnet_mask
  dns-server ip_address
  default-router ip_address
  option 43 hex controller_ip_address_in_hex
  ```

  Example:

  ```
  ip dhcp pool embedded-ap-pool
  network 60.0.0.0 255.255.255.0
  dns-server 171.70.168.183
  default-router 60.0.0.1
  option 43 hex f104.0a0a.0a0f /* single WLC IP address(10.10.10.15) in hex format */
  ```

- The AP801 and AP802 802.11n radio supports lower power levels than the 802.11n radio in the Cisco Aironet 1250 series access points. The AP801 and AP802 access points store the radio power levels and passes them to the controller when the access point joins the controller. The controller uses the supplied values to limit the user’s configuration.

  The AP801 and AP802 access points can be used in flexconnect mode.
Converting Autonomous Access Points to Lightweight Mode

This section contains the following topics:

- Information About Autonomous Access Points Converted to Lightweight Mode, page 9-28
- Guidelines and Limitations, page 9-29
- Reverting from Lightweight Mode to Autonomous Mode, page 9-29
- Authorizing Access Points, page 9-30
- Using DHCP Option 43 and DHCP Option 60, page 9-36
- Troubleshooting the Access Point Join Process, page 9-37
- Sending Debug Commands to Access Points Converted to Lightweight Mode, page 9-42
- Understanding How Converted Access Points Send Crash Information to the Controller, page 9-43
- Understanding How Converted Access Points Send Radio Core Dumps to the Controller, page 9-43
- Uploading Memory Core Dumps from Converted Access Points, page 9-45
- Viewing the AP Crash Log Information, page 9-47
- Displaying MAC Addresses for Converted Access Points, page 9-48
- Disabling the Reset Button on Access Points Converted to Lightweight Mode, page 9-48
- Configuring a Static IP Address on a Lightweight Access Point, page 9-48
- Supporting Oversized Access Point Images, page 9-51

Information About Autonomous Access Points Converted to Lightweight Mode

You can use an upgrade conversion tool to convert autonomous Cisco Aironet 1100, 1130AG, 1200, 1240AG, 1260, and 1300 Series Access Points to lightweight mode. When you upgrade one of these access points to lightweight mode, the access point communicates with a controller and receives a configuration and software image from the controller.

See the Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode document for instructions on upgrading an autonomous access point to lightweight mode. You can find this document at this URL:

Guidelines and Limitations

- Access points converted to lightweight mode do not support Wireless Domain Services (WDS). Converted access points communicate only with Cisco wireless LAN controllers and cannot communicate with WDS devices. However, the controller provides functionality that is equivalent to WDS when the access point associates to it.

- In controller software release 4.2 or later releases, all Cisco lightweight access points support 16 BSSIDs per radio and a total of 16 wireless LANs per access point. In previous releases, they supported only 8 BSSIDs per radio and a total of 8 wireless LANs per access point. When a converted access point associates to a controller, only wireless LANs with IDs 1 through 16 are pushed to the access point.

- Access points converted to lightweight mode must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.

- After you convert an access point to lightweight mode, the console port provides read-only access to the unit.

- The 1130AG and 1240AG access points support flexconnect mode. For more information about FlexConnect, see Chapter 16, “Configuring FlexConnect.”

- The upgrade conversion tool adds the self-signed certificate (SSC) key-hash to only one of the controllers on the Cisco WiSM. After the conversion has been completed, add the SSC key-hash to the second controller on the Cisco WiSM by copying the SSC key-hash from the first controller to the second controller. To copy the SSC key-hash, open the AP Policies page of the controller GUI (Security > AAA > AP Policies) and copy the SSC key-hash from the SHA1 Key Hash column under AP Authorization List (see Figure 9-11). Then, using the second controller’s GUI, open the same page and paste the key-hash into the SHA1 Key Hash text box under Add AP to Authorization List. If you have more than one Cisco WiSM, use WCS to push the SSC key-hash to all the other controllers.

Reverting from Lightweight Mode to Autonomous Mode

After you use the upgrade tool to convert an autonomous access point to lightweight mode, you can convert the access point from a lightweight unit back to an autonomous unit by loading a Cisco IOS release that supports autonomous mode (Cisco IOS Release 12.3(7)JA or earlier releases). If the access point is associated to a controller, you can use the controller to load the Cisco IOS release. If the access point is not associated to a controller, you can load the Cisco IOS release using TFTP. In either method, the access point must be able to access a TFTP server that contains the Cisco IOS release to be loaded.

This section contains the following topics:

- Reverting to a Previous Release (CLI), page 9-29
- Reverting to a Previous Release (Using the MODE Button and a TFTP Server), page 9-30

Reverting to a Previous Release (CLI)

Step 1 Log on to the CLI on the controller to which the access point is associated.

Step 2 Revert from lightweight mode, by entering this command:

```
config ap tftp-downgrade tftp-server-ip-address filename access-point-name
```
Step 3 Wait until the access point reboots and reconfigure the access point using the CLI or GUI.

Reverting to a Previous Release (Using the MODE Button and a TFTP Server)

Step 1 Configure the PC on which your TFTP server software runs with a static IP address in the range of 10.0.0.2 to 10.0.0.30.

Step 2 Make sure that the PC contains the access point image file (such as c1200-k9w7-tar.123-7.JA.tar for a 1200 series access point) in the TFTP server folder and that the TFTP server is activated.

Step 3 Rename the access point image file in the TFTP server folder to c1200-k9w7-tar.default for a 1200 series access point.

Step 4 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 5 Disconnect power from the access point.

Step 6 Press and hold the MODE button while you reconnect power to the access point.

Note The MODE button on the access point must be enabled. Follow the steps in the “Disabling the Reset Button on Access Points Converted to Lightweight Mode” section on page 9-48 to select the status of the access point MODE button.

Step 7 Hold the MODE button until the status LED turns red (approximately 20 to 30 seconds), and release the MODE button.

Step 8 Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

Step 9 After the access point reboots, reconfigure the access point using the GUI or the CLI.

Authorizing Access Points

In controller software releases prior to 5.2, the controller may either use self-signed certificates (SSCs) to authenticate access points or send the authorization information to a RADIUS server (if access points have manufactured-installed certificates [MICs]). In controller software release 5.2 or later releases, you can configure the controller to use a local significant certificate (LSC).

This section contains the following topics:

- Authorizing Access Points Using SSCs, page 9-31
- Authorizing Access Points Using MICs, page 9-31
- Authorizing Access Points Using LSCs, page 9-31
- Authorizing Access Points (GUI), page 9-35
- Authorizing Access Points (CLI), page 9-36
Authorizing Access Points Using SSCs

The Control and Provisioning of Wireless Access Points protocol (CAPWAP) secures the control communication between the access point and controller by a secure key distribution requiring X.509 certificates on both the access point and controller. CAPWAP relies on provisioning of the X.509 certificates. Cisco Aironet access points shipped before July 18, 2005 do not have a MIC, so these access points create an SSC when upgraded to operate in lightweight mode. Controllers are programmed to accept local SSCs for authentication of specific access points and do not forward those authentication requests to a RADIUS server. This behavior is acceptable and secure.

Authorizing Access Points Using MICs

You can configure controllers to use RADIUS servers to authorize access points using MICs. The controller uses an access point’s MAC address as both the username and password when sending the information to a RADIUS server. For example, if the MAC address of the access point is 000b85229a70, both the username and password used by the controller to authorize the access point are 000b85229a70.

**Note**
The lack of a strong password by the use of the access point’s MAC address should not be an issue because the controller uses MIC to authenticate the access point prior to authorizing the access point through the RADIUS server. Using MIC provides strong authentication.

**Note**
If you use the MAC address as the username and password for access point authentication on a RADIUS AAA server, do not use the same AAA server for client authentication.

Authorizing Access Points Using LSCs

You can use an LSC if you want your own public key infrastructure (PKI) to provide better security, to have control of your certificate authority (CA), and to define policies, restrictions, and usages on the generated certificates.

The LSC CA certificate is installed on access points and controllers. You need to provision the device certificate on the access point. The access point gets a signed X.509 certificate by sending a certRequest to the controller. The controller acts as a CA proxy and receives the certRequest signed by the CA for the access point.

**Note**
When the CA server is in manual mode and if there is an AP entry in the LSC SCEP table that is pending enrollment, the controller waits for the CA server to send a pending response. If there is no response from the CA server, the controller retries a total of three times to get a response, after which the fallback mode comes into effect where the AP provisioning times out and the AP reboots and comes up with MIC.

This section contains the following topics:
- Configuring LSC (GUI), page 9-31
- Configuring LSC (CLI), page 9-33

**Configuring LSC (GUI)**

**Step 1** Choose **Security > Certificate > LSC** to open the Local Significant Certificates (LSC) - General page.
Chapter 9  Controlling Lightweight Access Points

Converting Autonomous Access Points to Lightweight Mode

Step 2  Select the Enable LSC on Controller check box to enable the LSC on the system.

Step 3  In the CA Server URL text box, enter the URL to the CA server. You can enter either a domain name or an IP address.

Step 4  In the Params text boxes, enter the parameters for the device certificate. The key size is a value from 384 to 2048 (in bits), and the default value is 2048.

Step 5  Click Apply to commit your changes.

Step 6  To add the CA certificate into the controller’s CA certificate database, hover your cursor over the blue drop-down arrow for the certificate type and choose Add.

Step 7  Choose the AP Provisioning tab to open the Local Significant Certificates (LSC) - AP Provisioning page.

Step 8  Select the Enable check box and click Update to provision the LSC on the access point.

Step 9  When a message appears indicating that the access points will be rebooted, click OK.

Step 10 In the Number of Attempts to LSC text box, enter the number of times that the access point attempts to join the controller using an LSC before the access point reverts to the default certificate (MIC or SSC). The range is 0 to 255 (inclusive), and the default value is 3.

Note  If you set the number of retries to a nonzero value and the access point fails to join the controller using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate.

Note  If you are configuring LSC for the first time, we recommend that you configure a nonzero value.
Chapter 9  Controlling Lightweight Access Points

Converting Autonomous Access Points to Lightweight Mode

Step 11  Enter the access point MAC address in the AP Ethernet MAC Addresses text box and click Add to add access points to the provision list.

Note  To remove an access point from the provision list, hover your cursor over the blue drop-down arrow for the access point and choose Remove.

Note  If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning. If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

Step 12  Click Apply to commit your changes.

Step 13  Click Save Configuration to save your changes.

Configuring LSC (CLI)

Step 1  Enable LSC on the system by entering this command:

```
config certificate lsc { enable | disable }
```

Step 2  Configure the URL to the CA server by entering this command:

```
config certificate lsc ca-server http://url:port/path
```

where url can be either a domain name or IP address.

Note  You can configure only one CA server. To configure a different CA server, delete the configured CA server using the config certificate lsc ca-server delete command, and then configure a different CA server.

Step 3  Add the LSC CA certificate into the controller’s CA certificate database by entering this command:

```
config certificate lsc ca-cert { add | delete }
```

Step 4  Configure the parameters for the device certificate by entering this command:

```
config certificate lsc subject-params country state city orgn dept e-mail
```

Note  The common name (CN) is generated automatically on the access point using the current MIC/SSC format Cxxxx-MacAddr, where xxxx is the product number.

Step 5  Configure a key size by entering this command:

```
config certificate lsc other-params keysize
```

The keysize is a value from 384 to 2048 (in bits), and the default value is 2048.

Step 6  Add access points to the provision list by entering this command:

```
config certificate lsc ap-provision auth-list add AP_mac_addr
```
Converting Autonomous Access Points to Lightweight Mode

Note
To remove access points from the provision list, enter the `config certificate lsc ap-provision auth-list delete AP_mac_addr` command.

Note
If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning (in Step 8). If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

Step 7
Configure the number of times that the access point attempts to join the controller using an LSC before the access point reverts to the default certificate (MIC or SSC) by entering this command:

```
config certificate lsc ap-provision revert-cert retries
```

where `retries` is a value from 0 to 255, and the default value is 3.

Note
If you set the number of retries to a nonzero value and the access point fails to join the controller using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate.

Note
If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

Step 8
Provision the LSC on the access point by entering this command:

```
config certificate lsc ap-provision {enable | disable}
```

Step 9
See the LSC summary by entering this command:

```
show certificate lsc summary
```

Information similar to the following appears:

```
LSC Enabled.......................................... Yes
LSC CA-Server........................................ http://10.0.0.1:8080/caserver
LSC AP-Provisioning.................................. Yes
  Provision-List................................. Not Configured
  LSC Revert Count in AP reboots................... 3

LSC Params:
  Country.......................................... 4
  State............................................ ca
  City............................................. ss
  Orgn............................................. org
  Dept............................................. dep
  Email............................................ dep@co.com
  KeySize.......................................... 390

LSC Certs:
  CA Cert.......................................... Not Configured
  RA Cert.......................................... Not Configured
```

Step 10
See details about the access points that are provisioned using LSC by entering this command:
show certificate lsc ap-provision

Information similar to the following appears:

```
LSC AP-Provisioning......................... Yes
Provision-List............................... Present
```

<table>
<thead>
<tr>
<th>Idx</th>
<th>Mac Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>-------------------</td>
</tr>
<tr>
<td>1</td>
<td>00:18:74:c7:c0:90</td>
</tr>
</tbody>
</table>

**Authorizing Access Points (GUI)**

**Step 1** Choose **Security > AAA > AP Policies** to open the AP Policies page.

**Figure 9-11 AP Policies Page**

**Step 2** If you want the access point to accept self-signed certificates (SSCs), manufactured-installed certificates (MICs), or local significant certificates (LSCs), select the appropriate check box.

- If you want the access points to be authorized using a AAA RADIUS server, select the **Authorize MIC APs against auth-list or AAA** check box.
- If you want the access points to be authorized using an LSC, select the **Authorize LSC APs against auth-list** check box.

**Step 3** Click **Apply** to commit your changes.

**Step 4** Follow these steps to add an access point to the controller's authorization list:

a. Click **Add** to access the Add AP to Authorization List area.

b. In the MAC Address text box, enter the MAC address of the access point.

c. From the Certificate Type drop-down list, choose **MIC**, **SSC**, or **LSC**.

d. Click **Add**. The access point appears in the access point authorization list.
Authorizing Access Points (CLI)

- Configure an access point authorization policy by entering this command:
  ```
  config auth-list ap-policy {authorize-ap {enable | disable} | authorize-lsc-ap {enable | disable}}
  ```

- Configure an access point to accept manufactured-installed certificates (MICs), self-signed certificates (SSCs), or local significant certificates (LSCs) by entering this command:
  ```
  config auth-list ap-policy {mic | ssc | lsc {enable | disable}}
  ```

- Configure the user name to be used in access point authorization requests.
  ```
  config auth-list ap-policy {authorize-ap username {ap_name | ap_mac | both}}
  ```

- Add an access point to the authorization list by entering this command:
  ```
  config auth-list add {mic | ssc | lsc} ap_mac [ap_key]
  ```
  where `ap_key` is an optional key hash value equal to 20 bytes or 40 digits.

- To delete an access point from the authorization list, enter this command:
  ```
  config auth-list delete ap_mac.
  ```

- See the access point authorization list by entering this command:
  ```
  show auth-list
  ```

Using DHCP Option 43 and DHCP Option 60

Cisco Aironet access points use the type-length-value (TLV) format for DHCP option 43. DHCP servers must be programmed to return the option based on the DHCP Vendor Class Identifier (VCI) string (DHCP option 60) of the access point. Table 9-2 lists the VCI strings for Cisco access points capable of operating in lightweight mode.

<table>
<thead>
<tr>
<th>Access Point</th>
<th>VCI String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Aironet 1040 Series</td>
<td>Cisco AP c1040</td>
</tr>
<tr>
<td>Cisco Aironet 1130 Series</td>
<td>Cisco AP c1130</td>
</tr>
</tbody>
</table>
### Converting Autonomous Access Points to Lightweight Mode

The format of the TLV block is as follows:

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

See the product documentation for your DHCP server for instructions on configuring DHCP option 43. The *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* document contains example steps for configuring option 43 on a DHCP server.

If the access point is ordered with the Service Provider Option - AIR-OPT60-DHCP selected, the VCI string for that access point will be different than those listed above. The VCI string will have the "ServiceProvider". For example, a 1260 with this option will return this VCI string: "Cisco AP c1260-ServiceProvider".

---

**Note**

The controller IP address that you obtain from the DHCP server should be a unicast IP address. Do not configure the controller IP address as a multicast address when configuring DHCP Option 43.

---

## Troubleshooting the Access Point Join Process

Access points can fail to join a controller for many reasons such as a RADIUS authorization is pending, self-signed certificates are not enabled on the controller, the access point and controller’s regulatory domains do not match, and so on.

---

**Note**

For join information specific to an OfficeExtend access point, see the “Configuring OfficeExtend Access Points” section on page 9-51.

Controller software release 5.2 or later releases enable you to configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the controller because all of the CAPWAP error messages can be viewed from the syslog server itself.
The state of the access point is not maintained on the controller until it receives a CAPWAP join request from the access point, so it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining issues without enabling CAPWAP debug commands on the controller, the controller collects information for all access points that send a discovery message to this controller and maintains information for any access points that have successfully joined this controller.

The controller collects all join-related information for each access point that sends a CAPWAP discovery request to the controller. Collection begins with the first discovery message received from the access point and ends with the last configuration payload sent from the controller to the access point.

You can view join-related information for the following numbers of access points:

- Up to 250 access points for Cisco 5500 Series Controllers
- Up to 300 access points for 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Integrated Wireless LAN Controller Switch
- Up to three times the maximum number of access points supported by the platform for the Controller Network Module within the Cisco 28/37/38xx Series Integrated Services Routers

When the controller is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

An access point sends all syslog messages to IP address 255.255.255.255 by default when any of the following conditions are met:

- An access point that runs software release 4.2 or later releases has been newly deployed.
- An existing access point that runs a software release prior to 4.2 releases has been upgraded to 4.2 or a later release.
- An existing access point that runs software release 4.2 or later releases has been reset after clearing the configuration.

If any of these conditions are met and the access point has not yet joined a controller, you can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all syslog messages to this IP address.

You can also configure the syslog server IP address through the access point CLI, provided the access point is currently not connected to the controller by entering the `lwapp ap log-server syslog_server_IP_address` command.

When the access point joins a controller for the first time, the controller pushes the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address, until it is overridden by one of the following scenarios:

- The access point is still connected to the same controller, and the global syslog server IP address configuration on the controller has been changed using the `config ap syslog host global syslog_server_IP_address` command. In this case, the controller pushes the new global syslog server IP address to the access point.
- The access point is still connected to the same controller, and a specific syslog server IP address has been configured for the access point on the controller using the `config ap syslog host specific Cisco_AP syslog_server_IP_address` command. In this case, the controller pushes the new specific syslog server IP address to the access point.
- The access point gets disconnected from the controller, and the syslog server IP address has been configured from the access point CLI using the `lwapp ap log-server syslog_server_IP_address` command. This command works only if the access point is not connected to any controller.
- The access point gets disconnected from the controller and joins another controller. In this case, the new controller pushes its global syslog server IP address to the access point.
Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all syslog messages to the new IP address, provided the access point can reach the syslog server IP address.

This section contains the following topics:
- Configuring the Syslog Server for Access Points (CLI), page 9-39
- Viewing Access Point Join Information, page 9-39

### Configuring the Syslog Server for Access Points (CLI)

**Step 1** Perform one of the following:

- To configure a global syslog server for all access points that join this controller, enter this command:

  ```
  config ap syslog host global syslog_server_IP_address
  ```

  **Note** By default, the global syslog server IP address for all access points is 255.255.255.255. Make sure that the access points can reach the subnet on which the syslog server resides before configuring the syslog server on the controller. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.

- To configure a syslog server for a specific access point, enter this command:

  ```
  config ap syslog host specific Cisco_AP syslog_server_IP_address
  ```

  **Note** By default, the syslog server IP address for each access point is 0.0.0.0, which indicates that the access point is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.

**Step 2** Save your changes by entering this command:

```
save config
```

**Step 3** See the global syslog server settings for all access points that join the controller by entering this command:

```
show ap config global
```

Information similar to the following appears:

```
AP global system logging host ....................... 255.255.255.255
```

**Step 4** See the syslog server settings for a specific access point by entering this command:

```
show ap config general Cisco_AP
```

### Viewing Access Point Join Information

Join statistics for an access point that sends a CAPWAP discovery request to the controller at least once are maintained on the controller even if the access point is rebooted or disconnected. These statistics are removed only when the controller is rebooted or when you choose to clear the statistics.
This section contains the following topics:

- Viewing Access Point Join Information (GUI), page 9-40
- Viewing Access Point Join Information (CLI), page 9-41

**Viewing Access Point Join Information (GUI)**

**Step 1** Choose Monitor > Statistics > AP Join to open the AP Join Stats page.

**Figure 9-12 AP Join Stats Page**

This page lists all of the access points that are joined to the controller or that have tried to join. It shows the radio MAC address, access point name, current join status, Ethernet MAC address, IP address, and last join time for each access point.

The total number of access points appears in the upper right-hand corner of the page. If the list of access points spans multiple pages, you can view these pages by clicking the page number links. Each page shows the join statistics for up to 25 access points.

- **Note** If you want to remove an access point from the list, hover your cursor over the blue drop-down arrow for that access point and click **Remove**.

- **Note** If you want to clear the statistics for all access points and start over, click **Clear Stats on All APs**.

**Step 2** If you want to search for specific access points in the list of access points on the AP Join Stats page, follow these steps to create a filter to display only access points that meet certain criteria (such as MAC address or access point name).

- **Note** This feature is especially useful if your list of access points spans multiple pages, preventing you from viewing them all at once.

  a. Click **Change Filter** to open the Search AP dialog box.
  b. Select one of the following check boxes to specify the criteria used when displaying access points:
Chapter 9  Controlling Lightweight Access Points

Converting Autonomous Access Points to Lightweight Mode

- **MAC Address**—Enter the base radio MAC address of an access point.
- **AP Name**—Enter the name of an access point.

**Note** When you enable one of these filters, the other filter is disabled automatically.

c. Click **Find** to commit your changes. Only the access points that match your search criteria appear on the AP Join Stats page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1e:f7:75:0a:a0 or AP Name:pm-sk-ap).

**Note** If you want to remove the filter and display the entire access point list, click **Clear Filter**.

Step 3  To see detailed join statistics for a specific access point, click the radio MAC address of the access point. The AP Join Stats Detail page appears.

This page provides information from the controller’s perspective on each phase of the join process and shows any errors that have occurred.

---

Viewing Access Point Join Information (CLI)

Use these CLI commands to see access point join information:

- See the MAC addresses of all the access points that are joined to the controller or that have tried to join by entering this command:

  **show ap join stats summary all**

  Information similar to the following appears:

  Number of APs.......................... 4

<table>
<thead>
<tr>
<th>Base Mac</th>
<th>AP EthernetMac</th>
<th>AP Name</th>
<th>IP Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:85:57:bc:c0</td>
<td>00:0b:85:57:bc:c0</td>
<td>AP1130</td>
<td>10.10.163.217</td>
<td>Joined</td>
</tr>
<tr>
<td>00:1c:0f:81:db:80</td>
<td>00:1c:63:23:ac:a0</td>
<td>AP1140</td>
<td>10.10.163.216</td>
<td>Not joined</td>
</tr>
<tr>
<td>00:1c:0f:81:fc:20</td>
<td>00:1b:d5:9f:7d:b2</td>
<td>AP1</td>
<td>10.10.163.215</td>
<td>Joined</td>
</tr>
<tr>
<td>00:21:1b:ea:36:60</td>
<td>00:0c:d4:8a:6b:c1</td>
<td>AP2</td>
<td>10.10.163.214</td>
<td>Not joined</td>
</tr>
</tbody>
</table>

- See the last join error detail for a specific access point by entering this command:

  **show ap join stats summary ap_mac**

  where **ap_mac** is the MAC address of the 802.11 radio interface.

**Note** To obtain the MAC address of the 802.11 radio interface, enter the **show interfaces Dot11Radio 0** command on the access point.

Information similar to the following appears:

Is the AP currently connected to controller.............. Yes
Time at which the AP joined this controller last time..... Aug 21 12:50:36.061
Type of error that occurred last......................... AP got or has been disconnected
Reason for error that occurred last....................... The AP has been reset by the controller
Time at which the last join error occurred.............. Aug 21 12:50:34.374
• See all join-related statistics collected for a specific access point by entering this command:

  `show ap join stats detailed ap_mac`

  Information similar to the following appears:

  Discovery phase statistics
  - Discovery requests received......................... 2
  - Successful discovery responses sent................ 2
  - Unsuccessful discovery request processing........... 0
  - Reason for last unsuccessful discovery attempt...... Not applicable
  - Time at last successful discovery attempt........... Aug 21 12:50:23.335
  - Time at last unsuccessful discovery attempt........ Not applicable

  Join phase statistics
  - Join requests received................................ 1
  - Successful join responses sent....................... 1
  - Unsuccessful join request processing................ 1
  - Reason for last unsuccessful join attempt........... RADIUS authorization is pending for the AP
  - Time at last successful join attempt................ Aug 21 12:50:34.481
  - Time at last unsuccessful join attempt............. Aug 21 12:50:34.374

  Configuration phase statistics
  - Configuration requests received...................... 1
  - Successful configuration responses sent.............. 1
  - Unsuccessful configuration request processing........ 0
  - Reason for last unsuccessful configuration attempt... Not applicable
  - Time at last successful configuration attempt......... Aug 21 12:50:34.374
  - Time at last unsuccessful configuration attempt...... Not applicable

  Last AP message decryption failure details
  - Reason for last message decryption failure........... Not applicable

  Last AP disconnect details
  - Reason for last AP connection failure................ The AP has been reset by the controller

  Last join error summary
  - Type of error that occurred last...................... AP got or has been disconnected
  - Reason for error that occurred last................... The AP has been reset by the controller
  - Time at which the last join error occurred.......... Aug 21 12:50:34.374

• Clear the join statistics for all access points or for a specific access point by entering this command:

  `clear ap join stats { all | ap_mac }`

**Sending Debug Commands to Access Points Converted to Lightweight Mode**

You can enable the controller to send debug commands to an access point converted to lightweight mode by entering this command:

```
debug ap { enable | disable | command cmd } Cisco_AP
```

When this feature is enabled, the controller sends debug commands to the converted access point as character strings. You can send any debug command supported by Cisco Aironet access points that run Cisco IOS software in lightweight mode.
Understanding How Converted Access Points Send Crash Information to the Controller

When a converted access point unexpectedly reboots, the access point stores a crash file on its local flash memory at the time of the crash. After the unit reboots, it sends the reason for the reboot to the controller. If the unit rebooted because of a crash, the controller pulls up the crash file using existing CAPWAP messages and stores it in the controller flash memory. The crash info copy is removed from the access point flash memory when the controller pulls it from the access point.

Understanding How Converted Access Points Send Radio Core Dumps to the Controller

When a radio module in a converted access point generates a core dump, the access point stores the core dump file of the radio on its local flash memory at the time of the radio crash. It sends a notification message to the controller indicating which radio generated a core dump file. The controller sends a trap that alerts you so that you can retrieve the radio core file from the access point. The retrieved core file is stored in the controller flash and can be uploaded through TFTP or FTP to an external server for analysis. The core file is removed from the access point flash memory when the controller pulls it from the access point.

This section contains the following topics:
- Retrieving Radio Core Dumps (CLI), page 9-43
- Uploading Radio Core Dumps, page 9-43

Retrieving Radio Core Dumps (CLI)

**Step 1**
Transfer the radio core dump file from the access point to the controller by entering this command:

```
config ap crash-file get-radio-core-dump slot Cisco_AP
```
For the `slot` parameter, enter the slot ID of the radio that crashed.

**Step 2**
Verify that the file was downloaded to the controller by entering this command:

```
show ap crash-file
```
Information similar to the following appears:

```
Local Core Files:
lrad_AP1130.rdump0   (156)
```
The number in parentheses indicates the size of the file. The size should be greater than zero if a core dump file is available.

Uploading Radio Core Dumps

This section contains the following topics:
- Uploading Radio Core Dumps (GUI), page 9-44
- Uploading Radio Core Dumps (CLI), page 9-44
Uploading Radio Core Dumps (GUI)

**Step 1** Choose **Commands > Upload File** to open the Upload File from Controller page.

**Figure 9-13** Upload File from Controller Page

Step 2 From the File Type drop-down list, choose **Radio Core Dump**.

Step 3 From the Transfer Mode drop-down list, choose **TFTP** or **FTP**.

Step 4 In the IP Address text box, enter the IP address of the TFTP or FTP server.

Step 5 In the File Path text box, enter the directory path of the file.

Step 6 In the File Name text box, enter the name of the radio core dump file.

**Note** The filename that you enter should match the filename generated on the controller. You can determine the filename on the controller by entering the **show ap crash-file** command.

Step 7 If you chose FTP as the Transfer Mode, follow these steps:

a. In the Server Login Username text box, enter the FTP server login name.

b. In the Server Login Password text box, enter the FTP server login password.

c. In the Server Port Number text box, enter the port number of the FTP server. The default value for the server port is 21.

Step 8 Click **Upload** to upload the radio core dump file from the controller. A message appears indicating the status of the upload.

Uploading Radio Core Dumps (CLI)

**Step 1** Transfer the file from the controller to a TFTP or FTP server by entering these commands:

- `transfer upload mode {tftp | ftp}`
- `transfer upload datatype radio-core-dump`
- `transfer upload serverip server_ip_address`
- `transfer upload path server_path_to_file`
Converting Autonomous Access Points to Lightweight Mode

Note
The filename that you enter should match the filename generated on the controller. You can determine the filename on the controller by entering the show ap crash-file command.

Note
Ensure that the filename and server_path_to_file do not contain these special characters: \, :, *, ?, " , <, >, and |. You can use only / (forward slash) as the path separator. If you use the disallowed special characters in the filename, then the special characters are replaced with _ (underscores); and if you use the disallowed special characters in the server_path_to_file, then the path is set to the root path.

Step 2
If you are using an FTP server, also enter these commands:

- transfer upload username username
- transfer upload password password
- transfer upload port port

Note
The default value for the port parameter is 21.

Step 3
View the updated settings by entering this command:

transfer upload start

Step 4
When prompted to confirm the current settings and start the software upload, answer y.

Uploading Memory Core Dumps from Converted Access Points

By default, access points converted to lightweight mode do not send memory core dumps to the controller.

This section contains the following topics:
- Uploading Access Point Core Dumps (GUI), page 9-45
- Uploading Access Point Core Dumps (CLI), page 9-46

Uploading Access Point Core Dumps (GUI)

Step 1
Choose Wireless > Access Points > All APs > access point name > and choose the Advanced tab to open the All APs > Details for (Advanced) page.
Converting Autonomous Access Points to Lightweight Mode

Figure 9-14  All APs > Details for (Advanced) Page

Step 2  Select the **AP Core Dump** check box to upload a core dump of the access point.

Step 3  In the TFTP Server IP text box, enter the IP address of the TFTP server.

Step 4  In the File Name text box, enter a name of the access point core dump file (such as `dump.log`).

Step 5  Select the **File Compression** check box to compress the access point core dump file. When you enable this option, the file is saved with a `.gz` extension (such as `dump.log.gz`). This file can be opened with WinZip.

Step 6  Click **Apply** to commit your changes.

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

---

**Uploading Access Point Core Dumps (CLI)**

Step 1  Upload a core dump of the access point by entering this command on the controller:

```plaintext
config ap core-dump enable tftp_server_ip_address filename {compress | uncompress} {ap_name | all}
```

where

- `tftp_server_ip_address` is the IP address of the TFTP server to which the access point sends core dump files.
- `filename` is the name that the access point uses to label the core file.
- `compress` configures the access point to send compressed core files whereas `uncompress` configures the access point to send uncompressed core files.

**Note**  The access point must be able to reach the TFTP server.

- When you choose `compress`, the file is saved with a `.gz` extension (for example, `dump.log.gz`). This file can be opened with WinZip.
• ap_name is the name of a specific access point for which core dumps are uploaded and all is all access points converted to lightweight mode.

**Step 2**
Save your changes by entering this command:
```
save config
```

---

**Viewing the AP Crash Log Information**

Whenever the controller reboots or upgrades, the AP crash log information gets deleted from the controller. We recommend that you make a backup of AP crash log information before rebooting or upgrading the controller.

This section contains the following topics:

- Viewing the AP Crash Log information (GUI), page 9-47
- Viewing the AP Crash Log information (CLI), page 9-47

**Viewing the AP Crash Log information (GUI)**

**Step 1**
Choose Management > Tech Support > AP Crash Log to open the AP Crash Logs page.

**Viewing the AP Crash Log information (CLI)**

**Step 1**
Verify that the crash file was downloaded to the controller by entering this command:
```
show ap crash-file
```
Information similar to the following appears:
```
Local Core Files:
lrad_AP1130.rdump0 (156)
```
Converting Autonomous Access Points to Lightweight Mode

Chapter 9      Controlling Lightweight Access Points

Displaying MAC Addresses for Converted Access Points

There are some differences in the way that controllers display the MAC addresses of converted access points on information pages in the controller GUI:

- On the AP Summary page, the controller lists the Ethernet MAC addresses of converted access points.
- On the AP Detail page, the controller lists the BSS MAC addresses and Ethernet MAC addresses of converted access points.
- On the Radio Summary page, the controller lists converted access points by radio MAC address.

Disabling the Reset Button on Access Points Converted to Lightweight Mode

You can disable the reset button on access points converted to lightweight mode. The reset button is labeled MODE on the outside of the access point.

Use this command to disable or enable the reset button on one or all converted access points associated to a controller:

```
config ap reset-button {enable | disable} {ap-name | all}
```

The reset button on converted access points is enabled by default.

Configuring a Static IP Address on a Lightweight Access Point

If you want to specify an IP address for an access point rather than having one assigned automatically by a DHCP server, you can use the controller GUI or CLI to configure a static IP address for the access point. Static IP addresses are generally used only for deployments with a limited number of users.

An access point cannot discover the controller using domain name system (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs. Previously, these parameters could be configured only using the CLI, but controller software release 6.0 or later releases expand this functionality to the GUI.

Note

If you configure an access point to use a static IP address that is not on the same subnet on which the access point’s previous DHCP address was, the access point falls back to a DHCP address after the access point reboots. If the access point falls back to a DHCP address, enter the **show ap config general Cisco_AP** CLI command to show that the access point is using a fallback IP address. However, the GUI shows both the static IP address and the DHCP address, but it does not identify the DHCP address as a fallback address.

This section contains the following topics:
Configuring a Static IP Address (GUI)

**Step 1** Choose Wireless > Access Points > All APs to open the All APs page.

**Step 2** Click the name of the access point for which you want to configure a static IP address. The All APs > Details for (General) page appears.

**Figure 9-16 All APs > Details for (General) Page**

**Step 3** Under IP Config, select the Static IP check box if you want to assign a static IP address to this access point. The default value is unselected.

**Step 4** Enter the static IP address, netmask, and default gateway in the corresponding text boxes.

**Step 5** Click Apply to commit your changes. The access point reboots and rejoins the controller, and the static IP address that you specified in Step 4 is sent to the access point.

**Step 6** After the static IP address has been sent to the access point, you can configure the DNS server IP address and domain name as follows:

a. In the DNS IP Address text box, enter the IP address of the DNS server.

b. In the Domain Name text box, enter the name of the domain to which the access point belongs.

c. Click Apply to commit your changes.

d. Click Save Configuration to save your changes.


**Converting Autonomous Access Points to Lightweight Mode**

**Chapter 9      Controlling Lightweight Access Points**

**Configuring a Static IP Address (CLI)**

**Step 1**
Configure a static IP address on the access point by entering this command:

```
config ap static-ip enable Cisco_AP ip_address mask gateway
```

*Note*  
To disable static IP for the access point, enter the `config ap static-ip disable Cisco_AP` command.

**Step 2**
Save your changes by entering this command:

```
save config
```

The access point reboots and rejoins the controller, and the static IP address that you specified in Step 1 is pushed to the access point.

**Step 3**
After the static IP address has been sent to the access point, you can configure the DNS server IP address and domain name as follows:

a. To specify a DNS server so that a specific access point or all access points can discover the controller using DNS resolution, enter this command:

```
config ap static-ip add nameserver {Cisco_AP | all} ip_address
```

*Note*  
To delete a DNS server for a specific access point or all access points, enter the `config ap static-ip delete nameserver {Cisco_AP | all}` command.

b. To specify the domain to which a specific access point or all access points belong, enter this command:

```
config ap static-ip add domain {Cisco_AP | all} domain_name
```

*Note*  
To delete a domain for a specific access point or all access points, enter this command:

```
config ap static-ip delete domain {Cisco_AP | all}
```

c. To save your changes, enter this command:

```
save config
```

**Step 4**
See the IP address configuration for the access point by entering this command:

```
show ap config general Cisco_AP
```

Information similar to the following appears:

```
Cisco AP Identifier.............................. 4
Cisco AP Name..................................... AP6
...
IP Address Configuration.......................... Static IP assigned
IP Address......................................... 10.10.10.118
IP NetMask........................................... 255.255.255.0
Gateway IP Addr.................................... 10.10.10.1
Domain............................................. Domain1
Name Server....................................... 10.10.10.205
...
```
Supporting Oversized Access Point Images

Controller software release 5.0 or later releases allow you to upgrade to an oversized access point image by automatically deleting the recovery image to create sufficient space. This feature affects only access points with 8 MB of flash (the 1100, 1200, and 1310 series access points). All newer access points have a larger flash size than 8 MB.

Note
As of August 2007, there are no oversized access point images, but as new features are added, the access point image size will continue to grow.

The recovery image provides a backup image that can be used if an access point power-cycles during an image upgrade. The best way to avoid the need for access point recovery is to prevent an access point from power-cycling during a system upgrade. If a power-cycle occurs during an upgrade to an oversized access point image, you can recover the access point using the TFTP recovery procedure.

Recovering the Access Point (Using the TFTP Recovery Procedure)

Step 1  Download the required recovery image from Cisco.com (c1100-rcvk9w8-mx, c1200-rcvk9w8-mx, or c1310-rcvk9w8-mx) and install it in the root directory of your TFTP server.

Step 2  Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the controller to download the oversized access point image and complete the upgrade procedure.

Step 3  After the access point has been recovered, you may remove the TFTP server.

Configuring OfficeExtend Access Points

This section contains the following topics:

- Information About OfficeExtend Access Points, page 9-52
- OEAP 600 Series Access Points, page 9-52
- Implementing Security, page 9-61
- Licensing for an OfficeExtend Access Point, page 9-62
- Configuring OfficeExtend Access Points, page 9-62
- Configuring a Personal SSID on an OfficeExtend Access Point, page 9-67
- Viewing OfficeExtend Access Point Statistics, page 9-69
- Additional References, page 9-70
Information About OfficeExtend Access Points

An OfficeExtend access point provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee’s residence. The user’s experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Figure 9-17 shows a typical OfficeExtend access point setup.

![Figure 9-17 Typical OfficeExtend Access Point Setup](image)

Note

OfficeExtend access points are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), enabling an entire group of computers to be represented by a single IP address. In controller software release 6.0 or later releases, only one OfficeExtend access point can be deployed behind a NAT device. Prior controller releases could support only one device.

Currently, Cisco 1040, 1130, 1140, 3502I, and 3600 series access points that are associated with a controller can be configured to operate as OfficeExtend access points.

OEAP 600 Series Access Points

This section details the requirements for configuring a Cisco wireless LAN controller for use with the Cisco 600 Series OfficeExtend Access Point. The 600 Series OfficeExtend Access Point supports split mode operation, and it requires configuration through the WLAN controller in local mode. This section describes the configurations necessary for proper connection and supported feature sets.

Note

The Cisco 600 Series OfficeExtend access points are designed to work behind a router or other gateway device that is using Network Address Translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), enabling an entire group of computers to be represented by a single IP address. In controller software release 6.0 or later releases, only one OfficeExtend access point can be deployed behind a single NAT device.
The CAPWAP UDP 5246 and 5247 ports must be open on the firewall between the WLAN controller and the 600 Series OfficeExtend Access Point.

This section contains the following topics:
- Supported Controller Platforms, page 9-53
- OEAP in Local Mode, page 9-53
- Supported WLAN Settings for 600 Series OfficeExtend Access Point, page 9-54
- WLAN Security Settings for the 600 Series OfficeExtend Access Point, page 9-55
- Authentication Settings, page 9-58
- Supported User Count on 600 Series OfficeExtend Access Point, page 9-58
- Remote LAN Settings, page 9-59
- Channel Management and Settings, page 9-60
- Additional Caveats, page 9-61

**Supported Controller Platforms**

The 600 Series OfficeExtend Access Point is supported on the Cisco 5508 Series Controller, WISM-2, and Cisco 2500 Series Controllers and requires the controller software 7.0.116.0 release.

The 600 Series OfficeExtend Access Point has DTLS permanently enabled. You cannot disable DTLS on this access point.

**OEAP in Local Mode**

The 600 Series OfficeExtend Access Point connects to the controller in local mode. You cannot alter these settings.

**Note**

Monitor mode, flexconnect mode, sniffer mode, rogue detector, bridge, and SE-Connect are not supported on the 600 Series Office Extend Access Point and are not configurable.
Configuring OfficeExtend Access Points

Figure 9-18 OEAP Mode

Supported WLAN Settings for 600 Series OfficeExtend Access Point

The 600 Series OfficeExtend Access Point supports a maximum of three WLANs and one remote LAN. If your network deployment has more than three WLANs, you must place the 600 Series OfficeExtend Access Point in an AP group. If the 600 Series OfficeExtend Access Points are added to an AP group, the same limit of three WLANs and one remote LAN still applies for the configuration of the AP group.

If the 600 Series OfficeExtend Access Point is in the default group, which means that it is not in a defined AP group, the WLAN/remote LAN IDs must be set lower than ID 8.

Figure 9-19 WLAN ID for OEAP

If additional WLANs or remote LANs are created with the intent of changing the WLANs or remote LAN being used by the 600 Series OfficeExtend Access Point, you must disable the current WLANs or remote LAN that you are removing before enabling the new WLANs or remote LAN on the 600 Series OfficeExtend Access Point. If there are more than one remote LANs enabled for an AP group, disable all remote LANs and then enable only one of them.

If more than three WLANs are enabled for an AP group, disable all WLANs and then enable only three of them.
WLAN Security Settings for the 600 Series OfficeExtend Access Point

When configuring the security settings in the WLAN, note that there are specific elements that are not supported on the 600 Series OfficeExtend Access Point. CCX is not supported on the 600 Series OfficeExtend Access Point, and elements related to CCX are not supported.

For Layer 2 Security, the following options are supported for the 600 Series OfficeExtend Access Point:

- None
- WPA+WPA2
- Static WEP
- 802.1X (only for remote LANs)

Figure 9-20 WLAN Security Settings

From the Auth Key Mgmt drop-down list, do not select CCKM in WPA + WPA2 settings; select only 802.1X or PSK.

Figure 9-21 WLAN Security Settings
Security encryption settings must be identical for WPA and WPA2 for TKIP and AES. The following are examples of incompatible settings for TKIP and AES.

Figure 9-22 and Figure 9-23 show the incompatible configuration.

**Figure 9-22** Incompatible WPA and WPA2 Security Encryption Settings for OEAP 600 Series

The following are examples of compatible settings:

**Figure 9-24** Compatible Security Settings for OEAP Series
QoS settings are supported, but CAC is not supported and should not be enabled.

**Note**
Do not enable Coverage Hole Detection.

**Note**
Aironet IE should not be enabled. This option is not supported.

MFP is also not supported and should be disabled or set to optional.
Client Load Balancing and Client Band Select are not supported.

**Authentication Settings**

For authentication on the 600 Series OfficeExtend Access Point, LEAP is not supported. This configuration needs to be addressed on the clients and RADIUS servers to migrate them to EAP-Fast, EAP-TTLS, EAP-TLS, or PEAP.

If Local EAP is being utilized on the controller, the settings would also have to be modified not to utilize LEAP.

**Supported User Count on 600 Series OfficeExtend Access Point**

Only 15 users are allowed to connect on the WLAN Controller WLANs provided on the 600 Series OfficeExtend Access Point at any one time, a sixteenth user cannot authenticate until one of the first clients is deauthenticated or timeout on the controller occurs. This number is cumulative across the controller WLANs on the 600 Series OfficeExtend Access Point.
For example, if two controller WLANs are configured and there are fifteen users on one of the WLANs, no users can join the other WLAN on the 600 Series OfficeExtend Access Point at that time. This limit does not apply to the local private WLANs that the end user configures on the 600 Series OfficeExtend Access Point for personal use. Clients connected on these private WLANs or on the wired ports do not affect these limits.

### Remote LAN Settings

Only four clients can connect through a remote LAN port on the 600 Series OfficeExtend Access Point. This number does not affect the fifteen user limit imposed for the Controller WLANs. The remote LAN client limit supports connecting a switch or hub to the remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices can connect until one of the devices is idle for more than one minute.

Remote LAN is configured in the same way that a WLAN or Guest LAN is configured on the controller.

**Figure 9-29 Remote LAN Settings for OEAP 600 Series AP**

Security settings can be left open, set for MAC filtering, or set for Web Authentication. The default is to use MAC filtering. Additionally, you can specify 802.1X Layer 2 security settings.

The following figure shows Layer 2 security settings for OEAP 600 Series APs in a remote LAN.

**Figure 9-30 Layer 2 Security Settings for OEAP 600 Series APs in Remote LANs**

**Figure 9-31** shows the Layer 3 security configuration.
Channel Management and Settings

The radios for the 600 Series OfficeExtend Access Point are controlled through the Local GUI on the access point and not through the Wireless LAN Controller. Attempting to control the spectrum channel or power, or to disable the radios through the controller does not have effect on the 600 Series OfficeExtend Access Point. RRM is not supported on the 600 Series OfficeExtend Access Point.

The 600 series scans and chooses channels for 2.4 GHz and 5.0 GHz during startup as long as the default settings on the local GUI are left as default in both spectrums.

The channel bandwidth for 5.0 GHz is also configured on the 600 Series OfficeExtend Access Point Local GUI, for 20 MHz or 40 MHz wide channels. Setting the channel width to 40 MHz for 2.4 GHz is not supported and fixed at 20 MHz.
Additional Caveats

The 600 Series OfficeExtend Access Points are designed for single AP deployments, therefore client roaming between 600 Series OfficeExtend Access Points is not supported.

Disabling the 802.11a/n or 802.11b/g/n on the controller may not disable these spectrums on the 600 Series OfficeExtend Access Point since local SSID may be still working.

**Note**

Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.

Implementing Security

**Note**

Configuring LSC is not a requirement but an option. The OfficeExtend access points do not support LSC.

**Step 1**

Use local significant certificates (LSCs) to authorize your OfficeExtend access points, by following the instructions in the “Authorizing Access Points Using LSCs” section on page 9-31.

**Step 2**

Implement AAA server validation using the access point’s MAC address, name, or both as the username in authorization requests, by entering this command:

```
config auth-list ap-policy authorize-ap username { ap_mac | Cisco_AP | both }
```

Using the access point name for validation can ensure that only the OfficeExtend access points of valid employees can join the controller. To implement this security policy, make sure to name each OfficeExtend access point with an employee ID or employee number. When an employee is terminated, run a script to remove this user from the AAA server database, which prevents that employee’s OfficeExtend access point from joining the network.

**Step 3**

Enter the `save config` command to save your configuration.
CCX is not supported on the 600 OEAP. Elements related to CCX are not supported. Also, only 802.1x or PSK is supported. TKIP and AES security encryption settings must be identical for WPA and WPA2.

Licensing for an OfficeExtend Access Point

To use OfficeExtend access points, a base license must be installed and in use on the controller. After the license is installed, you can enable the OfficeExtend mode on an 1130 series, a 1140 series, a 1040 series, a 3500 (integrated antenna) series, or a 3600 (integrated antenna) series access point.

Note

See Chapter 4, “Configuring Controller Settings,” for information on obtaining and installing licenses.

Configuring OfficeExtend Access Points

After the 1130 series, 1140 series, 1040 series, 3500 (integrated antenna) series, or 3600 (integrated antenna) series access point has joined the controller, you can configure it as an OfficeExtend access point.

Note

Configuring LSC is not a requirement but an option. The OfficeExtend access points do not support LSC.

This section contains the following topics:

• Configuring OfficeExtend Access Points (GUI), page 9-62
• Configuring OfficeExtend Access Points (CLI), page 9-65

Configuring OfficeExtend Access Points (GUI)

Step 1
Choose Wireless to open the All APs page.

Step 2
Click the name of the desired access point to open the All APs > Details page.

Step 3
Enable FlexConnect on the access point as follows:

a. In the General tab, choose FlexConnect from the AP Mode drop-down list to enable FlexConnect for this access point.

Note
For more information on FlexConnect, see Chapter 16, “Configuring FlexConnect.”

Step 4
Configure one or more controllers for the access point as follows:

a. Click the High Availability tab.

b. Enter the name and IP address of the primary controller for this access point in the Primary Controller Name and Management IP Address text boxes.

Note
You must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.
c. If desired, enter the name and IP address of a secondary or tertiary controller (or both) in the corresponding Controller Name and Management IP Address text boxes.

d. Click **Apply** to commit your changes. The access point reboots and then rejoins the controller.

**Note**  
The names and IP addresses must be unique for the primary, secondary, and tertiary controllers.

**Step 5**  
Enable OfficeExtend access point settings as follows:

a. Click the **FlexConnect** tab.

**Figure 9-34  All APs > Details > Details for FlexConnect**

b. Select the **Enable OfficeExtend AP** check box to enable the OfficeExtend mode for this access point. The default value is selected.

Unselecting this check box disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point’s configuration and return it to the factory-default settings, enter `clear ap config Cisco_AP` on the controller CLI. If you want to clear only the access point’s personal SSID, click **Reset Personal SSID**.

**Note**  
Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable rogue detection for a specific access point by selecting the **Rogue Detection** check box on the All APs > Details for (Advanced) page. Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. See the “Managing Rogue Devices” section on page 7-81 for more information on rogue detection.

**Note**  
DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point by selecting the **Data Encryption** check box on the All APs > Details for (Advanced) page. See the “Configuring Data Encryption” section on page 9-3 for more information on DTLS data encryption.
Configuring OfficeExtend Access Points

Chapter 9 Controlling Lightweight Access Points

**Note**
Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point by selecting the Telnet or SSH check box on the All APs > Details for (Advanced) page. See the “Troubleshooting Access Points Using Telnet or SSH” section on page 18-49 for more information on Telnet and SSH.

**Note**
Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point by selecting the Enable Link Latency check box on the All APs > Details for (Advanced) page. See the “Configuring Link Latency” section on page 9-105 for more information on this feature.

c. Select the Enable Least Latency Controller Join check box if you want the access point to choose the controller with the least latency when joining. Otherwise, leave this check box unselected, which is the default value. When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the Cisco 5500 Series Controller that responds first.

d. Click Apply to commit your changes.

The OfficeExtend AP text box on the All APs page shows which access points are configured as OfficeExtend access points.

**Step 6** Configure a specific username and password for the OfficeExtend access point so that the user at home can log into the GUI of the OfficeExtend access point:

a. Click Credentials tab.

b. Select the Over-ride Global Credentials check box to prevent this access point from inheriting the global username, password, and enable password from the controller. The default value is unselected.

c. In the Username, Password, and Enable Password text boxes, enter the unique username, password, and enable password that you want to assign to this access point.

**Note** The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

d. Click Apply to commit your changes.

**Note** If you want to force this access point to use the controller’s global credentials, unselect the Over-ride Global Credentials check box.

**Step 7** Configure access to local GUI, LAN ports, and local SSID of the OfficeExtend access points:

a. Choose WIRELESS > Access Points > Global Configuration to open the Global Configuration page.

b. Under OEAP Config Parameters, select or unselect the Disable Local Access check box to enable or disable local access of the OfficeExtend access points.
Note: By default, the Disable Local Access check box is unselected and therefore the Ethernet ports and personal SSIDs are enabled. This configuration does not affect remote LAN. The port is enabled only when you configure a remote LAN.

Step 8: Click Save Configuration to save your changes.

Step 9: If your controller supports only OfficeExtend access points, see the “Configuring RRM” section on page 13-5 for instructions on setting the recommended values for the DCA interval, channel scan duration, and neighbor packet frequency.

Configuring OfficeExtend Access Points (CLI)

Step 1: Enable FlexConnect on the access point by entering this command:

```
config ap mode flexconnect Cisco_AP
```

Note: For more information on FlexConnect, see Chapter 16, “Configuring FlexConnect.”

Step 2: Configure one or more controllers for the access point by entering one or all of these commands:

```
config ap primary-base controller_name Cisco_AP controller_ip_address
config ap secondary-base controller_name Cisco_AP controller_ip_address
config ap tertiary-base controller_name Cisco_AP controller_ip_address
```

Note: You must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Note: The names and IP addresses must be unique for the primary, secondary, and tertiary controllers.

Step 3: Enable the OfficeExtend mode for this access point by entering this command:

```
config flexconnect office-extend { enable | disable } Cisco_AP
```

The default value is enabled. The disable parameter disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point’s configuration and return it to the factory-default settings, enter this command:

```
clear ap config Cisco_AP
```

If you want to clear only the access point’s personal SSID, enter this command:

```
config flexconnect office-extend clear-personalssid-config Cisco_AP
```
Chapter 9 Controlling Lightweight Access Points

Configuring OfficeExtend Access Points

Note: Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable rogue detection for a specific access point or for all access points using the `config rogue detection {enable | disable} {Cisco_AP | all}` command. Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. See the "Managing Rogue Devices" section on page 7-81 for more information on rogue detection.

Note: DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point or for all access points using the `config ap link-encryption {enable | disable} {Cisco_AP | all}` command. See the "Configuring Data Encryption" section on page 9-3 for more information on DTLS data encryption.

Note: Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point using the `config ap {telnet | ssh} {enable | disable} Cisco_AP` command. See the "Troubleshooting Access Points Using Telnet or SSH" section on page 18-49 for more information on Telnet and SSH.

Note: Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point or for all access points currently associated to the controller using the `config ap link-latency {enable | disable} {Cisco_AP | all}` command. See the "Configuring Link Latency" section on page 9-105 for more information on this feature.

Step 4: Enable the access point to choose the controller with the least latency when joining by entering this command:

`config flexconnect join min-latency {enable | disable} Cisco_AP`

The default value is disabled. When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the Cisco 5500 Series Controller that responds first.

Step 5: Configure a specific username and password that users at home can enter to log into the GUI of the OfficeExtend access point by entering this command:

`config ap mgmtuser add username user password password enablesecret enable_password Cisco_AP`

The credentials that you enter in this command are retained across controller and access point reboots and if the access point joins a new controller.

Note: If you want to force this access point to use the controller’s global credentials, enter the `config ap mgmtuser delete Cisco_AP` command. The following message appears after you execute this command: “AP reverted to global username configuration.”
Step 6  To configure access to the local network for the Cisco 600 Series OfficeExtend access points, enter the following command:

```
config network oeap-600 local-network {enable | disable}
```

When disabled, the local SSIDs, local ports are inoperative; and the console is not accessible. When reset, the default restores local access. This configuration does not affect the remote LAN configuration if configured on the access points.

Step 7  Configure the Dual R-LAN Ports feature, which allows the Ethernet port 3 of Cisco 600 Series OfficeExtend access points to operate as a remote LAN by entering this command:

```
config network oeap-600 dual-rlan-ports {enable | disable}
```

This configuration is global to the controller and is stored by the AP and the NVRAM variable. When this variable is set, the behavior of the remote LAN is changed. This feature supports different remote LANs per remote LAN port.

The remote LAN mapping is different depending on whether the default group or AP Groups is used:
- Default Group—If you are using the default group, a single remote LAN with an even numbered remote LAN ID is mapped to port 4. For example, a remote LAN with remote LAN ID 2 is mapped to port 4 (on the Cisco 600 OEAP). The remote LAN with an odd numbered remote LAN ID is mapped to port 3 (on the Cisco 600 OEAP). For example, a remote LAN with remote LAN ID 1 is mapped to port 3 (on the Cisco 600 OEAP).
- AP Groups—If you are using an AP group, the mapping to the OEAP-600 ports is determined by the order of the AP groups. To use an AP group, you must first delete all remote LANs and WLANs from the AP group leaving it empty. Then, add the two remote LANs to the AP group adding the port 3 AP remote LAN first, and the port 4 remote group second, followed by any WLANs.

Step 8  Save your changes by entering this command:

```
save config
```

Step 9  If your controller supports only OfficeExtend access points, see the “Configuring RRM” section on page 13-5 for instructions on setting the recommended value for the DCA interval.

---

## Configuring a Personal SSID on an OfficeExtend Access Point

Step 1  Find the IP address of your OfficeExtend access point by doing one of the following:
- Log into your home router and look for the IP address of your OfficeExtend access point.
- Ask your company’s IT professional for the IP address of your OfficeExtend access point.
- Use an application such as Network Magic to detect devices on your network and their IP addresses.

Step 2  With the OfficeExtend access point connected to your home router, enter the IP address of the OfficeExtend access point in the Address text box of your Internet browser and click Go.

**Note**  Make sure that you are not connected to your company’s network using a virtual private network (VPN) connection.

Step 3  When prompted, enter the username and password to log into the access point.

Step 4  On the OfficeExtend Access Point Welcome page, click Enter. The OfficeExtend Access Point Home page appears.
This page shows the access point name, IP address, MAC address, software version, status, channel, transmit power, and client traffic.

**Step 5** Choose **Configuration** to open the Configuration page.

**Step 6** Select the **Personal SSID** check box to enable this wireless connection. The default value is disabled.

**Step 7** In the SSID text box, enter the personal SSID that you want to assign to this access point. This SSID is locally switched.
Configuring OfficeExtend Access Points

Step 8 From the Security drop-down list, choose Open, WPA2/PSK (AES), or 104 bit WEP to set the security type to be used by this access point.

Note If you choose WPA2/PSK (AES), make sure that the client is configured for WPA2/PSK and AES encryption.

Step 9 If you chose WPA2/PSK (AES) in Step 8, enter an 8- to 38-character WPA2 passphrase in the Secret text box. If you chose 104 bit WEP, enter a 13-character ASCII key in the Key text box.

Step 10 Click Apply to commit your changes.

Note If you want to use the OfficeExtend access point for another application, you can clear this configuration and return the access point to the factory-default settings by clicking Clear Config. You can also clear the access point’s configuration from the controller CLI by entering the clear ap config Cisco_AP command.

Viewing OfficeExtend Access Point Statistics

Use these commands to view information about the OfficeExtend access points on your network:

1. See a list of all OfficeExtend access points by entering this command:

   show flexconnect office-extend summary

   Information similar to the following appears:

   Summary of OfficeExtend AP
   AP Name   Ethernet MAC    Encryption    Join-Mode    Join-Time
   ------------------- ------------------- ----------- ----------- ----------------------------

2. See the link delay for OfficeExtend access points by entering this command:

   show flexconnect office-extend latency

   Information similar to the following appears:

   Summary of OfficeExtend AP link latency
   AP Name   Status    Current    Maximum    Minimum
   ----------- ----------- ---------- ---------- ---------
   AP1130    Enabled    15 ms     45 ms     12 ms
   AP1140    Enabled    14 ms     179 ms    12 ms

3. See the encryption state of all access points or a specific access point by entering this command:

   show ap link-encryption [all | Cisco_AP]

   Information similar to the following appears:

   Encryption Dnstream Upstream Last
This command also shows authentication errors, which track the number of integrity check failures, and replay errors, which track the number of times that the access point receives the same packet. See the data plane status for all access points or a specific access point by entering this command:

```
show ap data-plane {all | Cisco_AP}
```

Information similar to the following appears:

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Min Data Round Trip</th>
<th>Max Data Round Trip</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP1130</td>
<td>0.012s</td>
<td>0.020s</td>
<td>13:46:23</td>
</tr>
<tr>
<td>AP1140</td>
<td>0.012s</td>
<td>0.111s</td>
<td>13:46:46</td>
</tr>
</tbody>
</table>

- To join the statistics for the OfficeExtend access points, see “Viewing Access Point Join Information (CLI)” section on page 9-41.

### Additional References

- To troubleshoot OfficeExtend access points, see Appendix 18, “Troubleshooting”.

### Using Cisco Workgroup Bridges

This section contains the following topics:

- Information About Cisco Workgroup Bridges, page 9-70
- Guidelines and Limitations, page 9-71
- WGB Configuration Example, page 9-73
- Viewing the Status of Workgroup Bridges, page 9-73
- Debugging WGB Issues (CLI), page 9-75

### Information About Cisco Workgroup Bridges

A workgroup bridge (WGB) is a mode that can be configured on an autonomous IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging. The WGB provides wireless access connectivity to wired clients by establishing a single wireless connection to the lightweight access point. The lightweight access point treats the WGB as a wireless client. See the example in Figure 9-37.
Guidelines and Limitations

- The WGB can be any autonomous access point that supports the workgroup bridge mode and is running Cisco IOS Release 12.4(3g)JA or later releases (on 32-MB access points) or Cisco IOS Release 12.3(8)JEB or later releases (on 16-MB access points). These access points include the AP1120, AP1121, AP1130, AP1231, AP1240, and AP1310. Cisco IOS releases prior to 12.4(3g)JA and 12.3(8)JEB are not supported.

Note: If your access point has two radios, you can configure only one for workgroup bridge mode. This radio is used to connect to the lightweight access point. We recommend that you disable the second radio.

Enable the workgroup bridge mode on the WGB as follows:

- On the WGB access point GUI, choose **Workgroup Bridge** for the role in radio network on the Settings > Network Interfaces page.
- On the WGB access point CLI, enter the `station-role workgroup-bridge` command.

Note: See the sample WGB access point configuration in the “WGB Configuration Example” section on page 9-73.

- The WGB can associate only to lightweight access points.
- Perform one of the following to enable client mode on the WGB:
  - On the WGB access point GUI, choose **Disabled** for the Reliable Multicast to WGB parameter.
  - On the WGB access point CLI, enter the `no infrastructure client` command.

Note: VLANs are not supported for use with WGBs.
Note: See the sample WGB access point configuration in the “WGB Configuration Example” section on page 9-73.

- These features are supported for use with a WGB:
  - Guest N+1 redundancy
  - Local EAP
  - Open, WEP 40, WEP 128, CKIP, WPA+TKIP, WPA2+AES, LEAP, EAP-FAST, and EAP-TLS authentication modes
  - Cisco Centralized Key Management (CCKM)
- These features are not supported for use with a WGB:
  - FlexConnect
  - Idle timeout
  - Web authentication

Note: If a WGB associates to a web-authentication WLAN, the WGB is added to the exclusion list, and all of the WGB wired clients are deleted.

- The WGB supports a maximum of 20 wired clients. If you have more than 20 wired clients, use a bridge or another device.
- Wired clients connected to the WGB are not authenticated for security. Instead, the WGB is authenticated against the access point to which it associates. Therefore, we recommend that you physically secure the wired side of the WGB.
- With Layer 3 roaming, if you plug a wired client into the WGB network after the WGB has roamed to another controller (for example, to a foreign controller), the wired client’s IP address displays only on the anchor controller, not on the foreign controller.
- If a wired client does not send traffic for an extended period of time, the WGB removes the client from its bridge table, even if traffic is continuously being sent to the wired client. As a result, the traffic flow to the wired client fails. To avoid the traffic loss, prevent the wired client from being removed from the bridge table by configuring the aging-out timer on the WGB to a large value using the following Cisco IOS commands on the WGB:

```
configure terminal
bridge bridge-group-number aging-time seconds
exit
end
```

where `bridge-group-number` is a value between 1 and 255, and `seconds` is a value between 10 and 1,000,000 seconds. We recommend configuring the `seconds` parameter to a value greater than the wired client’s idle period.
- When you delete a WGB record from the controller, all of the WGB wired clients’ records are also deleted.
- Wired clients connected to a WGB inherit the WGB’s QoS and AAA override attributes.
- These features are not supported for wired clients connected to a WGB:
  - MAC filtering
  - Link tests
- Idle timeout

- To enable the WGB to communicate with the lightweight access point, create a WLAN and make sure that Aironet IE is enabled.

- Wired clients behind a WGB cannot connect to a DMZ/Anchor controller. To enable wired clients behind a WGB to connect to an anchor controller in a DMZ, you must enable VLANs in the WGB using the `config wgb vlan enable` command.

- If you have to apply ACL to WGB during run time, do not modify the ACL configuration for interface in the controller during run time. If you need to modify any ACLs, then you must disable all WLANs that are in the controller or disable both the 802.11a and 80.11b networks. Also, ensure that there are no clients associated and mapped to that interface and then you can modify the ACL settings.

### WGB Configuration Example

The following is an example of the configuration of a WGB access point using static WEP with a 40-bit WEP key:

```
ap# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)# dot11 ssid WGB_with_static_WEP
ap(config-ssid)# authentication open
ap(config-ssid)# guest-mode
ap(config-ssid)# exit
ap(config)# interface dot11Radio 0
ap(config)# station-role workgroup-bridge
ap(config-if)# encry mode wep 40
ap(config-if)# encry key 1 size 40 0 1234567890
ap(config-if)# ssid WGB_with_static_WEP
ap(config-if)# end
```

Verify that the WGB is associated to an access point by entering this command on the WGB:

```
show dot11 association
```

Information similar to the following appears:

```
ap# show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address    IP address      Device        Name            Parent         State
000b.8581.6aee 10.11.12.1      WGB-client    map1            -              Assoc
```

### Viewing the Status of Workgroup Bridges

This section contains the following topics:

- Viewing the Status of Workgroup Bridges (GUI), page 9-73
- Viewing the Status of Workgroup Bridges (CLI), page 9-74

### Viewing the Status of Workgroup Bridges (GUI)

**Step 1** Choose Monitor > Clients to open the Clients page.
The WGB text box on the right side of the page indicates whether any of the clients on your network are workgroup bridges.

**Step 2**
Click the MAC address of the desired client. The Clients > Detail page appears.

The Client Type text box under Client Properties shows “WGB” if this client is a workgroup bridge, and the Number of Wired Client(s) text box shows the number of wired clients that are connected to this WGB.

**Step 3**
See the details of any wired clients that are connected to a particular WGB as follows:

a. Click **Back** on the Clients > Detail page to return to the Clients page.

b. Hover your cursor over the blue drop-down arrow for the desired WGB and choose **Show Wired Clients**. The WGB Wired Clients page appears.

**Note**
If you want to disable or remove a particular client, hover your cursor over the blue drop-down arrow for the desired client and choose **Remove** or **Disable**, respectively.

c. Click the MAC address of the desired client to see more details for this particular client. The Clients > Detail page appears.

The Client Type text box under Client Properties shows “WGB Client,” and the rest of the text boxes on this page provide additional information for this client.

### Viewing the Status of Workgroup Bridges (CLI)

**Step 1**
See any WGBs on your network by entering this command:

```plaintext
show wgb summary
```

Information similar to the following appears:

```
Number of WGBs....................... 1

MAC Address    IP Address  AP Name  Status  WLAN  Auth  Protocol  Clients
----------------- -------------- -------- ------  ----  ------ --------- --------
```

Step 2  
See the details of any wired clients that are connected to a particular WGB by entering this command:  
```
show wgb detail wgb_mac_address
```

Information similar to the following appears:

```
Number of wired client(s): 1

+-------------------+--------+------------+-------+-----+
<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>AP Name</th>
<th>Mobility</th>
<th>WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0d:60:fc:d5:0b</td>
<td>10.24.8.75</td>
<td>a1</td>
<td>Local</td>
<td>3</td>
</tr>
</tbody>
</table>
```

---

## Debugging WGB Issues (CLI)

- Enable debugging for IAPP messages, errors, and packets by entering these commands:
  - `debug iapp all enable`—Enables debugging for IAPP messages.
  - `debug iapp error enable`—Enables debugging for IAPP error events.
  - `debug iapp packet enable`—Enables debugging for IAPP packets.
- Debug an roaming issue by entering this command:
  ```
  debug mobility handoff enable
  ```
- Debug an IP assignment issue when DHCP is used by entering these commands:
  - `debug dhcp message enable`
  - `debug dhcp packet enable`
- Debug an IP assignment issue when static IP is used by entering these commands:
  - `debug dot11 mobile enable`
  - `debug dot11 state enable`

---

## Configuring Non-Cisco Workgroup Bridges

This section contains the following topics:

- Information About Non-Cisco Workgroup Bridges, page 9-75
- Guidelines and Limitations, page 9-76

---

## Information About Non-Cisco Workgroup Bridges

When a Cisco workgroup bridge (WGB) is used, the WGB informs the access points of all the clients that it is associated with. The controller is aware of the clients associated with the access point. When non-Cisco WGBs are used, the controller has no information about the IP address of the clients on the wired segment behind the WGB. Without this information, the controller drops the following types of messages:

- ARP REQ from the distribution system for the WGB client
Guidelines and Limitations

Starting in release 7.0.116.0, the controller can accommodate non-Cisco WGBs so that the controller can forward ARP, DHCP, and data traffic to and from the wired clients behind workgroup bridges by enabling the passive client feature. To configure your controller to work with non-Cisco WGBs, you must enable the passive client feature so that all traffic from the wired clients is routed through the WGB to the access point. All traffic from the wired clients is routed through the workgroup bridge to the access point.

To know more about how to configure the controller to use passive clients, see the “Configuring Passive Clients” section on page 74.

The following restrictions apply to non-Cisco WGB:

- Only Layer 2 roaming is supported for WGB devices.
- Layer 3 security (web authentication) is not support for WGB clients.
- Visibility of wired hosts behind a WGB on a controller is not supported because the non-Cisco WGB device performs MAC hiding. Cisco WGB supports IAPP.
- ARP poisoning detection does not work on a WLAN when the flag is enabled.
- VLAN select is not supported for WGB clients.
- Some third-party WGBs need to operate in non-DHCP relay mode. If problems occur with the DHCP assignment on devices behind the non-Cisco WGB, use the `config dhcp proxy disable` and `config dhcp proxy disable bootp-broadcast disable` commands.

  The default state is DHCP proxy enabled. The best combination depends on the third-party characteristics and configuration.

- When a WGB wired client leaves a multicast group, the downstream multicast traffic to other WGB wired clients is interrupted briefly.
- If you have clients that use PC virtualization software like VMware, you must enable this feature.

**Note**

We have tested multiple third-party devices for compatibility but cannot ensure that all non-Cisco devices work. Support for any interaction or configuration details on the third-party device should be discussed with the device manufacturer.

- You must enable the passive client functionality for all non Cisco workgroup bridges. For more information, see the “Configuring Passive Clients” section on page 74.

- You might need to use the following commands to configure DHCP on clients:
  - Disable DHCP proxy by using the `config dhcp proxy disable` command.
  - Enable DHCP boot broadcast by using the `config dhcp proxy disable bootp-broadcast enable` command.
Configuring Backup Controllers

This section contains the following topics:

- Information About Configuring Backup Controllers, page 9-77
- Guidelines and Limitations, page 9-77
- Configuring Backup Controllers, page 9-78

Information About Configuring Backup Controllers

A single controller at a centralized location can act as a backup for access points when they lose connectivity with the primary controller in the local region. Centralized and regional controllers do not need to be in the same mobility group. In controller software release 4.2 or later releases, you can specify a primary, secondary, and tertiary controller for specific access points in your network. Using the controller GUI or CLI, you can specify the IP addresses of the backup controllers, which allows the access points to fail over to controllers outside of the mobility group.

Guidelines and Limitations

- In controller software release 5.0 or later releases, you can also configure primary and secondary backup controllers (which are used if primary, secondary, or tertiary controllers are not specified or are not responsive) for all access points connected to the controller as well as various timers, including heartbeat timers and discovery request timers. To reduce the controller failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller.

- You can configure the fast heartbeat timer only for access points in local and flexconnect modes.

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

- When an access point’s primary controller comes back online, the access point disassociates from the backup controller and reconnects to its primary controller. The access point falls back to its primary controller and not to any secondary controller for which it is configured. For example, if an access point is configured with primary, secondary, and tertiary controllers, it falls over to the tertiary controller when the primary and secondary controllers become unresponsive and waits for the primary controller to come back online so that it can fall back to the primary controller. The access point does not fall back from the tertiary controller to the secondary controller if the secondary controller comes back online; it stays connected to the tertiary controller until the primary controller comes back up.
If you inadvertently configure a controller that is running software release 5.2 or later releases with a failover controller that is running a different software release (such as 4.2, 5.0, or 5.1), the access point might take a long time to join the failover controller because the access point starts the discovery process in CAPWAP and then changes to LWAPP discovery.

**Configuring Backup Controllers**

- Configuring Backup Controllers (GUI), page 9-78
- Configuring Backup Controllers (CLI), page 9-79

**Configuring Backup Controllers (GUI)**

**Step 1** Choose Wireless > Access Points > Global Configuration to open the Global Configuration page.

**Step 2** From the Local Mode AP Fast Heartbeat Timer State drop-down list, choose Enable to enable the fast heartbeat timer for access points in local mode or choose Disable to disable this timer. The default value is Disable.

**Step 3** If you chose Enable in Step 2, enter the Local Mode AP Fast Heartbeat Timeout text box to configure the fast heartbeat timer for access points in local mode. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure.

The range for the AP Fast Heartbeat Timeout value for Cisco Flex 7500 Controllers is 10–15 (inclusive) and is 1–10 (inclusive) for other controllers. The default value for the heartbeat timeout for Cisco Flex 7500 Controllers is 10. The default value for other controllers is 1 second.

**Step 4** From the FlexConnect Mode AP Fast Heartbeat Timer State drop-down list, choose Enable to enable the fast heartbeat timer for FlexConnect access points or choose Disable to disable this timer. The default value is Disable.

**Step 5** If you enable FlexConnect fast heartbeat, enter the FlexConnect Mode AP Fast Heartbeat Timeout value in the FlexConnect Mode AP Fast Heartbeat Timeout text box. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure.
Step 6  In the AP Primary Discovery Timeout text box, a value between 30 and 3600 seconds (inclusive) to configure the access point primary discovery request timer. The default value is 120 seconds.

Step 7  If you want to specify a primary backup controller for all access points, enter the IP address of the primary backup controller in the Back-up Primary Controller IP Address text box and the name of the controller in the Back-up Primary Controller Name text box.

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

Step 8  If you want to specify a secondary backup controller for all access points, enter the IP address of the secondary backup controller in the Back-up Secondary Controller IP Address text box and the name of the controller in the Back-up Secondary Controller Name text box.

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

Step 9  Click Apply to commit your changes.

Step 10  Configure primary, secondary, and tertiary backup controllers for a specific access point as follows:

a. Choose Access Points > All APs to open the All APs page.

b. Click the name of the access point for which you want to configure primary, secondary, and tertiary backup controllers.

c. Choose the High Availability tab to open the All APs > Details for (High Availability) page.

d. If desired, enter the name and IP address of the primary controller for this access point in the Primary Controller text boxes.

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

e. If desired, enter the name and IP address of the secondary controller for this access point in the Secondary Controller text boxes.

f. If desired, enter the name and IP address of the tertiary controller for this access point in the Tertiary Controller text boxes.

g. Click Apply to commit your changes.

Step 11  Click Save Configuration to save your changes.

Configuring Backup Controllers (CLI)

Step 1  Configure a primary controller for a specific access point by entering this command:
config ap primary-base controller_name Cisco_AP [controller_ip_address]

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

Step 2 Configure a secondary controller for a specific access point by entering this command:
config ap secondary-base controller_name Cisco_AP [controller_ip_address]

Step 3 Configure a tertiary controller for a specific access point by entering this command:
config ap tertiary-base controller_name Cisco_AP [controller_ip_address]

Step 4 Configure a primary backup controller for all access points by entering this command:
config advanced backup-controller primary backup_controller_name backup_controller_ip_address

Step 5 Configure a secondary backup controller for all access points by entering this command:
config advanced backup-controller secondary backup_controller_name backup_controller_ip_address

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

Step 6 Enable or disable the fast heartbeat timer for local or FlexConnect access points by entering this command:
config advanced timers ap-fast-heartbeat {local | flexconnect | all} {enable | disable} interval
where all is both local and FlexConnect access points, and interval is a value between 1 and 10 seconds (inclusive). Specifying a small heartbeat interval reduces the amount of time that it takes to detect a controller failure. The default value is disabled. Configure the access point heartbeat timer by entering this command:
config advanced timers ap-heartbeat-timeout interval
where interval is a value between 1 and 30 seconds (inclusive). This value should be at least three times larger than the fast heartbeat timer. The default value is 30 seconds.

Caution Do not enable the fast heartbeat timer with the high latency link. If you have to enable the fast heartbeat timer, the timer value must be greater than the latency.

Step 7 Configure the access point primary discovery request timer by entering this command:
config advanced timers ap-primary-discovery-timeout interval
where interval is a value between 30 and 3600 seconds. The default value is 120 seconds.

Step 8 Configure the access point discovery timer by entering this command:
config advanced timers ap-discovery-timeout interval
where interval is a value between 1 and 10 seconds (inclusive). The default value is 10 seconds.

Step 9 Configure the 802.11 authentication response timer by entering this command:
config advanced timers auth-timeout interval

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

Step 10
Save your changes by entering this command:

save config

Step 11
See an access point’s configuration by entering these commands:

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

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

Cisco AP Identifier......................... 1
Cisco AP Name................................. AP5
Country code................................. US - United States
Regulatory Domain allowed by Country...... 802.11bg:-AB  802.11a:-AB
AP Country code.............................. US - United States
AP Regulatory Domain......................... 802.11bg:-A  802.11a:-N
Switch Port Number........................... 1
MAC Address................................. 00:13:80:60:48:3e
IP Address Configuration..................... DHCP
IP Address.................................... 1.100.163.133
... Primary Cisco Switch Name.................. 1-4404
Primary Cisco Switch IP Address............. 2.2.2.2
Secondary Cisco Switch Name.................. 1-4404
Secondary Cisco Switch IP Address.......... 2.2.2.2
Tertiary Cisco Switch Name.................... 2-4404
Tertiary Cisco Switch IP Address............. 1.1.1.4
...

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

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

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

Authentication Response Timeout (seconds)... 10
Rogue Entry Timeout (seconds)................ 1300
AP Heart Beat Timeout (seconds).............. 30
AP Discovery Timeout (seconds).............. 10
AP Local mode Fast Heartbeat (seconds)..... 10 (enable)
AP flexconnect mode Fast Heartbeat (seconds)... disable
AP Primary Discovery Timeout (seconds)..... 120

== Configuring Failover Priority for Access Points ==

This section contains the following topics:
- Information About Configuring Failover Priority for Access Points, page 9-82
- Guidelines and Limitations, page 9-82
- Configuring Failover Priority for Access Points, page 9-82
Information About Configuring Failover Priority for Access Points

Each controller has a defined number of communication ports for access points. When multiple controllers with unused access point ports are deployed on the same network and one controller fails, the dropped access points automatically poll for unused controller ports and associate with them.

Guidelines and Limitations

- In controller software releases prior to 5.1, the backup controllers accept association requests in the order that the requests are received until all the ports are in use. As a result, the probability of an access point finding an open port on a backup controller is determined by where in the association request queue it is after the controller failure.
- In controller software release 5.1 or later releases, you can configure your wireless network so that the backup controller recognizes a join request from a higher-priority access point and if necessary disassociates a lower-priority access point as a means to provide an available port.
- Failover priority is not in effect during the regular operation of your wireless network. It takes effect only if there are more association requests after a controller failure than there are available backup controller ports.
- To configure this feature, you must enable failover priority on your network and assign priorities to the individual access points.
- By default, all access points are set to priority level 1, which is the lowest priority level. Therefore, you need to assign a priority level only to those access points that warrant a higher priority.

Configuring Failover Priority for Access Points

This section contains the following topics:
- Configuring Failover Priority for Access Points (GUI), page 9-82
- Configuring Failover Priority for Access Points (CLI), page 9-83
- Viewing Failover Priority Settings (CLI), page 9-84

Configuring Failover Priority for Access Points (GUI)

Step 1

Choose Wireless > Access Points > Global Configuration to open the Global Configuration page.
Step 2  From the Global AP Failover Priority drop-down list, choose **Enable** to enable access point failover priority or choose **Disable** to disable this feature and turn off any access point priority assignments. The default value is Disable.

Step 3  Click **Apply** to commit your changes.

Step 4  Click **Save Configuration** to save your changes.

Step 5  Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 6  Click the name of the access point for which you want to configure failover priority.

Step 7  Choose the **High Availability** tab. The All APs > Details for (High Availability) page appears.

Step 8  From the AP Failover Priority drop-down list, choose one of the following options to specify the priority of the access point:
- **Low**—Assigns the access point to the level 1 priority, which is the lowest priority level. This is the default value.
- **Medium**—Assigns the access point to the level 2 priority.
- **High**—Assigns the access point to the level 3 priority.
- **Critical**—Assigns the access point to the level 4 priority, which is the highest priority level.

Step 9  Click **Apply** to commit your changes.

Step 10  Click **Save Configuration** to save your changes.

---

**Configuring Failover Priority for Access Points (CLI)**

Step 1  Enable or disable access point failover priority by entering this command:

```
config network ap-priority {enable | disable}
```
Configuring Access Point Retransmission Interval and Retry Count

This section contains the following topics:

- Information About Configuring Access Point Retransmission Interval and Retry Count, page 9-85
Information About Configuring Access Point Retransmission Interval and Retry Count

The controller and the access points exchange packets using the CAPWAP reliable transport protocol. For each request, a response is defined. This response is used to acknowledge the receipt of the request message. Response messages are not explicitly acknowledged; therefore, if a response message is not received, the original request message is retransmitted after the retransmit interval. If the request is not acknowledged after a maximum number of retransmissions, the session is closed and the access points reassociate with another controller.

Guidelines and Limitations

- You can configure the retransmission intervals and retry count both at a global as well as a specific access point level. A global configuration applies these configuration parameters to all the access points. That is, the retransmission interval and the retry count are uniform for all access points. Alternatively, when you configure the retransmission level and retry count at a specific access point level, the values are applied to that particular access point. The access point specific configuration has a higher precedence than the global configuration.
- Retransmission intervals and the retry count do not apply for mesh access point.

Configuring the Access Point Retransmission Interval and Retry Count

You can configure the retransmission interval and retry count for all access points globally or a specific access point.

Global Configuration

Step 1 Choose Wireless > Access Points > Global Configuration.

Step 2 Choose one of the following options under the AP Transmit Config Parameters section:
- AP Retransmit Count—Enter the number of times you want the access point to retransmit the request to the controller. This parameter can take values between 3 and 8.
- AP Retransmit Interval—Enter the time duration between the retransmission of requests. This parameter can take values between 2 and 5.

Step 3 Click Apply.
Chapter 9  Controlling Lightweight Access Points

Configuring Access Point Retransmission Interval and Retry Count

Step 1 Choose Wireless > Access Points > All APs.
Step 2 Click on the AP Name link for the access point on which you want to set the values.
The All APs > Details page appears.
Step 3 Click the Advanced Tab to open the advanced parameters page.
Step 4 Choose one of the following parameters under the AP Transmit Config Parameters section:
   • AP Retransmit Count—Enter the number of times that you want the access point to retransmit the request to the controller. This parameter can take values between 3 and 8.
   • AP Retransmit Interval—Enter the time duration between the retransmission of requests. This parameter can take values between 2 and 5.
Step 5 Click Apply.

Configuring the Access Point Retransmission Interval and Retry Count (CLI)

You can configure the retransmission interval and retry count for all access points globally or a specific access point.

- Configure the retransmission interval and retry count for all access points globally by entering this command:

```plaintext
config ap retransmit {interval | count} seconds all
```

The valid range for the `interval` parameter is between 3 and 8. The valid range for the `count` parameter is between 2 and 5.

- Configure the retransmission interval and retry count for a specific access point, by entering this command:

```plaintext
config ap retransmit {interval | count} seconds Cisco_AP
```

The valid range for the `interval` parameter is between 3 and 8. The valid range for the `count` parameter is between 2 and 5.

- See the status of the configured retransmit parameters on all or specific APs by entering this command:

```plaintext
show ap retransmit all
```

(Cisco Controller) >show ap retransmit all
Global control packet retransmit interval: 5
Global control packet retransmit count: 6

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Retransmit Interval</th>
<th>Retransmit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP_1131</td>
<td>N/A(Mesh mode)</td>
<td>N/A(Mesh mode)</td>
</tr>
<tr>
<td>AP_cisco_</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>abhes_1240</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

Note Because retransmit and retry values cannot be set for access points in mesh mode, these values are displayed as N/A (not applicable).

- See the status of the configured retransmit parameters on a specific access point by entering this command:
show ap retransmit Cisco_AP

(Cisco Controller) > show ap retransmit cisco_AP1
Global control packet retransmit interval: 5
Global control packet retransmit count: 6
AP Name Retransmit Interval Retransmit count
------------------ ------------------- -------------------
cisco_AP1 5 6
(Cisco Controller) >

Configuring Country Codes

This section contains the following topics:

- **Information About Configuring Country Codes**, page 9-87
- **Guidelines and Limitations**, page 9-87
- **Configuring Country Codes**, page 9-88

Information About Configuring Country Codes

Controllers and access points are designed for use in many countries with varying regulatory requirements. The radios within the access points are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation (such as FR for France or ES for Spain). Configuring a country code ensures that each radio’s broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

Guidelines and Limitations

- Generally, you configure one country code per controller, the one matching the physical location of the controller and its access points. However, controller software release 4.1 or later releases allows you to configure up to 20 country codes per controller. This multiple-country support enables you to manage access points in various countries from a single controller.

- Although the controller supports different access points in different regulatory domains (countries), it requires all radios in a single access point to be configured for the same regulatory domain. For example, you should not configure a Cisco 1231 access point’s 802.11b/g radio for the US (-A) regulatory domain and its 802.11a radio for the Great Britain (-E) regulatory domain. Otherwise, the controller allows only one of the access point’s radios to turn on, depending on which regulatory domain you selected for the access point on the controller. Therefore, make sure that the same country code is configured for both of the access point’s radios.

    For a complete list of country codes supported per product, see http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

    or


- When the multiple-country feature is being used, all controllers that are going to join the same RF group must be configured with the same set of countries, configured in the same order.
Chapter 9      Controlling Lightweight Access Points

Configuring Country Codes

This section contains the following topics:

- Configuring Country Codes (GUI), page 9-88
- Configuring Country Codes (CLI), page 9-90

Configuring Country Codes (GUI)

Step 1  Follow these steps to disable the 802.11a and 802.11b/g networks as follows:

a. Choose Wireless > 802.11a/n > Network.
b. Unselect the 802.11a Network Status check box.
c. Click Apply to commit your changes.
d. Choose Wireless > 802.11b/g/n > Network.
e. Unselect the 802.11b/g Network Status check box.
f. Click Apply to commit your changes.

Step 2  Choose Wireless > Country to open the Country page.

- When multiple countries are configured and the RRM auto-RF feature is enabled, the RRM assigns the channels that are derived by performing a union of the allowed channels per the AP country code. The APs are assigned channels by the RRM based on their PID country code. APs are only allowed to use legal frequencies that match their PID country code. Ensure that your AP's country code is legal in the country that it is deployed.

- The access point can only operate on the channels for the countries that they are designed for.

Note  If an access point was already set to a higher legal power level or is configured manually, the power level is limited only by the particular country to which that access point is assigned.

- The country list configured on the RF group leader determines what channels the members would operate on. This list is independent of what countries have been configured on the RF group members.
Step 3 Select the check box for each country where your access points are installed. If you selected more than one check box, a message appears indicating that RRM channels and power levels are limited to common channels and power levels.

Step 4 Click **OK** to continue or **Cancel** to cancel the operation.

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

If you selected multiple country codes in Step 3, each access point is assigned to a country.

Step 6 See the default country chosen for each access point and choose a different country if necessary as follows:

**Note** If you remove a country code from the configuration, any access points currently assigned to the deleted country reboot and when they rejoin the controller, they get re-assigned to one of the remaining countries if possible.

- Perform one of the following:
  - Leave the 802.11a and 802.11b/g networks disabled.
  - Reenable the 802.11a and 802.11b/g networks and then disable only the access points for which you are configuring a country code. To disable an access point, choose **Wireless > Access Points > All APs**, click the link of the desired access point, choose **Disable** from the Status drop-down list, and click **Apply**.

- Choose **Wireless > Access Points > All APs** to open the All APs page.
- Click the link for the desired access point.
- Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

The default country for this access point appears in the Country Code drop-down list.
e. If the access point is installed in a country other than the one shown, choose the correct country from the drop-down list. The box contains only those country codes that are compatible with the regulatory domain of at least one of the access point’s radios.

f. Click **Apply** to commit your changes.

g. Repeat these steps to assign all access points joined to the controller to a specific country.

h. Reenable any access points that you disabled in Step a.

**Step 7** Reenable the 802.11a and 802.11b/g networks if you did not enable them in Step 6.

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

### Configuring Country Codes (CLI)

**Step 1** See a list of all available country codes by entering this command:

```plaintext
show country supported
```

**Step 2** Disable the 802.11a and 802.11b/g networks by entering these commands:

```plaintext
config 802.11a disable network
config 802.11b disable network
```

**Step 3** Configure the country codes for the countries where your access points are installed by entering this command:

```plaintext
config country code1,[code2,code3,...]
```

If you are entering more than one country code, separate each by a comma (for example, **config country US,CA,MX**). Information similar to the following appears:

Changing country code could reset channel configuration.
If running in RFM One-Time mode, reassign channels after this command.
Check customized APs for valid channel values after this command.
Are you sure you want to continue? (y/n) y

**Step 4** Enter **Y** when prompted to confirm your decision. Information similar to the following appears:

Configured Country......................... Multiple Countries:US,CA,MX
Auto-RF for this country combination is limited to common channels and power.

**KEY:**
- * = Channel is legal in this country and may be configured manually.
- A = Channel is the Auto-RF default in this country.
- . = Channel is not legal in this country.
- C = Channel has been configured for use by Auto-RF.
- x = Channel is available to be configured for use by Auto-RF.
- (-) = Regulatory Domains allowed by this country.

```
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-(+)
802.11BG    :
Channels    : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
: 1 2 3 4 5 6 7 8 9 0 1 2 3 4
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
802.11A     :
Channels    : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1
--More-- or (q)uit
: 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
```

---

Cisco Wireless LAN Controller Configuration Guide

OL-21524-03

9-90
**Step 5**
Verify your country code configuration by entering this command:

```
show country
```

**Step 6**
See the list of available channels for the country codes configured on your controller by entering this command:

```
show country channels
```

Information similar to the following appears:

```
Configured Country......................... Multiple Countries:US,CA,MX
Auto-RF for this country combination is limited to common channels and power.
KEY: * = Channel is legal in this country and may be configured manually.
A = Channel is the Auto-RF default in this country.
. = Channel is not legal in this country.
C = Channel has been configured for use by Auto-RF.
X = Channel is available to be configured for use by Auto-RF.
(-) = Regulatory Domains allowed by this country.

802.11BG :
Channels : 1 1 1 1 1
: 1 2 3 4 5 6 7 8 9 0 1 2 3 4

802.11A :
Channels : 3 3 3 4 4 4 4 5 5 6 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
: 4 6 8 0 2 4 6 8 2 6 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5

802.11G :
Channels :

```
Step 7
Save your settings by entering this command:

```
save config
```

**Step 8**
See the countries to which your access points have been assigned by entering this command:

```
show ap summary
```

To see a summary of specific access point you can specify the access point name. You can also use wildcard searches when filtering for access points.

Information similar to the following appears:

```
Number of APs................................. 2

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Slots</th>
<th>AP Model</th>
<th>Ethernet MAC</th>
<th>Location</th>
<th>Port</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap1</td>
<td>2</td>
<td>AP1030</td>
<td>00:0b:85:5b:8e:c0</td>
<td>default location</td>
<td>1</td>
<td>US</td>
</tr>
<tr>
<td>ap2</td>
<td>2</td>
<td>AIR-AP1242AG-A-K9</td>
<td>00:14:1c:ed:27:fe</td>
<td>default location</td>
<td>1</td>
<td>US</td>
</tr>
</tbody>
</table>
```
### Step 9
If you entered multiple country codes in Step 3, follow these steps to assign each access point to a specific country:

**a.** Perform one of the following:
- Leave the 802.11a and 802.11b/g networks disabled.
- Reenable the 802.11a and 802.11b/g networks and then disable only the access points for which you are configuring a country code. To reenable the networks, enter these commands:

  ```
  config 802.11a enable network
  config 802.11b enable network
  ```

  To disable an access point, enter this command:

  ```
  config ap disable ap_name
  ```

**b.** To assign an access point to a specific country, enter this command:

  ```
  config ap country code {ap_name | all}
  ```

  Make sure that the country code you choose is compatible with the regulatory domain of at least one of the access point’s radios.

  **Note**
  If you enabled the networks and disabled some access points and then run the `config ap country code all` command, the specified country code is configured on only the disabled access points. All other access points are ignored.

  For example, if you enter `config ap country mx all`, information similar to the following appears:

  To change country code: first disable target AP(s) (or disable all networks).
  Changing the country may reset any customized channel assignments.
  Changing the country will reboot disabled target AP(s).

  Are you sure you want to continue? (y/n) y

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Country</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap2</td>
<td>US</td>
<td>enabled (Disable AP before configuring country)</td>
</tr>
<tr>
<td>ap1</td>
<td>MX</td>
<td>changed (New country configured, AP rebooting)</td>
</tr>
</tbody>
</table>

  **c.** To reenable any access points that you disabled in Step a, enter this command:

  ```
  config ap enable ap_name
  ```

### Step 10
If you did not reenable the 802.11a and 802.11b/g networks in Step 9, enter these commands to reenable them now:

  ```
  config 802.11a enable network
  config 802.11b enable network
  ```

### Step 11
Save your settings by entering this command:

  ```
  save config
  ```
Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain

This section contains the following topics:

- Information About Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain, page 9-93
- Guidelines and Limitations, page 9-94
- Migrating Access Points to the -U Regulatory Domain (CLI), page 9-94

Information About Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain

The Japanese government has changed its 5-GHz radio spectrum regulations. These regulations allow a text box upgrade of 802.11a 5-GHz radios. Japan allows three frequency sets:

- J52 = 34 (5170 MHz), 38 (5190 MHz), 42 (5210 MHz), 46 (5230 MHz)
- W52 = 36 (5180 MHz), 40 (5200 MHz), 44 (5220 MHz), 48 (5240 MHz)
- W53 = 52 (5260 MHz), 56 (5280 MHz), 60 (5300 MHz), 64 (5320 MHz)

Cisco has organized these frequency sets into the following regulatory domains:

- -J regulatory domain = J52
- -P regulatory domain = W52 + W53
- -U regulatory domain = W53

Regulatory domains are used by Cisco to organize the legal frequencies of the world into logical groups. For example, most of the European countries are included in the -E regulatory domain. Cisco access points are configured for a specific regulatory domain at the factory and, with the exception of this migration process, never change. The regulatory domain is assigned per radio, so an access point’s 802.11a and 802.11b/g radios may be assigned to different domains.

Note

Controllers and access points may not operate properly if they are not designed for use in your country of operation. For example, an access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Australia. Always be sure to purchase controllers and access points that match your country’s regulatory domain.

The Japanese regulations allow the regulatory domain that is programmed into an access point’s radio to be migrated from the -J domain to the -U domain. New access points for the Japanese market contain radios that are configured for the -P regulatory domain. -J radios are no longer being sold. In order to make sure that your existing -J radios work together with the new -P radios in one network, you need to migrate your -J radios to the -U domain.

Country codes define the channels that can be used legally in each country. These country codes are available for Japan:

- JP—Allows only -J radios to join the controller
- J2—Allows only -P radios to join the controller
Note J2 -Q works with 7.0.116.0 for all access points except Cisco Aironet 1550 Outdoor Access Points, Cisco 2600 Series Wireless Access Points, and Cisco 3600 Series Access Points. These access points need the -J4 domain to join the controller.

- J3—Uses the -U frequencies but allows both -U and -P radios to join the controller
- J4—Allows 2.4G PQU and 5G JPQU to join the controller.

Note After migration, you need to use the J3 country code. If your controller is running software release 4.1 or later releases, you can use the multiple-country feature to choose both J2 and J3. You can manually configure your -P radios to use the channels not supported by J3.

See the Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points document for the list of channels and power levels supported by access points in the Japanese regulatory domains.

Guidelines and Limitations

- You can migrate only Cisco Aironet 1130, 1200, and 1240 lightweight access points that support the -J regulatory domain and Airespace AS1200 access points. Other access points cannot be migrated.
- Your controller and all access points must be running software release 4.1 or later releases or software release 3.2.193.0.

Note Software release 4.0 is not supported. If you migrate your access points using software release 3.2.193.0, you cannot upgrade to software release 4.0. You can upgrade only to software release 4.1 or later releases or to a later release of the 3.2 software.

- You must have had one or more Japan country codes (JP, J2, or J3) configured on your controller at the time you last booted your controller.
- You must have at least one access point with a -J regulatory domain joined to your controller.
- You cannot migrate your access points from the -U regulatory domain back to the -J domain. The Japanese government has made reverse migration illegal.

Note You cannot undo an access point migration. Once an access point has been migrated, you cannot return to software release 4.0. Migrated access points will have nonfunctioning 802.11a radios under software release 4.0.

- The migration process cannot be performed using the Controller GUI.

Migrating Access Points to the -U Regulatory Domain (CLI)

Step 1 Determine which access points in your network are eligible for migration by entering this command:

`show ap migrate`

Information similar to the following appears:
These 1 APs are eligible for migration:

No APs have already been migrated.

**Step 2**
Disable the 802.11a and 802.11b/g networks by entering these commands:
```plaintext
cfg 802.11a disable network
cfg 802.11b disable network
```

**Step 3**
Change the country code of the access points to be migrated to J3 by entering this command:
```plaintext
cfg country J3
```

**Step 4**
Wait for any access points that may have rebooted to rejoin the controller.

**Step 5**
Migrate the access points from the -J regulatory domain to the -U regulatory domain by entering this command:
```plaintext
cfg ap migrate j52w52 {all | ap_name}
```
Information similar to the following appears:

Migrate APs with 802.11A Radios in the "J" Regulatory Domain to the "U" Regulatory Domain. The "J" domain allows J52 frequencies, the "U" domain allows W52 frequencies.
WARNING: This migration is permanent and is not reversible, as required by law.
WARNING: Once migrated the 802.11A radios will not operate with previous OS versions.
WARNING: All attached "J" radios will be migrated.
WARNING: All migrated APs will reboot.
WARNING: All migrated APs must be promptly reported to the manufacturer.
Send the AP list and your company name to: abc@cisco.com

This AP is eligible for migration:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9ap1240

Begin to migrate Access Points from "J"(J52) to "U"(W52). Are you sure? (y/n)

**Step 6**
Enter Y when prompted to confirm your decision to migrate.

**Step 7**
Wait for all access points to reboot and rejoin the controller. This process may take up to 15 minutes, depending on access point. The AP1130, AP1200, and AP1240 reboot twice; all other access points reboot once.

**Step 8**
Verify migration for all access points by entering this command:
```plaintext
show ap migrate
```
Information similar to the following appears:

No APs are eligible for migration.

These 1 APs have already been migrated:

**Step 9**
Reenable the 802.11a and 802.11b/g networks by entering these commands:
```plaintext
cfg 802.11a enable network
cfg 802.11b enable network
```

**Step 10**
Send an e-mail with your company name and the list of access points that have been migrated to this e-mail address: migrateapj52w52@cisco.com. We recommend that you cut and paste the output from the `show ap migrate` command in Step 8 into the e-mail.
Using the W56 Band in Japan

The Japanese government is formally permitting wireless LAN use of the frequencies in the W56 band for 802.11a radios. The W56 band includes the following channels, frequencies, and power levels (in dBm):

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency (MHz)</th>
<th>Maximum Power for AIR-LAP1132AG-Q-K9</th>
<th>Maximum Power for AIR-LAP1242AG-Q-K9</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>5500</td>
<td>17</td>
<td>15</td>
</tr>
<tr>
<td>104</td>
<td>5520</td>
<td>17</td>
<td>15</td>
</tr>
<tr>
<td>108</td>
<td>5540</td>
<td>17</td>
<td>15</td>
</tr>
<tr>
<td>112</td>
<td>5560</td>
<td>17</td>
<td>15</td>
</tr>
<tr>
<td>116</td>
<td>5580</td>
<td>17</td>
<td>15</td>
</tr>
<tr>
<td>120</td>
<td>5600</td>
<td>17</td>
<td>15</td>
</tr>
<tr>
<td>124</td>
<td>5620</td>
<td>17</td>
<td>15</td>
</tr>
<tr>
<td>128</td>
<td>5640</td>
<td>17</td>
<td>15</td>
</tr>
<tr>
<td>132</td>
<td>5660</td>
<td>17</td>
<td>15</td>
</tr>
<tr>
<td>136</td>
<td>5680</td>
<td>17</td>
<td>15</td>
</tr>
<tr>
<td>140</td>
<td>5700</td>
<td>17</td>
<td>15</td>
</tr>
</tbody>
</table>

All of the channels in the W56 band require dynamic frequency selection (DFS). In Japan, the W56 band is subject to Japan’s DFS regulations. Currently, only the new 1130 and 1240 series access point SKUs (with the -Q product code) support this requirement: AIR-LAP1132AG-Q-K9 and AIR-LAP1242AG-Q-K9.

To set up a network consisting of only -P and -Q access points, configure the country code to J2. To set up a network consisting of -P, -Q, and -U access points, configure the country code to J3.

Dynamic Frequency Selection

The Cisco UWN solution complies with regulations that require radio devices to use dynamic frequency selection (DFS) to detect radar signals and avoid interfering with them.

When a lightweight access point with a 5-GHz radio operates on one of the 15 channels listed in Table 9-3, the controller to which the access point is associated automatically uses DFS to set the operating frequency.

When you manually select a channel for DFS-enabled 5-GHz radios, the controller checks for radar activity on the channel for 60 seconds. If there is no radar activity, the access point operates on the channel that you selected. If there is radar activity on the channel that you selected, the controller automatically selects a different channel, and after 30 minutes, the access point retries the channel.

Note

After radar has been detected on a DFS-enabled channel, it cannot be used for 30 minutes.
Optimizing RFID Tracking on Access Points

Note

The Rogue Location Detection Protocol (RLDP) and rogue containment are not supported on the channels listed in Table 9-3.

Note

The maximum legal transmit power is greater for some 5-GHz channels than for others. When the controller randomly selects a 5-GHz channel on which power is restricted, it automatically reduces transmit power to comply with power limits for that channel.

Table 9-3 DFS-Enabled 5-GHz Channels

<table>
<thead>
<tr>
<th>Channel 1</th>
<th>Channel 2</th>
<th>Channel 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>52 (5260 MHz)</td>
<td>104 (5520 MHz)</td>
<td>124 (5620 MHz)</td>
</tr>
<tr>
<td>56 (5280 MHz)</td>
<td>108 (5540 MHz)</td>
<td>128 (5640 MHz)</td>
</tr>
<tr>
<td>60 (5300 MHz)</td>
<td>112 (5560 MHz)</td>
<td>132 (5660 MHz)</td>
</tr>
<tr>
<td>64 (5320 MHz)</td>
<td>116 (5580 MHz)</td>
<td>136 (5680 MHz)</td>
</tr>
<tr>
<td>100 (5500 MHz)</td>
<td>120 (5600 MHz)</td>
<td>140 (5700 MHz)</td>
</tr>
</tbody>
</table>

Using DFS, the controller monitors operating frequencies for radar signals. If it detects radar signals on a channel, the controller takes these steps:

- It changes the access point channel to a channel that has not shown radar activity within the last 30 minutes. (The radar event is cleared after 30 minutes.) The controller selects the channel at random.
- If the channel selected is one of the channels in Table 9-3, it scans the new channel for radar signals for 60 seconds. If there are no radar signals on the new channel, the controller accepts client associations.
- It records the channel that showed radar activity as a radar channel and prevents activity on that channel for 30 minutes.
- It generates a trap to alert the network manager.

Optimizing RFID Tracking on Access Points

This section contains the following topics:
- Information About Optimizing RFID Tracking on Access Points, page 9-97
- Optimizing RFID Tracking on Access Points, page 9-98

Information About Optimizing RFID Tracking on Access Points

To optimize the monitoring and location calculation of RFID tags, you can enable tracking optimization on up to four channels within the 2.4-GHz band of an 802.11b/g access point radio. This feature allows you to scan only the channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).
Optimizing RFID Tracking on Access Points

This section contains the following topics:

- Optimizing RFID Tracking on Access Points (GUI), page 9-98
- Optimizing RFID Tracking on Access Points (CLI), page 9-99

Optimizing RFID Tracking on Access Points (GUI)

Step 1  Choose Wireless > Access Points > All APs to open the All APs page.
Step 2  Click the name of the access point for which you want to configure monitor mode. The All APs > Details page appears.
Step 3  From the AP Mode drop-down list, choose Monitor.
Step 4  Click Apply to commit your changes.
Step 5  Click OK when warned that the access point will be rebooted.
Step 6  Click Save Configuration to save your changes.
Step 7  Choose Wireless > Access Points > Radios > 802.11b/g/n to open the 802.11b/g/n Radios page.
Step 8  Hover your cursor over the blue drop-down arrow for the desired access point and choose Configure. The 802.11b/g/n Cisco APs > Configure page appears.

Step 9  Disable the access point radio by choosing Disable from the Admin Status drop-down list and click Apply.
Step 10 Enable tracking optimization on the radio by choosing Enable from the Enable Tracking Optimization drop-down list.
Step 11 From the four Channel drop-down lists, choose the channels on which you want to monitor RFID tags.

Note  You must configure at least one channel on which the tags will be monitored.
Step 12 Click Apply to commit your changes.

Step 13 Click Save Configuration to save your changes.

Step 14 To reenable the access point radio, choose Enable from the Admin Status drop-down list and click Apply.

Step 15 Click Save Configuration to save your changes.

Optimizing RFID Tracking on Access Points (CLI)

Step 1 Configure an access point for monitor mode by entering this command:

```
config ap mode monitor Cisco_AP
```

Step 2 When warned that the access point will be rebooted and asked if you want to continue, enter Y.

Step 3 Save your changes by entering this command:

```
save config
```

Step 4 Disable the access point radio by entering this command:

```
config 802.11b disable Cisco_AP
```

Step 5 Configure the access point to scan only the DCA channels supported by its country of operation by entering this command:

```
config ap monitor-mode tracking-opt Cisco_AP
```

**Note** To specify the exact channels to be scanned, enter the `config ap monitor-mode tracking-opt Cisco_AP` command in Step 6.

**Note** To disable tracking optimization for this access point, enter the `config ap monitor-mode no-optimization Cisco_AP` command.

Step 6 After you have entered the command in Step 5, you can enter this command to choose up to four specific 802.11b channels to be scanned by the access point:

```
config ap monitor-mode 802.11b fast-channel Cisco_AP channel1 channel2 channel3 channel4
```

**Note** In the United States, you can assign any value between 1 and 11 (inclusive) to the `channel` variable. Other countries support additional channels. You must assign at least one channel.

Step 7 Reenable the access point radio by entering this command:

```
config 802.11b enable Cisco_AP
```

Step 8 Save your changes by entering this command:

```
save config
```

Step 9 See a summary of all access points in monitor mode by entering this command:

```
show ap monitor-mode summary
```

Information similar to the following appears:
## Configuring Probe Request Forwarding

This section contains the following topics:

- Information About Configuring Probe Request Forwarding, page 9-100
- Configuring Probe Request Forwarding (CLI), page 9-100

### Information About Configuring Probe Request Forwarding

Probe requests are 802.11 management frames sent by clients to request information about the capabilities of SSIDs. By default, access points forward acknowledged probe requests to the controller for processing. Acknowledged probe requests are probe requests for SSIDs that are supported by the access point. If desired, you can configure access points to forward both acknowledged and unacknowledged probe requests to the controller. The controller can use the information from unacknowledged probe requests to improve the location accuracy.

### Configuring Probe Request Forwarding (CLI)

**Step 1**
Enable or disable the filtering of probe requests forwarded from an access point to the controller by entering this command:

```plaintext
config advanced probe filter { enable | disable }
```

If you enable probe filtering, the default filter setting, the access point forwards only acknowledged probe requests to the controller. If you disable probe filtering, the access point forwards both acknowledged and unacknowledged probe requests to the controller.

**Step 2**
Limit the number of probe requests sent to the controller per client per access point radio in a given interval by entering this command:

```plaintext
config advanced probe limit num_probes interval
```

where

- `num_probes` is the number of probe requests (from 1 to 100) forwarded to the controller per client per access point radio in a given interval.
- `interval` is the probe limit interval (from 100 to 10000 milliseconds).

The default value for `num_probes` is 2 probe requests, and the default value for `interval` is 500 milliseconds.

**Step 3**
Save your changes by entering this command:

```plaintext
save config
```

**Step 4**
See the probe request forwarding configuration by entering this command:

```plaintext
show advanced probe
```
Information similar to the following appears:
Probe request filtering..........................  Enabled
Probes fwd to controller per client per radio.... 2
Probe request rate-limiting interval............ 500 msec

Retrieving the Unique Device Identifier on Controllers and Access Points

This section contains the following topics:
- Information About Retrieving the Unique Device Identifier on Controllers and Access Points, page 9-101
- Retrieving the Unique Device Identifier on Controllers and Access Points, page 9-101

Information About Retrieving the Unique Device Identifier on Controllers and Access Points

The Unique Device Identifier (UDI) standard uniquely identifies products across all Cisco hardware product families, enabling customers to identify and track Cisco products throughout their business and network operations and to automate their asset management systems. The standard is consistent across all electronic, physical, and standard business communications. The UDI consists of five data elements:
- The orderable product identifier (PID)
- The version of the product identifier (VID)
- The serial number (SN)
- The entity name
- The product description
The UDI is burned into the EEPROM of controllers and lightweight access points at the factory.

Retrieving the Unique Device Identifier on Controllers and Access Points

This section contains the following topics:
- Retrieving the Unique Device Identifier on Controllers and Access Points (GUI), page 9-101
- Retrieving the Unique Device Identifier on Controllers and Access Points (CLI), page 9-102

Retrieving the Unique Device Identifier on Controllers and Access Points (GUI)

Step 1 Choose Controller > Inventory to open the Inventory page.
Performing a Link Test

This section contains the following topics:

- Information About Performing a Link Test, page 9-103
- Performing a Link Test, page 9-103
Information About Performing a Link Test

A link test is used to determine the quality of the radio link between two devices. Two types of link-test packets are transmitted during a link test: request and response. Any radio receiving a link-test request packet fills in the appropriate text boxes and echoes the packet back to the sender with the response type set.

The radio link quality in the client-to-access point direction can differ from that in the access point-to-client direction due to the asymmetrical distribution of the transmit power and receive sensitivity on both sides. Two types of link tests can be performed: a ping test and a CCX link test.

With the ping link test, the controller can test link quality only in the client-to-access point direction. The RF parameters of the ping reply packets received by the access point are polled by the controller to determine the client-to-access point link quality.

With the CCX link test, the controller can also test the link quality in the access point-to-client direction. The controller issues link-test requests to the client, and the client records the RF parameters (received signal strength indicator [RSSI], signal-to-noise ratio [SNR], and so on) of the received request packet in the response packet. Both the link-test requestor and responder roles are implemented on the access point and controller. Not only can the access point or controller initiate a link test to a CCX v4 or v5 client, but a CCX v4 or v5 client can initiate a link test to the access point or controller.

The controller shows these link-quality metrics for CCX link tests in both directions (out—access point to client; in—client to access point):

- Signal strength in the form of RSSI (minimum, maximum, and average)
- Signal quality in the form of SNR (minimum, maximum, and average)
- Total number of packets that are retried
- Maximum retry count for a single packet
- Number of lost packets
- Data rate of a successfully transmitted packet

The controller shows this metric regardless of direction:

- Link test request/reply round-trip time (minimum, maximum, and average)

The controller software supports CCX versions 1 through 5. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to limit the features for this client. If a client does not support CCXv4 or v5, the controller performs a ping link test on the client. If a client supports CCXv4 or v5, the controller performs a CCX link test on the client. If a client times out during a CCX link test, the controller switches to the ping link test automatically. See the “Configuring Cisco Client Extensions” section on page 8-57 for more information on CCX.

Note

CCX is not supported on the AP1030.

Performing a Link Test

This section contains the following topics:

- Performing a Link Test (GUI), page 9-104
- Performing a Link Test (CLI), page 9-105
Performing a Link Test (GUI)

Step 1  Choose Monitor > Clients to open the Clients page.

Figure 9-44  Clients Page

---

Step 2  Hover your cursor over the blue drop-down arrow for the desired client and choose Link Test. A link test page appears.

Note  You can also access this page by clicking the MAC address of the desired client and then clicking the Link Test button on the top of the Clients > Detail page.

Figure 9-45  Link Test Page

---

This page shows the results of the CCX link test.
Performing a Link Test (CLI)

Use these commands to run a link test using the controller CLI:

- Run a link test by entering this command:

  `linktest ap_mac`

When CCX v4 or later releases is enabled on both the controller and the client being tested, information similar to the following appears:

CCX Link Test to 00:0d:88:c5:8a:d1.
Link Test Packets Sent................................. 20
Link Test Packets Received............................ 10
Link Test Packets Lost (Total/AP to Client/Client to AP).... 10/5/5
Link Test Packets round trip time (min/max/average) ........ 5ms/20ms/15ms
RSSI at AP (min/max/average) .......................... -60dBm/-50dBm/-55dBm
RSSI at Client (min/max/average) ....................... -50dBm/-40dBm/-45dBm
SNR at AP (min/max/average) .......................... 40dB/30dB/35dB
SNR at Client (min/max/average) ....................... 40dB/30dB/35dB
Transmit Retries at AP (Total/Maximum) .................. 5/3
Transmit Retries at Client (Total/Maximum) .............. 4/2
Packet Count: 1M 2M 5.5M 6M 9M 11M 12M 18M 24M 36M 48M 54M 108M
Packet Count: 0 0 0 0 0 0 0 0 0 2 0 18 0
Packet Count: 0 0 0 0 0 0 0 0 0 2 0 8 0

When CCX v4 or later releases is not enabled on either the controller or the client being tested, fewer details appear:

Ping Link Test to 00:0d:88:c5:8a:d1.
Link Test Packets Sent................................. 20
Link Test Packets Received............................ 20
Local Signal Strength................................. -49dBm
Local Signal to Noise Ratio........................... 39dB

- Adjust the link-test parameters that are applicable to both the CCX link test and the ping test by entering these commands from configuration mode:

  `linktest frame-size size_of_link_test_frames`
  `linktest num-of-frame number_of_link-test_request_frames_per_test`

Configuring Link Latency

This section contains the following topics:
Information About Configuring Link Latency

You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to the controller but is especially useful for FlexConnect and OfficeExtend access points, for which the link could be a slow or unreliable WAN connection.

Guidelines and Limitations

- Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

  Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the access point to the controller and back. This time can vary due to the network link speed and controller processing loads. The access point timestamps the outgoing echo requests to the controller and the echo responses received from the controller. The access point sends this delta time to the controller as the system round-trip time. The access point sends heartbeat packets to the controller at a default interval of 30 seconds.

  Note  Link latency calculates the CAPWAP response time between the access point and the controller. It does not measure network latency or ping responses.

- The controller displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the controller is up or can be cleared and allowed to restart.

Configuring Link Latency

This section contains the following topics:

- Configuring Link Latency (GUI), page 9-106
- Configuring Link Latency (CLI), page 9-107

Configuring Link Latency (GUI)

Step 1  Choose Wireless > Access Points > All APs to open the All APs page.

Step 2  Click the name of the access point for which you want to configure link latency.

Step 3  Choose the Advanced tab to open the All APs > Details for (Advanced) page.
Configuring Link Latency

Step 4 Select the Enable Link Latency check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. The default value is unselected.

Step 5 Click Apply to commit your changes.

Step 6 Click Save Configuration to save your changes.

Step 7 When the All APs page reappears, click the name of the access point again.

Step 8 When the All APs > Details for page reappears, choose the Advanced tab again. The link latency and data latency results appear below the Enable Link Latency check box:

- **Current**—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.
- **Minimum**—Since link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.
- **Maximum**—Since link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.

Step 9 To clear the current, minimum, and maximum link latency and data latency statistics on the controller for this access point, click Reset Link Latency.

Step 10 After the page refreshes and the All APs > Details for page reappears, choose the Advanced tab. The updated statistics appear in the Minimum and Maximum text boxes.

Configuring Link Latency (CLI)

Step 1 Enable or disable link latency for a specific access point or for all access points currently associated to the controller by entering this command:
**Configuring the TCP MSS**

This section contains the following topics:
- Information About Configuring the TCP MSS, page 9-109
- Configuring TCP MSS, page 9-109

```plaintext
cfg ap link-latency {enable | disable} {Cisco_AP | all}
```

The default value is disabled.

**Note** The `cfg ap link-latency {enable | disable} all` command enables or disables link latency only for access points that are currently joined to the controller. It does not apply to access points that join in the future.

**Step 2** See the link latency results for a specific access point by entering this command:

```plaintext
show ap config general Cisco_AP
```

Information similar to the following appears:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP1
...
AP Link Latency.................................. Enabled
Current Delay.................................... 1 ms
Maximum Delay................................... 1 ms
Minimum Delay................................... 1 ms
Last updated (based on AP Up Time)............ 0 days, 05 h 03 m 25 s
```

The output of this command contains the following link latency results:

- **Current Delay**—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Maximum Delay**—Since link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Minimum Delay**—Since link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

**Step 3** Clear the current, minimum, and maximum link latency statistics on the controller for a specific access point by entering this command:

```plaintext
cfg ap link-latency reset Cisco_AP
```

**Step 4** See the results of the reset by entering this command:

```plaintext
show ap config general Cisco_AP
```
Information About Configuring the TCP MSS

If the client’s maximum segment size (MSS) in a Transmission Control Protocol (TCP) three-way handshake is greater than the maximum transmission unit can handle, the client might experience reduced throughput and the fragmentation of packets. To avoid this problem in controller software release 6.0 or later releases, you can specify the MSS for all access points that are joined to the controller or for a specific access point.

When you enable this feature, the access point selects for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

Configuring TCP MSS

This section contains the following topics:

- Configuring TCP MSS (GUI), page 9-109
- Configuring TCP MSS (CLI), page 9-109

Configuring TCP MSS (GUI)

Step 1
Choose WIRELESS > Access Points > Global Configuration to open the Global Configuration page.

Step 2
Under TCP MSS, select the Global TCP Adjust MSS check box and set the MSS for all access points that are associated with the controller. The valid range is between 536 and 1363 bytes.

Configuring TCP MSS (CLI)

Step 1
Enable or disable the TCP MSS on a particular access point or on all access points by entering this command:

```
config ap tcp-adjust-mss {enable | disable} {Cisco_AP | all} size
```

where the `size` parameter is a value between 536 and 1363 bytes. The default value varies for different clients.

Step 2
Save your changes by entering this command:

```
save config
```

Step 3
See the current TCP MSS setting for a particular access point or all access points by entering this command:

```
show ap tcp-mss-adjust {Cisco_AP | all}
```

Information similar to the following appears:

```
AP Name  TCP State  MSS Size
---------  ---------  ------
AP-1140   enabled   536
AP-1240   disabled  -
AP-1130   disabled  -
```
Configuring Power over Ethernet

This section contains the following topics:

- Information About Configuring Power over Ethernet, page 9-110
- Guidelines and Limitations, page 9-110
- Configuring Power over Ethernet, page 9-111

Information About Configuring Power over Ethernet

When an access point that has been converted to lightweight mode (such as an AP1131 or AP1242) or a 1250 series access point is powered by a power injector that is connected to a Cisco pre-Intelligent Power Management (pre-IPM) switch, you need to configure Power over Ethernet (PoE), also known as inline power.

The dual-radio 1250 series access points can operate in four different modes when powered using PoE:

- 20.0 W (Full Power)—This mode is equivalent to using a power injector or an AC/DC adapter.
- 16.8 W—Both transmitters are used but at reduced power. Legacy data rates are not affected, but the M0 to M15 data rates are reduced in the 2.4-GHz band. Throughput should be minimally impacted because all data rates are still enabled. The range is affected because of the lower transmit power. All receivers remain enabled.
- 15.4 W—Only a single transmitter is enabled. Legacy data rates and M0 to M7 rates are minimally affected. M8 to M15 rates are disabled because they require both transmitters. Throughput is better than that received with legacy access points but less than the 20 and 16.8 W power modes.
- 11.0 W (Low Power)—The access point runs, but both radios are disabled.

Guidelines and Limitations

- When a dual-radio 1250 series access point is powered using 15.4-W PoE, it cannot operate at full functionality, which requires 20 W. The access point can operate with dual radios on 15.4-W PoE, but performance is reduced in terms of throughput and range. If full functionality is required on 15.4 W, you can remove one of the radios from the 1250 series access point chassis or disable it in controller software release 6.0 or later releases so that the other radio can operate in full 802.11n mode. After the access point radio is administratively disabled, the access point must be rebooted for the change to take effect. The access point must also be rebooted after you reenable the radio to put it into reduced throughput mode.

These modes provide the flexibility of running the 1250 series access points with the available wired infrastructure to obtain the desired level of performance. With enhanced PoE switches (such as the Cisco Catalyst 3750-E Series Switches), the 1250 series access points can provide maximum features and functionality with a minimum total cost of ownership. Alternatively, if you decide to power the access point with the existing PoE (802.3af) switches, the access point chooses the appropriate mode of operation based on whether it has one radio or two.

Note

For more information on the Cisco PoE switches, see this URL:
- Table 9-4 shows the maximum transmit power settings for 1250 series access points using PoE.

### Table 9-4: Maximum Transmit Power Settings for 1250 Series Access Points Using PoE

<table>
<thead>
<tr>
<th>Radio Band</th>
<th>Data Rates</th>
<th>Number of Transmitters</th>
<th>Cyclic Shift Diversity (CSD)</th>
<th>Maximum Transmit Power (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>802.3af Mode (15.4 W)</td>
</tr>
<tr>
<td>2.4 GHz</td>
<td>802.11b</td>
<td>1</td>
<td>—</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>802.11g</td>
<td>1</td>
<td>—</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>802.11n MCS 0-7</td>
<td>1</td>
<td>Disabled (default)</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>802.11n MCS 8-15</td>
<td>2</td>
<td>—</td>
<td>Disabled</td>
</tr>
<tr>
<td>5 GHz</td>
<td>802.11a</td>
<td>1</td>
<td>—</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>802.11n MCS 0-7</td>
<td>1</td>
<td>Disabled (default)</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>802.11n MCS 8-15</td>
<td>2</td>
<td>—</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

1. Maximum transmit power varies by channel and according to individual country regulations. See the product documentation for specific details.

- When powered with a non-Cisco standard PoE switch, the 1250 series access point operates under 15.4 Watts. Even if the non-Cisco switch or midspan device is capable of providing higher power, the access point does not operate in enhanced PoE mode.

## Configuring Power over Ethernet

This section contains the following topics:

- Configuring Power over Ethernet (GUI), page 9-111
- Configuring Power over Ethernet (CLI), page 9-113

### Configuring Power over Ethernet (GUI)

**Step 1** Choose **Wireless > Access Points > All APs** and then the name of the desired access point.

**Step 2** Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.
Figure 9-47  All APs > Details for (Advanced) Page

The PoE Status text box shows the power level at which the access point is operating: High (20 W), Medium (16.8 W), or Medium (15.4 W). This text box is not configurable. The controller auto-detects the access point’s power source and displays the power level here.

Note  This text box applies only to 1250 series access points that are powered using PoE. There are two other ways to determine if the access point is operating at a lower power level. First, the “Due to low PoE, radio is transmitting at degraded power” message appears under the Tx Power Level Assignment section on the 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page. Second, the “PoE Status: degraded operation” message appears in the controller’s trap log on the Trap Logs page.

Step 3  Perform one of the following:

- Select the Pre-standard 802.3af switches check box if the access point is being powered by a high-power 802.3af Cisco switch. This switch provides more than the traditional 6 Watts of power but do not support the intelligent power management (IPM) feature.
- Unselect the Pre-standard 802.3af switches check box if power is being provided by a power injector. This is the default value.

Step 4  Select the Power Injector State check box if the attached switch does not support IPM and a power injector is being used. If the attached switch supports IPM, you do not need to select this check box.

Step 5  If you selected the Power Injector State check box in the previous step, the Power Injector Selection and Injector Switch MAC Address parameters appear. The Power Injector Selection parameter enables you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed. Choose one of these options from the drop-down list to specify the desired level of protection:

- Installed—This option examines and remembers the MAC address of the currently connected switch port and assumes that a power injector is connected. Choose this option if your network contains older Cisco 6-Watt switches and you want to avoid possible overloads by forcing a double-check of any relocated access points.

If you want to configure the switch MAC address, enter the MAC address in the Injector Switch MAC Address text box. If you want the access point to find the switch MAC address, leave the Injector Switch MAC Address text box blank.
Chapter 9  Controlling Lightweight Access Points

Configuring Power over Ethernet

Note
Each time an access point is relocated, the MAC address of the new switch port fails to match the remembered MAC address, and the access point remains in low-power mode. You must then physically verify the existence of a power injector and reselect this option to cause the new MAC address to be remembered.

- **Override**—This option allows the access point to operate in high-power mode without first verifying a matching MAC address. You can use this option if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The advantage of this option is that if you relocate the access point, it continues to operate in high-power mode without any further configuration. The disadvantage of this option is that if the access point is connected directly to a 6-W switch, an overload occurs.

**Step 6**
Click **Apply** to commit your changes.

**Step 7**
If you have a dual-radio 1250 series access point and want to disable one of its radios in order to enable the other radio to receive full power, follow these steps:

a. Choose **Wireless > Access Points > Radios > 802.11a/n or 802.11b/g/n** to open the 802.11a/n (or 802.11b/g/n) Radios page.

b. Hover your cursor over the blue drop-down arrow for the radio that you want to disable and choose **Configure**.

c. On the 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page, choose **Disable** from the Admin Status drop-down list.

d. Click **Apply** to commit your changes.

e. Manually reset the access point in order for the change to take effect.

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

**Configuring Power over Ethernet (CLI)**

Use these commands to configure and see PoE settings using the controller CLI:

- If your network contains any older Cisco 6-W switches that could be accidentally overloaded if connected directly to a 12-W access point, enter this command:

  ```
  config ap power injector enable {Cisco_AP | all} installed
  ```

  The access point remembers that a power injector is connected to this particular switch port. If you relocate the access point, you must reissue this command after the presence of a new power injector is verified.

  **Note** Make sure CDP is enabled before entering this command. Otherwise, this command will fail. See the “Configuring the Cisco Discovery Protocol” section on page 4-95 for information on enabling CDP.

- Remove the safety checks and allow the access point to be connected to any switch port by entering this command:

  ```
  config ap power injector enable {Cisco_AP | all} override
  ```
You can use this command if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The access point assumes that a power injector is always connected. If you relocate the access point, it continues to assume that a power injector is present.

- If you know the MAC address of the connected switch port and do not want to automatically detect it using the installed option, enter this command:

  ```
  config ap power injector enable {Cisco_AP | all} switch_port_mac_address
  ```

- If you have a dual-radio 1250 series access point and want to disable one of its radios in order to enable the other radio to receive full power, enter this command:

  ```
  config {802.11a | 802.11b} disable Cisco_AP
  ```

  **Note**  You must manually reset the access point in order for the change to take effect.

- See the PoE settings for a specific access point by entering this command:

  ```
  show ap config general Cisco_AP
  ```

  Information similar to the following appears:

  ```
  Cisco AP Identifier.............................. 1
  Cisco AP Name.................................... AP1
  ...
  PoE Pre-Standard Switch......................... Enabled
  PoE Power Injector MAC Addr.................... Disabled
  Power Type/Mode.................................. PoE/Low Power (degraded mode)
  ...
  ```

  The Power Type/Mode text box shows “degraded mode” if the access point is not operating at full power.

- See the controller’s trap log by entering this command:

  ```
  show traplog
  ```

  If the access point is not operating at full power, the trap contains “PoE Status: degraded operation.”

### Configuring Flashing LEDs

This section contains the following topics:

- Information About Configuring Flashing LEDs, page 9-114
- Configuring Flashing LEDs (CLI), page 9-114

### Information About Configuring Flashing LEDs

Controller software release 4.0 or later releases enables you to flash the LEDs on an access point in order to locate it. All IOS lightweight access points support this feature.

### Configuring Flashing LEDs (CLI)

Use these commands to configure LED flashing from the privileged EXEC mode of the controller:
To disable LED flashing for a specific access point by entering this command:

debug ap command “led flash disable” Cisco_AP

This command disables LED flashing immediately. For example, if you run the previous command (with the seconds parameter set to 60 seconds) and then disable LED flashing after only 20 seconds, the access point’s LEDs stop flashing immediately.

**Viewing Clients**

This section contains the following topics:

- Viewing Clients (GUI), page 9-115
- Viewing Clients (CLI), page 9-119

**Viewing Clients (GUI)**

**Step 1**

Choose Monitor > Clients to open the Clients page.

**Figure 9-48 Clients Page**

This page lists all of the clients that are associated to the controller’s access points. It provides the following information for each client:

- Client MAC Address
- AP Name
- WLAN Profile
- Protocol
- Status
- Auth
- Port
- WCR
Viewing Clients

- The MAC address of the client
- The name of the access point to which the client is associated
- The name of the WLAN used by the client
- The type of client (802.11a, 802.11b, 802.11g, or 802.11n)

Note: If the 802.11n client associates to an 802.11a radio that has 802.11n enabled, then the client type shows as 802.11a/n. If the 802.11n client associates to an 802.11b/g radio with 802.11n enabled, then the client type shows as 802.11b/n.

- The status of the client connection
- The authorization status of the client
- The port number of the access point to which the client is associated
- An indication of whether the client is a WGB

Note: See the “Using Cisco Workgroup Bridges” section on page 9-70 for more information on the WGB status.

Note: If you want to remove or disable a client, hover your cursor over the blue drop-down arrow for that client and choose Remove or Disable, respectively. If you want to test the connection between the client and the access point, hover your cursor over the blue drop-down arrow for that client and choose Link Test.

Step 2
Create a filter to display only clients that meet certain criteria (such as the MAC address, status, or radio type) as follows:

a. Click Change Filter to open the Search Clients dialog box.

Figure 9-49 Search Clients Dialog Box

<table>
<thead>
<tr>
<th>Search Clients</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td></td>
</tr>
<tr>
<td>AP Name</td>
<td></td>
</tr>
<tr>
<td>WLAN Profile</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>Radio Type</td>
<td></td>
</tr>
<tr>
<td>WGB</td>
<td></td>
</tr>
</tbody>
</table>

b. Select one or more of the following check boxes to specify the criteria used when displaying clients:
   - MAC Address—Enter a client MAC address.
Note When you enable the MAC address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC address filter is disabled automatically.

- **AP Name**—Enter the name of an access point.
- **WLAN Profile**—Choose one of the available WLAN profiles from the drop-down list.
- **Status**—Select the **Associated**, **Authenticated**, **Excluded**, and/or **Idle** check boxes.
- **Radio Type**—Choose **802.11a**, **802.11b**, **802.11g**, **802.11an**, **802.11bn** or **Mobile**.
- **WGB**—Enter the WGB clients associated to the controller’s access points.

   c. Click **Apply** to commit your changes. The Current Filter parameter at the top of the Clients page shows the filters that are currently applied.

Note If you want to remove the filters and display the entire client list, click **Clear Filter**.

**Step 3** Click the MAC address of the client to view detailed information for a specific client. The Clients > Detail page appears.
### Figure 9-50  Clients > Detail Page

<table>
<thead>
<tr>
<th>Client Properties</th>
<th>AP Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>00:0b:15:81:04:53</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.30.0/24</td>
</tr>
<tr>
<td>Client Type</td>
<td>Regular</td>
</tr>
<tr>
<td>User Name</td>
<td>webserver</td>
</tr>
<tr>
<td>Port Number</td>
<td>80</td>
</tr>
<tr>
<td>Interface</td>
<td>management</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>0</td>
</tr>
<tr>
<td>SSID</td>
<td>MyNetwork</td>
</tr>
<tr>
<td>Security Settings</td>
<td></td>
</tr>
<tr>
<td>QoS</td>
<td>Disabled</td>
</tr>
<tr>
<td>EAP Type</td>
<td>EAP-TLS</td>
</tr>
<tr>
<td>RADIUS</td>
<td>disabled</td>
</tr>
<tr>
<td>RA</td>
<td>0</td>
</tr>
<tr>
<td>DHCP</td>
<td>Enabled</td>
</tr>
<tr>
<td>Client Statistics</td>
<td></td>
</tr>
<tr>
<td>Bytes Received</td>
<td>0</td>
</tr>
<tr>
<td>Bytes Sent</td>
<td>0</td>
</tr>
<tr>
<td>Packets Received</td>
<td>0</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>0</td>
</tr>
<tr>
<td>Policies</td>
<td></td>
</tr>
<tr>
<td>Policies Errors</td>
<td></td>
</tr>
<tr>
<td>Policies Errors</td>
<td></td>
</tr>
</tbody>
</table>

This page shows the following information:

- The general properties of the client
- The security settings of the client
- The QoS properties of the client
Viewing Clients (CLI)

Use these commands to view client information:

- See the clients associated to a specific access point by entering this command:

  ```
  show client ap {802.11a | 802.11b} Cisco_AP
  ```

  Information similar to the following appears:

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>AP Id</th>
<th>Status</th>
<th>WLAN Id</th>
<th>Authenticated</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:13:ce:cc:8e:b8</td>
<td>1</td>
<td>Associated</td>
<td>1</td>
<td>No</td>
</tr>
</tbody>
</table>

- See a summary of the clients associated to the controller’s access points by entering this command:

  ```
  show client summary
  ```

  Information similar to the following appears:

  Number of Clients................................ 1

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>AP Name</th>
<th>Status</th>
<th>WLAN/Guest-Lan Auth</th>
<th>Protocol</th>
<th>Port</th>
<th>Wired</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:13:02:2d:96:24</td>
<td>AP_1130</td>
<td>Associated</td>
<td>Yes</td>
<td>802.11a</td>
<td>1</td>
<td>No</td>
</tr>
</tbody>
</table>

- See detailed information for a specific client by entering this command:

  ```
  show client detail client_mac
  ```

  Information similar to the following appears:

  Client MAC Address............................... 00:40:96:b2:a3:44
  Client Username ................................ N/A
  AP MAC Address................................... 00:18:74:c7:c0:90
  Client State..................................... Associated
  Wireless LAN Id.................................. 1
  BSSID............................................ 00:18:74:c7:c0:9f
  Channel.......................................... 56
  IP Address....................................... 192.168.10.28
  Association Id................................... 1
  Authentication Algorithm......................... Open System
  Reason Code...................................... 0
  Status Code...................................... 0
  Session Timeout.................................. 0
  Client CCX version............................... 5
  Client E2E version............................... No E2E support
  Diagnostics Capability........................... Supported
  S69 Capability................................... Supported
  Mirroring.......................................... Disabled
  QoS Level......................................... Silver
  ...
Configuring LED States for Access Points

In a wireless LAN network, there may be numerous access points that could be associated with a controller. It can be difficult to locate a specific access point associated with the controller. You can configure the controller to set the LED state of an access point so that it blinks and the access point can be located. This configuration can be done in the wireless network on a global as well as per-AP level.

Guidelines and Limitations

The LED state configuration at the global level takes precedence over the AP level.

Configuring LED State of Access Point in a Network Globally (GUI)

Step 1 Choose Wireless > Access Points > Global Configuration to open the Global Configuration page.
Step 2 Select the LED state checkbox.
Step 3 Select Enable from the drop-down list adjacent to this text box.
Step 4 Click Apply.

Configuring LED State of Access Point in a Network Globally (CLI)

Use the following command to set the LED state of all access points associated to a controller:

```plaintext
config ap led-state {enable | disable} all
```

Configuring LED State on an Access Point (GUI)

Step 1 Choose Wireless > Access Points > All APs and then the name of the desired access point.
Step 2 Choose the Advanced tab to open the All APs > Details for (Advanced) page.
Step 3 Select the LED state checkbox.
Step 4 Select Enable from the drop-down list adjacent to this text box.
Step 5 Click Apply.

Configuring LED State on an Access Point (CLI)

Use the following command to set the LED state of a specific access point:

```plaintext
Step 1 Determine the access point for which you want to configure the LED state by entering this command:
show ap summary
```
Obtain the access point ID from the list.

**Step 2** Configure the LED state by entering the following command:

```
config ap led-state {enable | disable} Cisco_AP
```
Controlling Mesh Access Points

This chapter contains these sections:

- Information About Cisco Aironet Mesh Access Points, page 10-1
- Architecture Overview, page 10-11
- Design Considerations, page 10-12
- Adding Mesh Access Points to the Mesh Network, page 10-18
- Configuring Advanced Features, page 10-63
- Converting Indoor Access Points to Mesh Access Points, page 10-123
- Converting Indoor Mesh Access Points to Nonmesh Lightweight Access Points (1130AG, 1240AG), page 10-124
- Configuring Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers, page 10-125

Information About Cisco Aironet Mesh Access Points

Mesh networking employs Cisco Aironet 1500 Series outdoor mesh access points and indoor mesh access points (Cisco Aironet 1040, 1130, 1140, 1240, 1250, 1260, series access points) along with the Cisco Wireless LAN Controller, and Cisco Wireless Control System (WCS) to provide scalable, central management, and mobility between indoor and outdoor deployments. Control and Provisioning of Wireless Access Points (CAPWAP) protocol manages the connection of mesh access points to the network.

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

Controller software release 7.0.116.0 and later releases support these Cisco Aironet mesh access points:

- Cisco Aironet 1520 series outdoor mesh access points consist of the 1522 dual-radio mesh access point and the 1524PS/Serial Backhaul multi-radio mesh access point.

Note

AP1130 and AP1240 must be converted to operate as indoor mesh access points. See the “Converting Indoor Access Points to Mesh Access Points” section on page 10-123.

- Cisco Aironet 1550 series outdoor mesh access points consist of four models:
Chapter 10  Controlling Mesh Access Points

Information About Cisco Aironet Mesh Access Points

- 1552E
- 1552C
- 1552I
- 1552H

In the 7.0.98.0 release, indoor mesh is available on dual band Cisco Aironet 1130 and 1240 series access points. In the 7.0.116.0 release, indoor mesh is also available on dual band 11n access points (Cisco Aironet 1040, 1140, 1250, 1260, 3500 and 3600 series access points). Indoor mesh is not supported with 802.11b/g only access points because 5 GHz is required for mesh backhaul access.

Guidelines and Limitations

- All features discussed in this chapter apply to indoor (1040, 1140, 1250, 1260, 3500, 3600) and outdoor mesh access points (1500 series) unless noted otherwise. Mesh access point or MAP is hereafter used to refer to both indoor and outdoor mesh access points.
- Cisco Aironet 1505 and 1510 access points are not supported in this release.

Additional References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>
| Physical installation and initial configuration of the mesh access points | Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide  
| Converting indoor access points to operate as mesh access points | “Converting Indoor Access Points to Mesh Access Points” section on page 10-123 |
| Mesh feature summary, important notes, and software upgrade steps to migrate from 4.1.19x.xx mesh releases to controller release 7.0.116.0 | Release Notes for Cisco Wireless LAN controllers and Lightweight Access Points for Release 7.0.116.0  

Access Point Roles

Access points within a mesh network operate as either a Root Access Point (RAP) or a Mesh Access Point (MAP).

RAPs have wired connections to their controller, and MAPs have wireless connections to their controller. MAPs communicate among themselves and back to the RAP using wireless connections over the 802.11a 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.

All the possible paths between the MAPs and RAPs form the wireless mesh network. Figure 10-1 shows the relationship between RAPs and MAPs in a mesh network.
Network Access

Wireless mesh networks can simultaneously carry two different traffic types: wireless LAN client traffic and 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:

- MAC authentication—Mesh access points are added to a database to ensure that they are allowed access to a given controller and the mesh network. See the “Converting Indoor Access Points to Mesh Access Points” section on page 10-123.
- External RADIUS authentication—Mesh access points can be externally authorized to use a RADIUS server such as Cisco ACS 4.1 and later releases that support the client authentication type of EAP-FAST with certificates. See the “Configuring RADIUS Servers” section on page 10-28.
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. See the “Configuring Antenna Gain (GUI)” section on page 10-54.

Cisco Indoor Mesh Access Points

With the 7.0.116.0 release, indoor mesh is also available on 802.11n access points (Cisco Aironet 1040, 1140, 1250, 1260, 3500, and 3600 series access points).

With the 7.0 release, indoor mesh is available on Cisco Aironet 1130 and 1240 series access points.

Enterprise 11n mesh is an enhancement added to the CUWN feature to work with the 802.11n access points. Enterprise 11n mesh features are compatible with non-802.11n mesh but adds higher backhaul and client access speeds. The 802.11n 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. Enterprise 11n mesh supports P2P, P2MP, and mesh types of architectures.

You have a choice of ordering indoor access points directly into the bridge mode, so that these access points can be used directly as mesh access points. If you have these access points in a local mode (nonmesh), then you have to connect these access points to the controller and change the 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 nonmesh 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

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 1552 11n outdoor mesh access points, 1522 dual-radio mesh access points, and 1524 multi-radio mesh access points. There are two models of the 1524, which are the following:

- The public safety model, 1524PS
- The serial backhaul model, 1524SB

Note

In the 6.0 release, the AP1524SB access point was launched in A, C and N domains. In the 7.0 release, the AP1524SB access point is launched also in -E, -M, -K, -S, and -T domains.

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 WCS. Communication between outdoor mesh access points (MAPs and RAPs) is over the 802.11a/n radio backhaul. Client traffic is generally transmitted over the 802.11b/g/n radio (802.11a/n can also be configured to accept client traffic), and public safety traffic (AP1524PS only) is transmitted over the 4.9-GHz radio.
The mesh access point can also operate as a relay node for other access points not directly connected to a wired network. Intelligent wireless routing is provided by the Adaptive Wireless Path Protocol (AWPP). This Cisco protocol enables each mesh access point to identify its neighbors and intelligently choose the optimal path to the wired network by calculating the cost of each path in terms of the signal strength and the number of hops required to get to a controller.

AP1500s are manufactured in two different configurations: cable and noncable.

- The cable configuration can be mounted to a cable strand and supports power-over-cable (POC).
- The noncable 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 (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.

Note
See the Cisco Aironet 1520 Series Lightweight Outdoor Access Point Ordering Guide for power, mounting, antenna, and regulatory support by model:

Mesh Deployment Modes

Mesh access points support multiple deployment modes, including the following:

- Wireless mesh
- Wireless backhaul
- Point-to-Multipoint Wireless Bridging
- Point-to-Point Wireless Bridging

Wireless Mesh Network

In a Cisco wireless outdoor mesh network, multiple mesh access points comprise a network that provides secure, scalable outdoor wireless LAN. Figure 10-2 shows an example of a simple mesh network deployment composed of mesh access point (MAPs and RAPs), controllers, and Cisco WCS.

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

Both MAPs and RAPs can provide WLAN client access; however, the location of RAPs are often not suitable for providing client access. All the three access points in Figure 10-2 are located on the building roofs and are functioning as RAPs. These RAPs are connected to the network at each location.

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

Note
For more details on CAPWAP, see the “Architecture Overview” section on page 10-11.
Wireless Backhaul

In a Cisco wireless backhaul network, traffic can be bridged between MAPs and RAPs. Outdoor Mesh AP and indoor AP converted to MAP mode are supported if CAPWAP over CAPWAP using ethernet bridging is supported. Both, local and flexconnect modes are support in MAP using ethernet bridging. This traffic can be from wired devices that are being bridged by the wireless mesh or CAPWAP traffic from the mesh access points. This traffic is always AES encrypted when it crosses a wireless mesh link such as a wireless backhaul (see Figure 10-3).

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

Only 5 GHz backhaul is possible on all mesh access points except 1522 in which either 2.4 or 5 GHz radio can be configured as a backhaul radio (see the “Configuring Advanced Features” section on page 10-63).
Universal Access

You can configure the backhaul on mesh access points to accept client traffic over its 802.11a radio. This feature is identified as Backhaul Client Access in the controller GUI (Monitor > Wireless). When this feature is disabled, backhaul traffic is transmitted only over the 802.11a or 802.11a/n radio and client association is allowed only over the 802.11b/g or 802.11b/g/n radio. For more information about the configuration, see the “Configuring Advanced Features” section on page 10-63.

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 10-4 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 10-4 Point-to-Multipoint Bridging Example

Point-to-Point Wireless Bridging

In a point-to-point bridging scenario, a 1500 Series Mesh AP can be used to extend a remote network by using the backhaul radio to bridge two segments of a switched network (see Figure 10-5). This is fundamentally a wireless mesh network with one MAP and no WLAN clients. Just as in point-to-multipoint networks, client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access.

If you intend to use an Ethernet bridged application, we recommend that you enable the bridging feature on the RAP and on all MAPs in that segment. You must verify that any attached switches to the Ethernet ports of your MAPs are not using VLAN Trunking Protocol (VTP). VTP can reconfigure the trunked VLANs across your mesh and possibly cause a loss in connection for your RAP to its primary WLC. An incorrect configuration can take down your mesh deployment.
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 (see Figure 10-6).

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

1. When you want to use the mesh nodes as bridges.
2. 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.

Range Parameters have to be configured for longer links under the Wireless > Mesh tab. Optimum distance (in feet) should exist between the root access point (RAP) and the farthest mesh access point (MAP). Range from the RAP bridge to the MAP bridge has to be mentioned in feet.
Chapter 10  Controlling Mesh Access Points

Information About Cisco Aironet Mesh Access Points

Figure 10-7 Configuring Range Parameters

The following global parameter applies to all mesh access points when they join the controller and all existing mesh access points in the network:
Range: 150 to 132,000 feet
Default: 12,000 feet

Configuring Mesh Range (CLI)

- To configure the distance between the nodes doing the bridging, enter this command:
  ```
  config mesh range range-in-feet
  ```
- To get the mesh range, enter the following command:
  ```
  show mesh config
  ```
  Information similar to the following:
  ```
  Mesh Range................................. 12000
  Mesh Statistics update period.............. 3 minutes
  Backhaul with client access status........ disabled
  Background Scanning State.................. enabled
  Backhaul Amsdu State....................... disabled
  
  Mesh Security
  Security Mode................................ EAP
  External-Auth.............................. disabled
  Use MAC Filter in External AAA server...... disabled
  Force External Authentication............ disabled
  
  Mesh Alarm Criteria
  Max Hop Count............................... 4
  Recommended Max Children for MAP......... 10
  Recommended Max Children for RAP......... 20
  Low Link SNR................................ 12
  High Link SNR.............................. 60
  Max Association Number.................... 10
  Association Interval....................... 60 minutes
  Parent Change Numbers..................... 3
  Parent Change Interval.................... 60 minutes
Information About Cisco Aironet Mesh Access Points

Mesh Multicast Mode............................... In-Out
Mesh Full Sector DFS.............................. enabled
Mesh Ethernet Bridging VLAN Transparent Mode..... enabled

*Note*
APs reboot after you specify the range.

To estimate the range, you can use range calculators that are available at:
- Cisco 1520 Series Outdoor Mesh Range Calculation Utility:
- Range Calculator for 1550 Series Outdoor Mesh Access Points:

**Assumptions for the AP1522 Range Calculator**

- The AP1522 Range Calculator has been edited to stay within limitations for Tx power and EIRP under the listed regulatory domains. There may be cases where it exceeds the limitations. You must verify that the installation is within the laws of the location in which it is being installed.
- When you use the AP1522 Range Calculator, available power levels change based upon the regulatory domain, the antenna (or antenna gain) selected, the modulation mode, which is based on the data rate selected (OFDM requires a lower power level in some domains). You must verify all parameters after making any parameter changes.
- Rx sensitivity in 2.4 GHz is the composite sensitivity of all three Rx paths. That is, MRC is included in 2.4 GHz. There is only one Rx for 5 GHz.
- You can choose only the channels that the access point is certified for.
- You can select only valid power levels.

**Assumptions for the AP1552 Range Calculator**

- The AP1552 Range Calculator has been edited to stay within limitations for Tx power and EIRP under the listed regulatory domains. There may be cases where it exceeds the limitations. You must verify that the installation is within the laws of the location in which it is being installed.
- All three antenna ports must be used for external antenna models of 1552 for effective performance. Otherwise, range is significantly compromised. 1552 radios have two Tx paths and three Rx paths.
- The Tx power is the total composite power of both Tx paths.
- Rx sensitivity is the composite sensitivity of all three Rx paths. That is, MRC is included.
- The AP1552 Range Calculator assumes that ClientLink (Beamforming) is switched on.
- When you use the AP1552 Range Calculator, available power levels change based upon the regulatory domain, the antenna (or antenna gain) selected, and the data rate selected. You must verify all parameters after making any parameter changes.
- You can select a different antenna than the two that are available by default. If you enter a high gain antenna and choose a power that goes over the EIRP limit, then you get a warning and the range equals 0.
- You can choose only the channels that the access point is certified for.
- You can only select only valid power levels.
Architecture Overview

This section contains the following sections:

- Control And Provisioning of Wireless Access Points (CAPWAP), page 10-11

Control And Provisioning of Wireless Access Points (CAPWAP)

CAPWAP is the provisioning and control protocol used by the controller to manage access points (mesh and nonmesh) in the network. This protocol replaces LWAPP in controller software 5.2 or later releases.

Cisco Adaptive Wireless Path Protocol Wireless Mesh Routing

The Cisco Adaptive Wireless Path Protocol (AWPP) is designed specifically for wireless mesh networking. The path decisions of AWPP are based on the link quality and the number of hops. Ease of deployment, fast convergence, and minimal resource consumption are also key components of AWPP.

The goal of AWPP is to find the best path back to a RAP for each MAP that is part of the RAP’s bridge group. To do this, the MAP actively solicits for neighbor MAPs. 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.

Mesh Neighbors, Parents, and Children

Relationships among access points with the mesh network are labeled as parent, child, or neighbor (see Figure 10-8) as follows:

- 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, 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 the radio frequency (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.
Design Considerations

Each outdoor wireless mesh deployment is unique, and each environment has its own challenges with available locations, obstructions, and available network infrastructure. Design requirements driven by expected users, traffic, and availability needs are also major design criteria. This section describes important design considerations and provides an example of a wireless mesh design.

Wireless Mesh Constraints

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

Wireless Backhaul Data Rate

Backhaul is used to create only the wireless connection between the access points. The backhaul interface by default is 802.11a or 802.11a/n depending upon the access point. The rate selection is important for effective use of the available RF spectrum. The rate can also affect the throughput of client devices, and throughput is an important metric used by industry publications to evaluate vendor devices. Dynamic Rate Adaptation (DRA) introduces a process to estimate optimal transmission rate for packet transmissions. It is important to select rates correctly. If the rate is too high, packet transmissions fail resulting in communication failure. If the rate is too low, the available channel bandwidth is not used, resulting in inferior products, and the potential for catastrophic network congestion and collapse.

Data rates also affect the RF coverage and network performance. Lower data rates, for example 6 Mbps, can extend farther from the access point than can higher data rates, for example 300 Mbps. As a result, the data rate affects cell coverage and consequently the number of access points required. Different data rates are achieved by sending a more redundant signal on the wireless link, allowing data to be easily recovered from noise. The number of symbols sent out for a packet at the 1-Mbps data rate is higher than
the number of symbols used for the same packet at 11 Mbps. Therefore, sending data at the lower bit rates takes more time than sending the equivalent data at a higher bit rate, resulting in reduced throughput.

A lower bit rate might allow a greater distance between MAPs, but there are likely to be gaps in the WLAN client coverage, and the capacity of the backhaul network is reduced. An increased bit rate for the backhaul network either requires more MAPs or results in a reduced SNR between MAPs, limiting mesh reliability and interconnection. For more information about configuring wireless backhaul data rate, see the “Configuring Wireless Backhaul Data Rate” section on page 10-38.

Note

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

The required minimum Link SNR for backhaul links per data rate is shown in Table 10-1.

<table>
<thead>
<tr>
<th>802.11a Data Rate (Mbps)</th>
<th>Minimum Required Link SNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>54</td>
<td>31</td>
</tr>
<tr>
<td>48</td>
<td>29</td>
</tr>
<tr>
<td>36</td>
<td>26</td>
</tr>
<tr>
<td>24</td>
<td>22</td>
</tr>
<tr>
<td>18</td>
<td>18</td>
</tr>
<tr>
<td>12</td>
<td>16</td>
</tr>
<tr>
<td>9</td>
<td>15</td>
</tr>
<tr>
<td>6</td>
<td>14</td>
</tr>
</tbody>
</table>

- The required minimum LinkSNR value is driven by the data rate and the following formula: \( \text{Minimum SNR} + \text{fade margin} \).

Table 10-2 summarizes the calculation by data rate.

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

<table>
<thead>
<tr>
<th>802.11n Data Rate (Mbps)</th>
<th>Minimum SNR (dB) + Fade Margin =</th>
<th>Minimum Required Link SNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>5 + 9 = 14</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>6 + 9 = 15</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>7 + 9 = 16</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>9 + 9 = 18</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>13 + 9 = 22</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>17 + 9 = 26</td>
<td></td>
</tr>
</tbody>
</table>
If you take into account the effect of MRC for calculating Minimum Required Link SNR. Table 10-3 shows the required Link SNR for 802.11a/g (2.4 GHz and 5 GHz) for AP1552 and 1522 with 3 Rx antennas (MRC gain).

\[ \text{LinkSNR} = \text{Minimum SNR} - \text{MRC} + \text{Fade Margin (9 dB)} \]

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

If you consider only 802.11n rates, Table 10-4 shows Link SNR requirements with AP1552 for 2.4 and 5 GHz.

<table>
<thead>
<tr>
<th>No. of Spatial Streams</th>
<th>M CS</th>
<th>Modulation</th>
<th>Minimum SNR (dB)</th>
<th>MRC Gain from 3 RXs (dB)</th>
<th>Fade Margin (dB)</th>
<th>Link SNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MCS 0</td>
<td>BPSK 1/2</td>
<td>5</td>
<td>4.7</td>
<td>9</td>
<td>9.3</td>
</tr>
<tr>
<td>1</td>
<td>MCS 1</td>
<td>QPSK 1/2</td>
<td>7</td>
<td>4.7</td>
<td>9</td>
<td>11.3</td>
</tr>
<tr>
<td>1</td>
<td>MCS 2</td>
<td>QPSK 3/4</td>
<td>9</td>
<td>4.7</td>
<td>9</td>
<td>13.3</td>
</tr>
<tr>
<td>1</td>
<td>MCS 3</td>
<td>16QAM 1/2</td>
<td>13</td>
<td>4.7</td>
<td>9</td>
<td>17.3</td>
</tr>
<tr>
<td>1</td>
<td>MCS 4</td>
<td>16QAM 3/4</td>
<td>17</td>
<td>4.7</td>
<td>9</td>
<td>21.3</td>
</tr>
<tr>
<td>1</td>
<td>MCS 5</td>
<td>64QAM 2/3</td>
<td>20</td>
<td>4.7</td>
<td>9</td>
<td>24.3</td>
</tr>
<tr>
<td>1</td>
<td>MCS 6</td>
<td>64QAM 3/4</td>
<td>22</td>
<td>4.7</td>
<td>9</td>
<td>26.3</td>
</tr>
<tr>
<td>1</td>
<td>MCS 7</td>
<td>64QAM 5/6</td>
<td>23</td>
<td>4.7</td>
<td>9</td>
<td>27.3</td>
</tr>
<tr>
<td>2</td>
<td>MCS 8</td>
<td>BPSK 1/2</td>
<td>5</td>
<td>1.7</td>
<td>9</td>
<td>12.3</td>
</tr>
<tr>
<td>2</td>
<td>MCS 9</td>
<td>QPSK 1/2</td>
<td>7</td>
<td>1.7</td>
<td>9</td>
<td>14.3</td>
</tr>
<tr>
<td>2</td>
<td>MCS 10</td>
<td>QPSK 3/4</td>
<td>9</td>
<td>1.7</td>
<td>9</td>
<td>16.3</td>
</tr>
<tr>
<td>2</td>
<td>MCS 11</td>
<td>16QAM 1/2</td>
<td>13</td>
<td>1.7</td>
<td>9</td>
<td>20.3</td>
</tr>
<tr>
<td>2</td>
<td>MCS 12</td>
<td>16QAM 3/4</td>
<td>17</td>
<td>1.7</td>
<td>9</td>
<td>24.3</td>
</tr>
<tr>
<td>2</td>
<td>MCS 13</td>
<td>64QAM 2/3</td>
<td>20</td>
<td>1.7</td>
<td>9</td>
<td>27.3</td>
</tr>
<tr>
<td>2</td>
<td>MCS 14</td>
<td>64QAM 3/4</td>
<td>22</td>
<td>1.7</td>
<td>9</td>
<td>29.3</td>
</tr>
<tr>
<td>2</td>
<td>MCS 15</td>
<td>64QAM 5/6</td>
<td>23</td>
<td>1.7</td>
<td>9</td>
<td>30.3</td>
</tr>
</tbody>
</table>
With two spatial streams, the MRC gain is halved, that is the MRC gain is reduced by 3 dB. This is because the system has 10 log (3/2 SS) instead of 10 log (3/1 SS). If there were to have been 3 SS with 3 RX, then the MRC gain would have been zero.

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

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

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

- Number of mesh access points supported per controller. For more information, see the “Controller Planning” section.

### 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 can help solve problems related to adoption of 802.11n in mixed-client networks by ensuring that 802.11a/g clients operate at the best possible rates, especially when they are near cell boundaries.

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

The 802.11n systems take advantage of multipath by sending multiple radio signals simultaneously. Each of these signals, called a spatial stream, is sent from its own antenna using its own transmitter. Because there is some space between these antennas, each signal follows a slightly different path to the receiver, a situation called spatial diversity. The receiver has multiple antennas as well, each with its own radio that independently decodes the arriving signals, and each signal is combined with signals from the other receiver radios which 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.
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. For 802.11 a/g clients, some of the capabilities of the extra transmit path was lying idle. In addition, for many networks, the performance of the installed 802.11 a/g client base would be a limiting factor on the network.

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

Cisco ClientLink technology effectively enables the access point to optimize the SNR exactly at the position where the client is placed. Cisco 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 Cisco 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, Cisco ClientLink increases the overall capacity of the system, which means an efficient use of spectrum resources.

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

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

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

**Configuring Cisco ClientLink (CLI)**

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

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

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

**Step 2**
Reenable the network by entering this command:

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

**Step 3**
Save your changes by entering this command:

```
save config
```
Commands Related to Cisco ClientLink

- The following commands are to be entered in the AP console:
  - To find a client in the AP rbf table, enter the `show interface dot110` command.
- The following commands on the AP console are used for troubleshooting:
  - To show that ClientLink is enabled on a radio, enter the `show controllers | inc Beam` command.

  The output is displayed as follows:
  
  Legacy Beamforming: Configured Yes, Active Yes, RSSI Threshold -50 dBm
  Legacy Beamforming: Configured Yes, Active Yes, RSSI Threshold -60 dBm

Controller Planning

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

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

  For example, you can have 72 Cisco 4400 Series Controllers in a mobility group, and each Cisco 4400 Series Controller supports 100 local access points, which gives a total number of 7200 possible access points per mobility group.

- Number of mesh access points supported per controller. See Table 10-5.

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

<table>
<thead>
<tr>
<th>Controller Model</th>
<th>Local AP Support (nonmesh)¹</th>
<th>Maximum Possible Mesh AP Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>5508</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td>4404</td>
<td>100</td>
<td>150</td>
</tr>
<tr>
<td>2504</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>2106</td>
<td>6</td>
<td>11</td>
</tr>
<tr>
<td>2112</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>2125</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>WiSM</td>
<td>300</td>
<td>375</td>
</tr>
<tr>
<td>WiSM2</td>
<td>500</td>
<td>500</td>
</tr>
</tbody>
</table>

¹. Local AP support is the total number of nonmesh APs supported on the controller model.

Note

The Wireless LAN Controller modules NM and NME now support mesh 1520 series access points from Wireless LAN Controller (WLC) software release 5.2 and later releases.
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.

Mesh APs (MAPs/RAPs) are counted as full APs on Cisco 5508 Controllers.

With other controller platforms, MAPs are counted as half APs.

Data Plane Transport Layer Security (DTLS) is not supported on mesh access points.

Adding Mesh Access Points to the Mesh Network

This section assumes that the controller is already active in the network and is operating in Layer 3 mode. Controller ports that the mesh access points connect to should be untagged.

Ensure that you do the following:

1. Add the MAC address of the mesh access point to the controller’s MAC filter. See the “Adding MAC Addresses of Mesh Access Points to the MAC Filter” section on page 10-19.

2. Define the role (RAP or MAP) for the mesh access point. See the “Defining Mesh Access Point Role” section on page 10-20.

Note: CAPWAP supports only layer3 mode and it does not support layer2 mode.

3. Configure a primary, secondary, and tertiary controller for each mesh access point. See the “Configuring Multiple Controllers Using DHCP 43 and DHCP 60” section on page 10-21.

4. Configure a backup controller. See the “Configuring Backup Controllers” procedure on page 10-22.


7. Configure universal client access. Configuring universal client access is part of the Configuring Advanced Features section. See the “Universal Client Access” section on page 10-66.

8. Configure local mesh parameters. See the “Configuring Local Mesh Parameters” section on page 10-38.

9. Configure mobility groups (if desired) and assign controllers. See Chapter 12, Configuring Mobility Groups.
Adding MAC Addresses of Mesh Access Points to the MAC Filter

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

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

**Note**

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

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

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

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

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

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

**Step 5** In the Description field, specify a description of the mesh access point. The text that you enter identifies the mesh access point on the controller.
Adding Mesh Access Points to the Mesh Network

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

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

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

Step 8
Click Save Configuration to save your changes.

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

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

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

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

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

Step 2
To save your changes, enter this command:

```
save config
```

Defining Mesh Access Point Role

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

Information About MAP and RAP Association With the Controller

- A MAP always sets the Ethernet port as the primary backhaul if it is UP, and secondarily the 802.11a/n radio. This gives the network administrator time to reconfigure the mesh access point as a RAP, initially. For faster convergence on the network, we recommend that you do not connect any Ethernet device to the MAP until it has joined the mesh network.
- A MAP that fails to connect to a controller on a UP Ethernet port, sets the 802.11a/n radio as the primary backhaul. If a MAP fails to find a neighbor or fails to connect to a controller through a neighbor, the Ethernet port is set as the primary backhaul again.
- A MAP connected to a controller over an Ethernet port does not build a mesh topology (unlike a RAP).
- A RAP always sets the Ethernet port as the primary backhaul.
If the Ethernet port is DOWN on a RAP, or a RAP fails to connect to a controller on a UP Ethernet port, the 802.11a/n radio is set as the primary backhaul for 15 minutes. Failing to find a neighbor or failing to connect to a controller via any neighbor on the 802.11a/n radio causes the primary backhaul to go into the scan state. The primary backhaul begins its scan with the Ethernet port.

**Configuring the AP Role (GUI)**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Click <strong>Wireless</strong> to open the All APs page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the name of an access point. The All APs &gt; Details (General) page appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the <strong>Mesh</strong> tab.</td>
</tr>
</tbody>
</table>

![All APs > Details for (Mesh) Page](image)

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Choose <strong>RootAP</strong> or <strong>MeshAP</strong> from the AP Role drop-down list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>Click <strong>Apply</strong> to commit your changes and to cause the access point to reboot.</td>
</tr>
</tbody>
</table>

**Configuring the AP Role (CLI)**

```text
config ap role {rootAP | meshAP} Cisco_AP
```

**Configuring Multiple Controllers Using DHCP 43 and DHCP 60**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Enter configuration mode at the Cisco IOS CLI.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Create the DHCP pool, including the necessary parameters such as the default router and name server. The commands used to create a DHCP pool are as follows:</td>
</tr>
<tr>
<td></td>
<td><code>ip dhcp pool pool_name</code></td>
</tr>
<tr>
<td></td>
<td><code>network IP Network Netmask</code></td>
</tr>
</tbody>
</table>
**default-router** Default router

dns-server DNS Server

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

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

```
option 60 ascii VCI string
```

For the VCI string, use one of the values below. The quotation marks must be included.
- For Cisco 1550 series access points, enter `Cisco AP c1550`
- For Cisco 1520 series access points, enter `Cisco AP c1520`
- For Cisco 1240 series access points, enter `Cisco AP c1240`
- For Cisco 1130 series access points, enter `Cisco AP c1130`

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

```
option 43 hex hex string
```

The hex string is assembled by concatenating the TLV values as follows:

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

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

The resulting Cisco IOS command added to the DHCP scope is as follows:

```
option 43 hex f1080a7e7e020a7f7f02
```

---

**Configuring Backup Controllers**

This section contains the following topics:
- **Information About Configuring Backup Controllers**, page 10-23
- **Guidelines and Limitations**, page 10-23
- **Configuring Backup Controllers (GUI)**, page 10-23
- **Configuring Backup Controllers (CLI)**, page 10-25
Info about Configuring Backup Controllers

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

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

Guidelines and Limitations

- The fast heartbeat timer is not supported on mesh access points. The fast heartbeat timer is only configured on access points in local and flexconnect modes.

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

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

- If you inadvertently configure a controller that is running software release 6.0 with a failover controller that is running a different software release (such as 4.2, 5.0, 5.1, or 5.2), the mesh access point might take a long time to join the failover controller because the mesh access point starts the discovery process in LWAPP and then changes to CAPWAP discovery.

Configuring Backup Controllers (GUI)

Step 1 Choose Wireless > Access Points > Global Configuration to open the Global Configuration page.
Figure 10-11  Global Configuration Page

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

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

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

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

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

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

Step 5  Click Apply to commit your changes.

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

a. Choose Access Points > All APs to open the All APs page.

b. Click the name of the access point for which you want to configure primary, secondary, and tertiary backup controllers.

c. Click the High Availability tab.
d. If desired, specify the name and IP address of the primary backup controller for this access point in the Primary Controller fields.

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

e. If desired, specify the name and IP address of the secondary backup controller for this mesh access point in the Secondary Controller fields.

f. If desired, specify the name and IP address of the tertiary backup controller for this mesh access point in the Tertiary Controller fields.

g. No change is required to the AP Failover Priority value. The default value for mesh access points is `critical` and it cannot be modified.

h. Click **Apply** to commit your changes.

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

### Configuring Backup Controllers (CLI)

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

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

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

**Step 2** To configure a secondary controller for a specific mesh access point, enter this command:
Adding Mesh Access Points to the Mesh Network

Chapter 10  Controlling Mesh Access Points

config ap secondary-base controller_name Cisco_AP [controller_ip_address]

Step 3  To configure a tertiary controller for a specific mesh access point, enter this command:
config ap tertiary-base controller_name Cisco_AP [controller_ip_address]

Step 4  To configure a primary backup controller for all mesh access points, enter this command:
config advanced backup-controller primary backup_controller_name backup_controller_ip_address

Step 5  To configure a secondary backup controller for all mesh access points, enter this command:
config advanced backup-controller secondary backup_controller_name backup_controller_ip_address

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

Step 6  To configure the mesh access point primary discovery request timer, enter this command:
config advanced timers ap-primary-discovery-timeout interval
where interval is a value between 30 and 3600 seconds. The default value is 120 seconds.

Step 7  To configure the mesh access point discovery timer, enter this command:
config advanced timers ap-discovery-timeout interval
where interval is a value between 1 and 10 seconds (inclusive). The default value is 10 seconds.

Step 8  To configure the 802.11 authentication response timer, enter this command:
config advanced timers auth-timeout interval
where interval is a value between 10 and 600 seconds (inclusive). The default value is 10 seconds.

Step 9  To save your changes, enter this command:
save config

Step 10 To view a mesh access point’s configuration, enter these commands:
  •  show ap config general Cisco_AP
  •  show advanced backup-controller
  •  show advanced timers
  •  show mesh config

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

Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP5
Country code..................................... US - United States
Regulatory Domain allowed by Country......... 802.11bg:-AB  802.11a:-AB
AP Country code.................................. US - United States
AP Regulatory Domain......................... 802.11bg:-A  802.11a:-N
Switch Port Number.............................. 1
MAC Address..................................... 00:13:80:60:48:3e
IP Address Configuration...................... DHCP
IP Address...................................... 1.100.163.133
...
Primary Cisco Switch Name.................... 1-4404
Primary Cisco Switch IP Address.............. 2.2.2.2
Secondary Cisco Switch Name................. 1-4404
Secondary Cisco Switch IP Address.......... 2.2.2.2
Tertiary Cisco Switch Name.................... 2-4404
Tertiary Cisco Switch IP Address................. 1.1.1.4

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

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

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

- Authentication Response Timeout (seconds)........ 10
- Rogue Entry Timeout (seconds).................. 1300
- AP Heart Beat Timeout (seconds)................ 30
- AP Discovery Timeout (seconds).................. 10
- AP Primary Discovery Timeout (seconds)......... 120

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

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

---

**Configuring External Authentication and Authorization Using a RADIUS Server**

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

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

- The RADIUS server to be used as an AAA server must be configured on the controller.
- The controller must also be configured on the RADIUS server.
- Add the mesh access point configured for external authorization and authentication to the user list of the RADIUS server. For additional details, see the “Adding a Username to a RADIUS Server” section on page 10-28.
- Configure EAP-FAST on the RADIUS server and install the certificates. EAP-FAST authentication is required if mesh access points are connected to the controller using an 802.11a interface; the external RADIUS servers need to trust Cisco Root CA 2048. For information about installing and trusting the CA certificates, see the “Configuring RADIUS Servers” section on page 10-28.
Chapter 10  Controlling Mesh Access Points

Adding Mesh Access Points to the Mesh Network

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

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

Configuring RADIUS Servers

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

Step 2  Install the certificates as follows:
  a. From the CiscoSecure ACS main menu, click System Configuration > ACS Certificate Setup > ACS Certification Authority Setup.
  b. In the CA certificate file box, type the CA certificate location (path and name). For example: C:\Certs\crca2048.cer.
  c. Click Submit.

Step 3  Configure the external RADIUS servers to trust the CA certificate as follows:
  b. Select the check box next to the Cisco Root CA 2048 (Cisco Systems) certificate name.
  c. Click Submit.
  d. To restart ACS, choose System Configuration > Service Control, and then click Restart.

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

Adding a Username to a RADIUS Server

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

For remote authorization and authentication, EAP-FAST uses the manufacturer’s certificate (CERT) to authenticate the child mesh access point. Additionally, this manufacturer certificate-based identity serves as the username for the mesh access point in user validation.
For Cisco IOS-based mesh access points, in addition to adding the MAC address to the user list, you need to enter the `platform_name_string–MAC_address` string to the user list (for example, c1240-001122334455). The controller first sends the MAC address as the username; if this first attempt fails, then the controller sends the `platform_name_string–MAC_address` string as the username.

**Example: RADIUS Server Username Entry**

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

- **platform_name_string–MAC_address**
  - User: c1520-aabbccddeeff
  - Password: cisco
- **Hyphen Delimited MAC Address**
  - User: aa-bb-cc-dd-ee-ff
  - Password: aa-bb-cc-dd-ee-ff

*Note*
The platform AP1552 uses a platform name of c1520.

**Enabling External Authentication of Mesh Access Points**

This section contains the following topics:

- Enabling External Authentication of Mesh Access Points (GUI), page 10-30
- Enable External Authentication of Mesh Access Points (CLI), page 10-30
Enabling External Authentication of Mesh Access Points (GUI)

**Step 1** Choose **Wireless > Mesh**. The Mesh page appears.

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

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

**Step 4** Click **Apply**.

**Step 5** Click **Save Configuration**.

Enable External Authentication of Mesh Access Points (CLI)

**Step 1** `config mesh security eap`

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

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

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

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

Viewing Security Statistics

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

`show mesh security-stats Cisco_AP`
Use this command to display packet error statistics and a count of failures, timeouts, and association and authentication successes as well as reassociations and re authentications for the specified access point and its child.

## Configuring Global Mesh Parameters

This section contains the following topics:

- Information About Configuring Global Mesh Parameters, page 10-31
- Configuring Global Mesh Parameters (GUI), page 10-31
- Configuring Global Mesh Parameters (CLI), page 10-36

### Information About Configuring Global Mesh Parameters

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

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

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

### Configuring Global Mesh Parameters (GUI)

**Step 1** Choose Wireless > Mesh.
Step 2 Modify the mesh parameters as appropriate.

Table 10-6 Global Mesh Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range (RootAP to MeshAP)</td>
<td>The optimum distance (in feet) that should exist between the root access point (RAP) and the mesh access point (MAP). This global parameter applies to all mesh access points when they join the controller and all existing mesh access points in the network.</td>
</tr>
<tr>
<td><strong>Range:</strong> 150 to 132,000 feet</td>
<td><strong>Default:</strong> 12,000 feet</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>After this feature is enabled, all mesh access points reboot.</td>
</tr>
<tr>
<td>IDS (Rogue and Signature Detection)</td>
<td>When you enable this feature, IDS reports are generated for all traffic on the client access only and not on the backhaul.  When you disable this feature, no IDS reports are generated, which preserves bandwidth on the backhaul. You have to use the following command to enable or disable it on the mesh APs: &lt;br&gt; `config mesh ids-state [enable</td>
</tr>
</tbody>
</table>
**Table 10-6  Global Mesh Parameters (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backhaul Client Access</td>
<td><strong>Note</strong> This parameter applies to mesh access points with two or more radios (1552, 1524SB, 1522, 1240, 1130, and 11n indoor mesh APs) <em>excluding</em> the 1524PS. When Universal Client Access is enabled, it allows wireless client association over the backhaul radio. Generally, backhaul radio is a 5-GHz radio for most of the mesh access points except for 1522 where backhaul can be 2.4 GHz. This means that a backhaul radio can carry both backhaul traffic and client traffic. When Universal Client Access is disabled, only backhaul traffic is sent over the backhaul radio and client association is only over the second radio(s). <strong>Default:</strong> Disabled <strong>Note</strong> After this feature is enabled, all mesh access points reboot.</td>
</tr>
</tbody>
</table>
Adding Mesh Access Points to the Mesh Network

VLAN Transparent

This feature determines how a mesh access point handles VLAN tags for Ethernet bridged traffic.

**Note**  See the “Configuring Advanced Features” section on page 10-63 for overview and additional configuration details.

If VLAN Transparent is enabled, then VLAN tags are not handled and packets are bridged as untagged packets.

**Note**  No configuration of Ethernet ports is required when VLAN transparent is enabled. The Ethernet port passes both tagged and untagged frames without interpreting the frames.

If VLAN Transparent is disabled, then all packets are handled according to the VLAN configuration on the port (trunk, access, or normal mode).

**Note**  If the Ethernet port is set to Trunk mode, Ethernet VLAN tagging must be configured. See “Enabling Ethernet Bridging (GUI)” section on page 10-44.

**Note**  For an overview of normal, access, and trunk Ethernet port use, see “Ethernet Port Notes” section on page 10-72.

**Note**  To use VLAN tagging, you must uncheck the VLAN Transparent check box.

**Note**  VLAN Transparent is enabled as a default to ensure a smooth software upgrade from 4.1.192.xxM releases to release 5.2. Release 4.1.192.xxM does not support VLAN tagging (see Figure 10-14).

**Default:** Enabled.

Security Mode

Defines the security mode for mesh access points: Pre-Shared Key (PSK) or Extensible Authentication Protocol (EAP).

**Note**  EAP must be selected if external MAC filter authorization using a RADIUS server is configured.

**Note**  Local EAP or PSK authentication is performed within the controller if the External MAC Filter Authorization parameter is disabled (check box unchecked).

**Options:** PSK or EAP

**Default:** EAP
External MAC Filter Authorization

MAC filtering uses the local MAC filter on the controller by default.

When external MAC filter authorization is enabled, if the MAC address is not found in the local MAC filter, then the MAC address in the external RADIUS server is used.

This protects your network against rogue mesh access points by preventing mesh access points that are not defined on the external server from joining.

Before employing external authentication within the mesh network, the following configuration is required:

- The RADIUS server to be used as an AAA server must be configured on the controller.
- The controller must also be configured on the RADIUS server.
- The mesh access point configured for external authorization and authentication must be added to the user list of the RADIUS server.
  - For remote authorization and authentication, EAP-FAST uses the manufacturer’s certificate (CERT) to authenticate the child mesh access point. Additionally, this manufacturer certificate-based identity serves as the username for the mesh access point in user validation.
  - For IOS-based mesh access points (1130, 1240, 1522, 1524), the platform name of the mesh access point is located in front of its Ethernet address within the certificate; therefore, their username for external RADIUS servers is $platform_name_{string}\_Ethernet\_MAC\_address$ such as $c1520\_001122334455$.
- The certificates must be installed and EAP-FAST must be configured on the RADIUS server.

**Note** When this capability is not enabled, by default, the controller authorizes and authenticates mesh access points using the MAC address filter.

**Default:** Disabled.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External MAC Filter Authorization</td>
<td>MAC filtering uses the local MAC filter on the controller by default. When external MAC filter authorization is enabled, if the MAC address is not found in the local MAC filter, then the MAC address in the external RADIUS server is used. This protects your network against rogue mesh access points by preventing mesh access points that are not defined on the external server from joining. Before employing external authentication within the mesh network, the following configuration is required: - The RADIUS server to be used as an AAA server must be configured on the controller. - The controller must also be configured on the RADIUS server. - The mesh access point configured for external authorization and authentication must be added to the user list of the RADIUS server. - For remote authorization and authentication, EAP-FAST uses the manufacturer’s certificate (CERT) to authenticate the child mesh access point. Additionally, this manufacturer certificate-based identity serves as the username for the mesh access point in user validation. - For IOS-based mesh access points (1130, 1240, 1522, 1524), the platform name of the mesh access point is located in front of its Ethernet address within the certificate; therefore, their username for external RADIUS servers is $platform_name_{string}_Ethernet_MAC_address$ such as $c1520_001122334455$. - The certificates must be installed and EAP-FAST must be configured on the RADIUS server. <strong>Note</strong> When this capability is not enabled, by default, the controller authorizes and authenticates mesh access points using the MAC address filter. <strong>Default:</strong> Disabled.</td>
</tr>
</tbody>
</table>
Adding Mesh Access Points to the Mesh Network

Step 3 Click Apply to commit your changes.
Step 4 Click Save Configuration to save your changes.

Configuring Global Mesh Parameters (CLI)

Note See the “Configuring Global Mesh Parameters (GUI)” section on page 10-31 for descriptions, valid ranges, and default values of the parameters used in the CLI commands.

Step 1 To specify the maximum range (in feet) of all mesh access points in the network, enter this command:
```config mesh range feet```
To see the current range, enter the show mesh range command.

Step 2 To enable or disable IDS reports for all traffic on the backhaul, enter this command:
```config mesh ids-state { enable | disable }```

Step 3 To specify the rate (in Mbps) at which data is shared between access points on the backhaul interface, enter this command:
```config ap bhrate { rate | auto } Cisco_AP```

Step 4 To enable or disable client association on the primary backhaul (802.11a) of a mesh access point, enter these commands:
```config mesh client-access { enable | disable }
config ap wlan { enable | disable } 802.11a Cisco_AP
config ap wlan { add | delete } 802.11a wlan_id Cisco_AP```

Step 5 To enable or disable VLAN transparent, enter this command:
```config mesh ethernet-bridging VLAN-transparent { enable | disable }```

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

a. To provide local authentication of the mesh access point by the controller, enter this command:
```config mesh security { eap | psk }```

b. To store the MAC address filter in an external RADIUS server for authentication instead of the controller (local), enter these commands:
```config macfilter mac-delimiter colon
cfg mesh security rad-mac-filter enable
cfg mesh radius-server index enable```

c. To provide external authentication on a RADIUS server and define a local MAC filter on the controller, enter these commands:
```config mesh security eap
cfg macfilter mac-delimiter colon
cfg mesh security rad-mac-filter enable
cfg mesh radius-server index enable
cfg mesh security force-ext-auth enable```
d. To provide external authentication on a RADIUS server using a MAC username (such as c1520-123456) on the RADIUS server, enter these commands:

- `config macfilter mac-delimiter colon`
- `config mesh security rad-mac-filter enable`
- `config mesh radius-server index enable`
- `config mesh security force-ext-auth enable`

**Step 7** To save your changes, enter this command:

`save config`

---

**Viewing Global Mesh Parameter Settings (CLI)**

- `show mesh client-access`—When Universal Client Access is enabled, it allows wireless client association over the backhaul radio. Generally, backhaul radio is a 5-GHz radio for most of the mesh access points except for 1522 where backhaul can be 2.4 GHz. This means that a backhaul radio can carry both backhaul traffic and client traffic.

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

Example:

`show mesh client-access`

Backhaul with client access status: enabled

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

Example:

`show mesh ids-state`

Outdoor Mesh IDS(Rogue/Signature Detect): .... Disabled

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

Example:

`show mesh config`

Mesh Range....................................... 12000
Mesh Statistics update period.................... 3 minutes
Backhaul with client access status............ disabled
Background Scanning State....................... enabled
Backhaul Amsdu State.......................... disabled

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

Mesh Alarm Criteria
- Max Hop Count.................................. 4
- Recommended Max Children for MAP.......... 10
- Recommended Max Children for RAP......... 20
- Low Link SNR................................. 12
- High Link SNR............................... 60
Adding Mesh Access Points to the Mesh Network

Max Association Number........................ 10
Association Interval.......................... 60 minutes
Parent Change Numbers......................... 3
Parent Change Interval........................ 60 minutes

Mesh Multicast Mode.............................. In-Out
Mesh Full Sector DFS............................. enabled
Mesh Ethernet Bridging VLAN Transparent Mode..... enabled

Configuring Local Mesh Parameters

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

- Backhaul Data Rate. See the “Configuring Wireless Backhaul Data Rate” section on page 10-38.
- Ethernet Bridging. See the “Configuring Ethernet Bridging” section on page 10-43.
- Bridge Group Name. See the “Configuring Ethernet Bridging” section on page 10-43.
- Workgroup Bridge. See the “Configuring Workgroup Bridges” section on page 10-82.
- Public Safety Band Settings. See the “Configuring Public Safety Band Settings” section on page 10-46.
- Cisco 3200 Series Association and Interoperability. See the “Table 10-10 identifies mesh access points and their respective frequency bands that support WGB.” section on page 10-91.
- Power and Channel Setting. See the “Configuring Power and Channel Settings” section on page 10-51.
- Antenna Gain Settings. See the “Configuring Antenna Gain” section on page 10-54.
- Backhaul channel deselection on serial backhaul access point. See the “Backhaul Channel Deselection on Serial Backhaul Access Point” section on page 10-55.
- Dynamic Channel Assignment. See the “Configuring Dynamic Channel Assignment (GUI)” section on page 10-60.

Configuring Wireless Backhaul Data Rate

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

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

Data rates also affect the RF coverage and network performance. Lower data rates, for example 6 Mbps, can extend farther from the access point than can higher data rates, for example 300 Mbps. As a result, the data rate affects cell coverage and consequently the number of access points required. Different data rates are achieved by sending a more redundant signal on the wireless link, allowing data to be easily recovered from noise. The number of symbols sent out for a packet at the 1-Mbps data rate is higher than the number of symbols used for the same packet at 11 Mbps. Therefore, sending data at the lower bit rates takes more time than sending the equivalent data at a higher bit rate, resulting in reduced throughput.
In the controller release 5.2, the default data rate for the mesh 5-GHz backhaul is 24 Mbps. It remains the same with 6.0 and 7.0 controller releases.

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

We recommend that you configure the mesh backhaul to Auto.

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

A lower bit rate might allow a greater distance between MAPs, but there are likely to be gaps in the WLAN client coverage, and the capacity of the backhaul network is reduced. An increased bit rate for the backhaul network either requires more MAPs or results in a reduced SNR between MAPs, limiting mesh reliability and interconnection.

Figure 10-15 shows the RAP using the "auto" backhaul data rate, and it is currently using 54 Mbps with its child MAP.

**Figure 10-15  Bridge Rate Set to Auto**

![Bridge Rate Set to Auto](image)

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

**Related Commands**

Use these commands to obtain information about backhaul:

- **config ap bhrate**—Configures the Cisco Bridge backhaul Tx rate.
  
  Syntax:
  
  `config ap bhrate backhaul-rate ap-name`

  **Note**
  Preconfigured data rates for each AP (RAP=18 Mbps, MAP1=36 Mbps) are preserved after the upgrade to 6.0 or later software releases.

  Before you upgrade to the 6.0 release, if you have the backhaul data rate configured to any data rate, then the configuration is preserved.
This example shows how to configure a backhaul rate of 36000 Kbps on a RAP:

```
config ap bhrate 36000 HPRAP1
```

- `show ap bhrate`—Displays the Cisco Bridge backhaul rate.

Syntax:

```
show ap bhrate ap-name
```

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

Example:

```
show mesh neigh summary HPRAP1
```

<table>
<thead>
<tr>
<th>AP Name/Radio</th>
<th>Channel</th>
<th>Rate</th>
<th>Link-Snr</th>
<th>Flags</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0B:85:5C:B9:20</td>
<td>auto</td>
<td>4</td>
<td>0x10e8fcb8</td>
<td>BEACON</td>
<td></td>
</tr>
<tr>
<td>00:0B:85:5F:60:60</td>
<td>auto</td>
<td>4</td>
<td>0x10e8fcb8</td>
<td>BEACON DEFAULT</td>
<td></td>
</tr>
<tr>
<td>00:0B:85:62:1E:00</td>
<td>auto</td>
<td>4</td>
<td>0x10e8fcb8</td>
<td>BEACON</td>
<td></td>
</tr>
<tr>
<td>00:0B:85:70:88:C:A0</td>
<td>auto</td>
<td>1</td>
<td>0x10e8fcb8</td>
<td>BEACON</td>
<td></td>
</tr>
<tr>
<td>HPMAP1</td>
<td>165</td>
<td>54</td>
<td>40</td>
<td>0x36</td>
<td>CHILD BEACON</td>
</tr>
<tr>
<td>HJMAP2</td>
<td>0</td>
<td>auto</td>
<td>4</td>
<td>0x10e8fcb8</td>
<td>BEACON</td>
</tr>
</tbody>
</table>

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

In AP1524 SB, Slot 2 in the 5-GHz radio in the RAP is used to extend the backhaul in the downlink direction, whereas Slot 2 in the 5-GHz radio in the MAP is used for backhaul in the uplink. We recommend using a directional antenna with the Slot 2 radio. MAPs extend Slot 1 radio in the downlink direction with Omni or directional antenna also providing client access. Client access can be provided on the Slot 2 radio from the 7.0 release onwards.

AP1524SB provides you with better throughput, and throughput rarely degrades after the first hop. The performance of AP1524SB is better than AP1522 and AP1524PS because these APs have only a single radio for the backhaul uplink and downlink (see Figure 10-16, Figure 10-17, Figure 10-18, and Figure 10-19).
**Note**

With DRA, each hop uses the best possible data rate for the backhaul. The data rate can be changed on a per-AP basis.
Adding Mesh Access Points to the Mesh Network

Figure 10-18 1524SB TCP Downstream Rate Auto

Figure 10-19 1524 TCP Downstream (24 Mbps)

Note Using 1552 802.11n provides you higher throughput and more capacity. It offers a very fat backhaul pipe to start with from the RAP.
For security reasons, the Ethernet port on all MAPs is disabled by default. It can be enabled only by configuring Ethernet bridging on the root and its respective MAP.

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

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

Due to the exceptions and to prevent loop issues, we recommend that you do not connect two MAPs to each other over their Ethernet ports, unless they are configured as trunk ports on different native VLANs, and each is connected to a similarly configured switch.

Ethernet bridging has to be enabled for two scenarios:

1. When you want to use the mesh nodes as bridges. (See Figure 10-21.)

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

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

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

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

**Step 3** At the details page click the Mesh tab.

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

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

**Step 6** Click Apply to commit your changes. An Ethernet Bridging section appears at the bottom of the page listing each of the Ethernet ports of the mesh access point.
Step 7  Ensure that you enable Ethernet bridging for every parent mesh AP taking the path from the mesh AP in question to the controller. For example, if you enable Ethernet bridging on MAP2 in Hop 2, then you must also enable Ethernet bridging on MAP1 (parent MAP), and on the RAP connecting to the controller.

Configuring Bridge Group Names

Bridge group names (BGNs) control the association of mesh access points. BGNs can logically group radios to avoid two networks on the same channel from communicating with each other. The setting is also useful if you have more than one RAP in your network in the same sector (area). BGN is a string of 10 characters maximum.

A BGN of NULL VALUE is assigned by default by manufacturing. Although not visible to you, it allows a mesh access point to join the network prior to your assignment of your network-specific BGN.

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

Configuring Bridge Group Names (CLI)

- Using the CLI, enter the following command:

  `config ap bridgegroupname set bridge-group-name`

  Information similar to the following appears:

  Setting bridgegroupname on an AP permanently restricts the APs to which it may connect, use with caution.
  Are you sure you want to continue? (y/n) n

  AP bridgegroupname not changed!

  The mesh access point reboots after a BGN configuration.

Caution

Exercise caution when you configure a BGN on a live network. Always start a BGN assignment from the farthest-most node (last node, bottom of mesh tree) and move up toward the RAP to ensure that no mesh access points are dropped due to mixed BGNs (old and new BGNs) within the same network.

Verifying Bridge Group Names (CLI)

- To verify the BGN, enter the following command:

  `show ap config general AP_Name`

  Information similar to the following is displayed.
Verifying Bridge Group Names (GUI)

**Step 1**  Click Wireless > Access Points > AP Name. The details page for the selected mesh access point appears.

**Step 2**  Click the Mesh tab. Details for the mesh access point including the BGN appears.

### Figure 10-23  AP Name > Mesh

<table>
<thead>
<tr>
<th>Bridge Group Name</th>
<th>Primary Cisco Switch Name</th>
<th>Administrative State</th>
<th>Operation State</th>
<th>Mirroring Mode</th>
<th>AP Mode</th>
<th>AP Role</th>
<th>Ethernet Bridging</th>
<th>Basic Safety Band</th>
<th>BGN Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuring Public Safety Band Settings

A public safety band (4.9 GHz) is supported on the AP1522 and AP1524PS.

---

Verifying Bridge Group Names (GUI)

**Step 1**  Click Wireless > Access Points > AP Name. The details page for the selected mesh access point appears.

**Step 2**  Click the Mesh tab. Details for the mesh access point including the BGN appears.

### Figure 10-23  AP Name > Mesh

<table>
<thead>
<tr>
<th>Bridge Group Name</th>
<th>Primary Cisco Switch Name</th>
<th>Administrative State</th>
<th>Operation State</th>
<th>Mirroring Mode</th>
<th>AP Mode</th>
<th>AP Role</th>
<th>Ethernet Bridging</th>
<th>Basic Safety Band</th>
<th>BGN Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuring Public Safety Band Settings

A public safety band (4.9 GHz) is supported on the AP1522 and AP1524PS.
For the AP1524PS, the 4.9-GHz radio is independent of the 5-GHz radio and is not used for backhaul. The 5.8 GHz is used only for backhaul, and there is no client access possible on it. On the AP1524PS, the 4.9-GHz band is enabled by default.
- In Japan, 4.9 GHz is enabled by default as 4.9 GHz is unlicensed.
- For AP1522s, you can enable the 4.9-GHz public safety band on the backhaul. This step can only be done at the global level and cannot be done on a per mesh access point basis.
  - For client access on the 4.9-GHz band on the AP1522, you have to enable the feature universal client access.
- For public safety-only deployments, the AP1522 and the AP1524PS must each be connected to its own separate RAP-based tree. For such deployments, the 1522 must use the 4.9-GHz backhaul and the 1524PS must be in its own RAP tree and use the 5.8-GHz backhaul.
- In some parts of the world including the USA, you can only have public safety traffic on the 4.9-GHz backhaul. Check the destination countries compliance before installing.

The 4.9-GHz subband radio on the AP1524PS supports public safety channels within the 5-MHz (channels 1 to 10), 10-MHz (channels 11 to 19), and 20-MHz (channels 20 to 26) bandwidths.
- The following data rates are supported within the 5 MHz bandwidth: 1.5, 2.25, 3, 4.5, 6, 9, 12, and 13.5 Mbps. The default rate is 6 Mbps.
- The following data rates are supported within the 10-MHz bandwidth: 3, 4.5, 6, 9, 12, 18, 24, and 27 Mbps. The default rate is 12 Mbps.

Note
- Those AP1522s with serial numbers prior to FTX1150XXXX do not support 5 and 10 MHz channels on the 4.9-GHz radio; however, a 20-MHz channel is supported.
- Those AP1522s with serial numbers after FTX1150XXXX support 5, 10, and 20 MHz channels.

Enabling the 4.9-GHz Band

When you attempt to enable the 4.9-GHz band, you get a warning that the band is a licensed band in most parts of the world.
Chapter 10  Controlling Mesh Access Points

Adding Mesh Access Points to the Mesh Network

Figure 10-25  Public Safety Warning During Configuration

To verify that a public safety band is on the mesh access point using the CLI, enter this command:

```
show mesh public-safety
```

The following appears:

```
Global Public Safety status: enabled
```

To verify that a public safety band is on the mesh access point using the GUI:

Wireless > Access Points > 802.11a radio > Configure (from the Antenna drop-down list)

Configuring Interoperability with Cisco 3200

Cisco AP1522 and AP1524PS can interoperate with the Cisco 3200 on the public safety channel (4.9-GHz) as well as the 2.4-GHz access and 5.8-GHz backhaul.

The Cisco 3200 creates an *in-vehicle network* in which devices such as PCs, surveillance cameras, digital video recorders, printers, PDAs, and scanners can share wireless networks such as cellular or WLAN based services back to the main infrastructure. This feature allows data collected from in-vehicle deployments such as a police cars to be integrated into the overall wireless infrastructure.

This section provides configuration guidelines and step-by-step instructions for configuring interoperability between the Cisco 3200 and the AP1522 and the AP1524PS.

For specific interoperability details between series 1130, 1240, and 1520 (1522, 1524PS) mesh access points and Cisco 3200 see the table below.

<table>
<thead>
<tr>
<th>Mesh Access Point Model</th>
<th>Cisco 3200 Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP1552, AP1522, AP1524PS</td>
<td>c3201, c3202, c3205</td>
</tr>
<tr>
<td>1524SB, 1130, 1240, Indoor 802.11n mesh access points</td>
<td>c3201, c3205</td>
</tr>
</tbody>
</table>

1. Universal access must be enabled on the AP1522 if connecting to a Cisco 3200 on the 802.11a radio or 4.9-GHz band.
Adding Mesh Access Points to the Mesh Network

Configuration Guidelines for Public Safety 4.9-GHz Band

- Client access must be enabled on the backhaul (mesh global parameter). This feature is not supported on the AP1524PS.
- Public safety must be enabled globally on all mesh access points (MAPs) in the mesh network.
- The channel number assignment on the AP1522 or AP1524PS must match those on the Cisco 3200 radio interfaces:
  - Channels 20 (4950 GHz) through 26 (4980 GHz) and subband channels 1 through 19 (5 and 10 MHz) are used for Cisco 3200 interoperability. This configuration change is made on the controller. No changes are made to the mesh access point configuration.
  - Channel assignments are only made to the RAP. Updates to the MAP are propagated by the RAP.
- The default channel width for Cisco 3200s is 5 MHz. You must either change the channel width to 10 or 20 MHz to enable WGBs to associate with the AP1522 and AP1524PS or change the channel on the AP1522 or AP1524PS to a channel in the 5-MHz band (channels 1 to 10) or 10-MHz band (channels 11 to 19).
- Radio (802.11a) must be disabled when configuring channels and then reenabled when using the CLI. When using the GUI, enabling and disabling of the 802.11a radio for channel configuration is not required.
- Cisco 3200s can scan channels within but not across the 5, 10, or 20-MHz bands.

Enabling AP1522 to Associate with Cisco 3200 (GUI)

| Step 1 | To enable the backhaul for client access, choose Wireless > Mesh to access the Mesh page. |
| Step 2 | Select the Backhaul Client Access Enabled check box to allow wireless client association over the 802.11a radio. Click Apply. |
| Note   | You are prompted with a message to allow reboot of all the mesh access points to enable Backhaul Client Access on a network. Click OK. |
| Step 3 | To assign the channel to use for the backhaul (channels 20 through 26), click Wireless > Access Points > Radio and select 802.11a/n from the Radio subheading. A summary page for all 802.11a radios appears. |
| Step 4 | At the Antenna drop-down list for the appropriate RAP, select Configure. The Configure page appears. |

2. Model c3201 is a Cisco 3200 with an 802.11b/g radio (2.4-GHz).
3. Model c3202 is a Cisco 3200 with a 4-9-GHz subband radio.
4. Model c3205 is a Cisco 3200 with a 802.11a radio (5.8-GHz subband.)
Step 5 At the RF Channel Assignment section, choose the **WLC Controlled** option for the Assignment Method option and choose any channel between 1 and 26.

Step 6 Click **Apply** to commit your changes.

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

---

**Enabling 1522 and 1524PS Association with Cisco 3200 (CLI)**

Step 1 To enable client access mode on the AP1522, enter this command:

```
config mesh client-access enable
```

Step 2 To enable the public safety on a global basis, enter this command:

```
config mesh public-safety enable all
```

Step 3 To enable the public safety channels, enter these commands:

a. On the AP1522, enter these commands:

```
config 802.11a disable Cisco_MAP
config 802.11a channel ap Cisco_MAP channel number
config 802.11a enable Cisco_MAP
```

b. On the AP1524PS, enter these commands:

```
config 802.11–a49 disable Cisco_MAP
config 802.11–a49 channel ap Cisco_MAP channel number
config 802.11–a49 enable Cisco_MAP
```
Adding Mesh Access Points to the Mesh Network

Step 4 To save your changes, enter this command:

save config

Step 5 To verify your configuration, enter these commands:

show mesh public-safety
show mesh client-access
show ap config 802.11a summary (1522 only)
show ap config 802.11–a49 summary (1524PS only)

Note Enter the show config 802.11-a58 summary command to display configuration details for a 5.8-GHz radio.

Configuring Power and Channel Settings

The backhaul channel (802.11a/n) can be configured on a RAP. MAPs tune to the RAP channel. The local access can be configured independently for MAP.

Configuring Power and Channel Settings (GUI)

Step 1 Choose Wireless > Access Points > 802.11a/n.

The Access Points > 802.11a/n Radios page appears.

Figure 10-27 Access Points > 802.11a/n Radios Page

Note In Figure 10-27, radio slots are displayed for each radio. For an AP1524SB, the 802.11a radio will display for slots 1 and 2 that operate in the 5-GHz band. For an AP1524PS, the 802.11a radio will display for slots 1 and 2, operating in the 5-GHz and 4.9-GHz bands respectively.
Adding Mesh Access Points to the Mesh Network

**Step 2**
From the Antenna drop-down list for the 802.11a/n radio, choose **configure**. The Configure page appears.

**Note**
For the 1524SB, choose the Antenna drop-down list for a RAP with a radio role of downlink.

**Figure 10-28  802.11a/n Cisco APs > Configure Page**

**Step 3**
Assign a channel (assignment methods of AP Controlled and WLC Controlled) for the radio.

**Note**
When you assign a channel to the AP1524SB, choose the **WLC Controlled** assignment method, and select one of the supported channels for the 5-GHz band.

**Step 4**
Assign Tx power levels (AP Controlled and WLC Controlled) for the radio.

There are five selectable power levels for the 802.11a backhaul for AP1500s.

**Note**
The default Tx power level on the backhaul is the highest power level (Level 1).

**Note**
Radio Resource Management (RRM) is OFF (disabled) by default. RRM cannot be turned ON (enabled) for the backhaul.

**Step 5**
Click **Apply** when power and channel assignment are complete.

**Step 6**
From the 802.11a/n Radios page, verify that channel assignments were made correctly.
Configuring the Channels on the Serial Backhaul (CLI)

**Step 1** To configure the backhaul channel on the radio in slot 2 of the RAP, enter this command:

```
config slot 2 channel ap Cisco_RAPSB channel
```

The available channels for the 5.8-GHz band are 149, 153, 157, 161, and 165.

**Step 2** To configure the transmit power level on the radio in slot 2 of the RAP, enter this command:

```
config slot 2 txPower ap Cisco_RAPSB power
```

Valid values are 1 through 5; the default value is 1.

**Step 3** To display the configurations on the mesh access points, enter these commands:

- **show mesh path MAP**

  Information similar to the following appears:

  ```
  AP Name/Radio Channel Rate Link-Snr Flags State
  MAP1SB 161 auto 60 0x10ea9d54 UPDATED NEIGH PARENT BEACON
  RAPSB 153 auto 51 0x10ea9d54 UPDATED NEIGH PARENT BEACON
  ```

  RAPSB is a Root AP.

- **show mesh backhaul RAPSB**

  Information similar to the following appears:

  ```
  Current Backhaul Slot(s) ........................ 1, 2,
  ```

  **Basic Attributes for Slot 1**
  - Radio Type ................................... RADIO_TYPE_80211a
  - Radio Role .................................... ACCESS
  - Administrative State ........................ ADMIN_ENABLED
  - Operation State .............................. UP
  - Current Tx Power Level ...................... 1
  - Current Channel .............................. 165
  - Antenna Type .................................. EXTERNAL_ANTENNA
  - External Antenna Gain (in .5 dBm units)..... 0

  **Basic Attributes for Slot 2**
  - Radio Type ................................... RADIO_TYPE_80211a
  - Radio Role .................................... RADIO_DOWNLINK
  - Administrative State ........................ ADMIN_ENABLED
  - Operation State .............................. UP
  - Current Tx Power Level ...................... 3
  - Current Channel .............................. 153
Adding Mesh Access Points to the Mesh Network

Antenna Type......................... EXTERNAL_ANTENNA
External Antenna Gain (in .5 dBm units)..... 0

- `show ap channel MAP1SB`

  Information similar to the following appears:

  802.11b/g Current Channel ................. 11
  Slot Id ................................... 0
  Allowed Channel List....................... 1,2,3,4,5,6,7,8,9,10,11
  802.11a(5.8Ghz) Current Channel .......... 161
  Slot Id ................................... 1
  Allowed Channel List....................... 149,153,157,161,165
  802.11a(5.8Ghz) Current Channel .......... 153
  Slot Id ................................... 2
  Allowed Channel List....................... 149,153,157,161,165

Configuring Antenna Gain

You must configure the antenna gain for the mesh access point to match that of the antenna installed using the controller GUI or controller CLI.

Configuring Antenna Gain (GUI)

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Wireless &gt; Access Points &gt; Radio &gt; 802.11a/n to open the 802.11a/n Radios page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>For the mesh access point antenna you want to configure, hover the mouse over the blue arrow (far right) to display antenna options. Choose Configure.</td>
</tr>
</tbody>
</table>

Note: Only external antennas have configurable gain settings.

Figure 10-30 802.11a/n Radios Page

| Step 3 | In the Antenna Parameters section, enter the antenna gain. The gain is entered in 0.5 dBm units. For example, 2.5 dBm = 5. |

Note: The entered gain value must match that value specified by the vendor for that antenna.
Step 4  Click **Apply** and **Save Configuration** to save the changes.

**Configuring Antenna Gain (CLI)**

Enter this command to configure the antenna gain for the 802.11a backhaul radio using the controller CLI:

```
config 802.11a antenna extAntGain antenna_gain AP_name
```

where gain is entered in 0.5-dBm units (for example, 2.5 dBm = 5).

**Backhaul Channel Deselection on Serial Backhaul Access Point**

This feature is applicable to mesh APs with two 5-GHz radios, such as 1524SB (serial backhaul).

The backhaul channel deselection feature helps you to restrict the set of channels available to be assigned for the serial backhaul MAPs and RAPs. Because 1524SB MAP channels are automatically assigned, this feature helps in regulating the set of channels that get assigned to mesh access points. For example, if you do not want channel 165 to get assigned to any of the 1524SB mesh access points, you need to remove channel 165 from the DCA list and enable this feature.

When you remove certain channels from the DCA list and enable the **mesh backhaul dca-channel** command, those channels will not be assigned to any serial backhaul access points in any scenario. Even if a radar is detected on all channels within the DCA list channels, the radio will be shut down rather than moved to channels outside it. A trap message is sent to the WCS, and the message is displayed showing that the radio has been shut down because of DFS. You will not be able to assign channels to the serial backhaul RAP outside of the DCA list with the **config mesh backhaul dca-channels enable** command enabled. However, this is not case for the APs with one 5-GHz radio such as 1552, 1522, and 1524PS APs. For these APs, you can assign any channel outside of the DCA list for a RAP, and the controller/AP can also select a channel outside of the DCA list if no radar-free channel is available from the list.
Adding Mesh Access Points to the Mesh Network

This feature is best suited in an interoperability scenario with indoor mesh access points or workgroup bridges that support a channel set that is different from outdoor access points. For example, channel 165 is supported by outdoor access points but not by indoor access points in the -A domain. By enabling the backhaul channel deselection feature, you can restrict the channel assignment to only those channels that are common to both indoor and outdoor access points.

**Note** Channel deselection is applicable to 7.0 and later releases.

In some scenarios, there may be two linear tracks or roads for mobility side by side. Because channel selection of MAPs happens automatically, there can be a hop at a channel, which is not available on the autonomous side, or the channel has to be skipped when the same or adjacent channel is selected in a neighborhood access point that belongs to a different linear chain.

**Configuring Backhaul Channel Deselection (GUI)**

**Step 1** Choose **Controller > Wireless > 802.11a/n > RRM > DCA**.

The Dynamic Channel Assignment Algorithm page appears.

**Step 2** Select one or more channels to include in the DCA list.

The channels included in the DCA list will not be assigned to the access points associated to this controller during automatic channel assignment.

**Step 3** Choose **Wireless > Mesh**.

The Mesh page appears.

**Step 4** Select the Mesh DCA Channels check box to enable the backhaul channel deselection using the DCA list. This option is applicable for serial backhaul access points.

**Step 5** After you enable the backhaul deselection option, choose **Wireless > Access Points > Radios > 802.11a/n** to configure the channel for the RAP downlink radio.

**Step 6** From the list of access points, click on the Antenna drop-down list for a RAP and choose **Configure**.

The Configure page appears.

**Step 7** In the RF Backhaul Channel assignment section, choose **Custom**.

**Step 8** Select a channel for the RAP downlink radio from the drop-down list, which appears when you choose **Custom**.

**Step 9** Click **Apply** to apply and save the backhaul channel deselection configuration changes.

**Configuring Backhaul Channel Deselection (CLI)**

**Step 1** To review the channel list already configured in the DCA list, enter this command:

```
show advanced 802.11a channel
```

Information similar to the following appears:

```
Automatic Channel Assignment
   Channel Assignment Mode....................... AUTO
   Channel Update Interval......................... 600 seconds
   Anchor time (Hour of the day)........... 0
   Channel Update Contribution................ SNI
   CleanAir Event-driven RRM option........... Enabled
```
To add a channel to the DCA list, enter the `config advanced 802.11a channel add channel number` command, where `channel number` is the channel number that you want to add to the DCA list.

You can also delete a channel from the DCA list by entering the `config advanced 802.11a channel delete channel number` command, where `channel number` is the channel number that you want to delete from the DCA list.

Before you add or delete a channel to or from the DCA list, ensure that the 802.11a network is disabled.

- To disable the 802.11a network, enter this command:
  ```
  config 802.11a disable network
  ```

- To enable the 802.11a network, enter this command:
  ```
  config 802.11a enable network
  ```

You cannot directly delete a channel from the DCA list if it is assigned to any 1524 RAP. To delete a channel assigned to a RAP, you must first change the channel assigned to the RAP and then enter the `config advanced 802.11a channel delete channel number` command from the controller.

The following is a sample output of the `add channel` and `delete channel` commands:

```
(Controller) > config 802.11a disable network
Disabling the 802.11a network may strand mesh APs. Are you sure you want to continue? (y/n)y

(Controller) > config advanced 802.11a channel add 132

(Controller) > config advanced 802.11a channel delete 116
```
Failed to delete channel.
Reason: Channel 116 is configured for one of the Serial Backhaul RAPs.
Disable mesh backhaul dca-channels or configure a different channel for Serial Backhaul RAPs.

(Controller) > config advanced 802.11a channel delete 132

802.11a 5 GHz Auto-RF:
Allowed Channel List......................... 36,40,44,48,52,56,60,64,116,132,140
DCA channels for Serial Backhaul Mesh APs is enabled.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul Mesh APs.
Otherwise, the Serial Backhaul Mesh APs can get stranded.
Are you sure you want to continue? (y/N)y

(Controller) > config 802.11a enable network

Step 3
After a suitable DCA list has been created, enter the config mesh backhaul dca-channels enable command to enable the backhaul channel deselection feature for mesh access points.
You can enter the config mesh backhaul dca-channels disable command if you want to disable the backhaul channel deselection feature for mesh access points.
It is not required that you disable 802.11a network to enable or disable this feature.

Information similar to the following appears:

(Controller) > config mesh backhaul dca-channels enable
802.11a 5 GHz Auto-RF:
  Allowed Channel List......................... 36,40,44,48,52,56,60,64,116,140
Enabling DCA channels for c1524 mesh APs will limit the channel set to the DCA channel list.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul Mesh APs.
Otherwise, the Serial Backhaul Mesh APs can get stranded.
Are you sure you want to continue? (y/N)y

(Controller) > config mesh backhaul dca-channels disable

Step 4
To check the current status of the backhaul channel deselection feature, enter the show mesh config command.

Information similar to the following appears:

(Controller) > show mesh config

Mesh Range........................................ 12000
Mesh Statistics update period.................... 3 minutes
Backhaul with client access status............. enabled
Background Scanning State..................... enabled
Backhaul Amsdu State............................ disabled

Mesh Security
  Security Mode..................................... PSK
  External-Auth.................................... enabled
  Radius Server 1................................. 209.165.200.240
  Use MAC Filter in External AAA server........ disabled
  Force External Authentication............... disabled

Mesh Alarm Criteria
  Max Hop Count................................. 4
  Recommended Max Children for MAP........... 10
Step 5  Enter the `config slot slot number channel ap ap-name channel number` command to assign a particular channel to the 1524 RAP downlink radio.

- *slot number* refers to the slot of the downlink radio to which the channel is assigned.
- *ap-name* refers to the name of the access point on which the channel is configured.
- *channel number* refers to the channel that is assigned to a slot on the access point.

Slot 2 of the 1524 RAP acts as a downlink radio. If backhaul channel deselection is enabled, you can assign only those channels that are available in the DCA list the access point.

The following is a sample output:

```
(Controller) > config slot 2 channel ap Controller-RAP2-1524 136
Mesh backhaul dca-channels is enabled. Choose a channel from the DCA list.
(Controller) > config slot 2 channel ap Controller-RAP2-1524 140
```

**Backhaul Channel Deselection Guidelines**

- Channels for serial backhaul RAP 11a access radio and both 11a radios of serial backhaul MAPs are assigned automatically. You cannot configure these channels.

- Look out for trap logs on the controller. In case of radar detection and subsequent channel change, messages similar to the following appear:

  Channel changed for Base Radio MAC: 00:1e:bd:19:7b:00 on 802.11a radio. Old channel: 132. New Channel: 116. Why: Radar. Energy before/after change: 0/0. Noise before/after change: 0/0. Interference before/after change: 0/0.

  Radar signals have been detected on channel 132 by 802.11a radio with MAC: 00:1e:bd:19:7b:00 and slot 2

- For every serial backhaul AP, channels on downlink and uplink radios should always be noninterfering (for example, if the uplink is channel 104, the 100, 104, and 108 channels cannot be assigned for a downlink radio on that AP). An alternate adjacent channel is also selected for an 11a access radio on RAP.

- If radar signals are detected on all channels except the uplink radio channel, the downlink radio will be shut down and the uplink radio will act as both an uplink and a downlink (that is, the behavior is similar to 1522 APs in this case).
Adding Mesh Access Points to the Mesh Network

- Radar detection is cleared after 30 minutes. Any radio that is shut down because of radar detection should be back up and operational after this duration.
- There is a 60-second silent period immediately after moving to a DFS-enabled channel (irrespective of whether the channel change is because of radar detection or user configured in case of a RAP) during which the AP scans for radar signals without transmitting anything. A small period (60 seconds) of downtime may occur because of radar detection, if the new channel is also DFS-enabled. If radar detection occurs again on the new channel during the silent period, the parent changes its channel without informing the child AP because it is not allowed to transmit during the silent period. In this case, the child AP dissociates and goes back to scan mode, rediscovers the parent on the new channel and then joins back, which causes a slightly longer (approximately 3 minutes) downtime.
- For a RAP, the channel for the downlink radio is always selected from within the DCA list, irrespective of whether the backhaul channel deselection feature is enabled or not. The behavior is different for a MAP because the MAP can pick any channel that is allowed for that domain, unless the backhaul channel deselection feature is enabled. We recommend that you have quite a few channels added to the 802.11a DCA channel list to prevent any radios getting shut down because of a lack of channels even if the backhaul channel deselection feature is not in use.
- Because the DCA list that was used for the RRM feature is also used for mesh APs through the backhaul channel deselection feature, keep in mind that any addition or deletion of channels from the DCA list will affect the channel list input to the RRM feature for nonmesh access points as well. RRM is off for mesh.
- For -M domain APs, a slightly longer time interval (25 to 50 percent more time than usual) may be required for the mesh network to come up because there is a longer list of DFS-enabled channels in the -M domain, which each AP scans before joining the parent.

Configuring Dynamic Channel Assignment (GUI)

Using the controller GUI, follow these steps to specify the channels that the dynamic channel assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning. This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

**Note**
The steps outlined in this section are only relevant to mesh networks.

**Step 1**
To disable the 802.11a/n or 802.11b/g/n network, follow these steps:

a. Choose **Wireless > 802.11a/n or 802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Deselect the **802.11a (or 802.11b/g) Network Status** check box.

c. Click **Apply** to commit your changes.

**Step 2**
Choose **Wireless > 802.11a/n or 802.11b/g/n > RRM > DCA** to open the 802.11a (or 802.11b/g) > RRM > Dynamic Channel Assignment (DCA) page.
Step 3  Choose one of the following options from the Channel Assignment Method drop-down list to specify the controller’s DCA mode:

- **Automatic**—Causes the controller to periodically evaluate and, if necessary, update the channel assignment for all joined mesh access points. This is the default value.

- **Freeze**—Causes the controller to evaluate and update the channel assignment for all joined mesh access points, if necessary, but only when you click **Invoke Channel Update Once**.

  **Note**  The controller does not evaluate and update the channel assignment immediately after you click **Invoke Channel Update Once**. It waits for the next interval to elapse.

- **OFF**—Turns off DCA and sets all mesh access point radios to the first channel of the band, which is the default value. If you choose this option, you must manually assign channels on all radios.

Step 4  From the Interval drop-down list, choose one of the following options to specify how often the DCA algorithm is allowed to run: 10 minutes, 1 hour, 2 hours, 3 hours, 4 hours, 6 hours, 8 hours, 12 hours, or 24 hours. The default value is 10 minutes.
Step 5  From the AnchorTime drop-down list, choose a number to specify the time of day when the DCA algorithm is to start. The options are numbers between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.

Step 6  Select the Avoid Foreign AP Interference check box to cause the controller’s RRM algorithms to consider 802.11 traffic from foreign access points (those access points not included in your wireless network) when assigning channels to lightweight access points, or deselect it to disable this feature. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign access points. The default value is checked.

Step 7  Select the Avoid Cisco AP Load check box to cause the controller’s RRM algorithms to consider 802.11 traffic from Cisco lightweight access points in your wireless network when assigning channels, or deselect it to disable this feature. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load. The default value is deselected.

Step 8  Select the Avoid Non-802.11a (802.11b) Noise check box to cause the controller’s RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight access points, or deselect it to disable this feature. For example, RRM may have access points avoid channels with significant interference from nonaccess point sources, such as microwave ovens. The default value is checked.

Step 9  From the DCA Channel Sensitivity drop-down list, choose one of the following options to specify how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channels:

- **Low**—The DCA algorithm is not particularly sensitive to environmental changes.
- **Medium**—The DCA algorithm is moderately sensitive to environmental changes.
- **High**—The DCA algorithm is highly sensitive to environmental changes.

The default value is **Medium**. The DCA sensitivity thresholds vary by radio band, as noted in Table 10-9.

Table 10-9  DCA Sensitivity Thresholds

<table>
<thead>
<tr>
<th>Option</th>
<th>2.4-GHz DCA Sensitivity Threshold</th>
<th>5-GHz DCA Sensitivity Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>5 dB</td>
<td>5 dB</td>
</tr>
<tr>
<td>Medium</td>
<td>10 dB</td>
<td>15 dB</td>
</tr>
<tr>
<td>Low</td>
<td>20 dB</td>
<td>20 dB</td>
</tr>
</tbody>
</table>

Step 10 For 802.11a/n networks only, choose one of the following Channel Width options to specify the channel bandwidth supported for all 802.11n radios in the 5-GHz band:

- **20 MHz**—The 20-MHz channel bandwidth (default)

**Note**  To override the globally configured DCA channel width setting, you can statically configure an access point’s radio for 20-MHz mode on the 802.11a/n Cisco APs > Configure page. If you ever change the static RF channel assignment method to WLC Controlled on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

This page also shows the following nonconfigurable channel parameter settings:

- **Channel Assignment Leader**—The MAC address of the RF group leader, which is responsible for channel assignment.
- **Last Auto Channel Assignment**—The last time RRM evaluated the current channel assignments.
**Step 11** In the DCA Channel List section, the DCA Channels field shows the channels that are currently selected. To choose a channel, select its check box in the Select column. To exclude a channel, deselect its check box.

Range:
- 802.11b/g—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

Default:
- 802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161
- 802.11b/g—1, 6, 11

**Note** These extended UNII-2 channels in the 802.11a band do not appear in the channel list: 100, 104, 108, 112, 116, 132, 136, and 140. If you have Cisco Aironet 1500 series mesh access points in the -E regulatory domain, you must include these channels in the DCA channel list before you start operation. If you are upgrading from a previous release, verify that these channels are included in the DCA channel list. To include these channels in the channel list, select the Extended UNII-2 Channels check box.

**Step 12** If you are using AP1500s in your network, you must set the 4.9-GHz channels in the 802.11a band on which they are to operate. The 4.9-GHz band is for public safety client access traffic only. To choose a 4.9-GHz channel, select its check box in the Select column. To exclude a channel, deselect its check box.

Range:
- 802.11a—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26

Default:
- 802.11a—20, 26

**Step 13** Click **Apply** to commit your changes.

**Step 14** To reenable the 802.11a or 802.11b/g network, follow these steps:

a. Click **Wireless > 802.11a/n or 802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Select the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

**Step 15** Click **Save Configuration** to save your changes.

To see why the DCA algorithm changed channels, click **Monitor** and then **View All** under Most Recent Traps. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change.

---

**Configuring Advanced Features**

This section includes the following topics:

- Using the 2.4-GHz Radio for Backhaul, page 10-64
Using the 2.4-GHz Radio for Backhaul

Until the 7.0 release, mesh used the 5-GHz radio for backhaul, and the 2.4-GHz radio was used only for client access. The reasons for using only the 5-GHz radio for backhaul are as follows:

- More channels are available
- More EIRP is available
- Less interference occurs
- Most of the client access occurs over the 2.4-GHz band

However, under certain conditions, such as dense foliage areas, you might have needed to use the 2.4-GHz band for a backhaul because it has better penetration.

With the 7.0.116.0 release, you can configure an entire mesh network to use a single backhaul that can be either 5 GHz or 2.4 GHz.

Caution
This feature is available only for AP1522 (two radios). This feature should be used only after exploring the 5-GHz backhaul option.

Caution
We recommend that you use 5 GHz as the first option and use 2.4 GHz only if the 5-GHz option does not work.

Changing the Backhaul from 5 GHz to 2.4 GHz

When you specify only the RAP name as an argument to the command, the whole mesh sector changes to 2.4 GHz or 5 GHz backhaul. The warning messages indicate the change in backhaul, whether it is from 2.4 GHz to 5 GHz or vice versa.

Note
The 2.4-GHz backhaul cannot be configured using the controller user interface, but only through the CLI.

Step 1
To change the backhaul, enter this command:

```
cfg mesh backhaul slot 0 enable RAP
```
A message similar to the following appears:

Warning! Changing backhaul slot will bring down the mesh for renegotiation!!!
After backhaul is changed, 5 GHz client access channels need to be changed manually
Are you sure you want to continue? (y/N)

Step 2 Press y.

Note When you change the 5-GHz backhaul to local client access, the 5-GHz client access frequencies on all the APs are the same, because the backhaul frequency is ported on these 5-GHz radios for client access. You need to configure these channels for a better frequency planning.

Changing the Backhaul from 2.4 GHz to 5 GHz

Step 1 To change the backhaul, enter the following command:

```config mesh backhaul slot 1 enable RAP```

A message similar to the following appears:

Warning! Changing backhaul slot will bring down the mesh for renegotiation!!!
Are you sure you want to continue? (y/N)

Step 2 Press y.

Note You cannot configure the 2.4-GHz backhaul using the controller GUI, but you can configure the 2.4-GHz backhaul using the CLI.

Verifying the Current Backhaul in Use

To verify the current backhaul in use, enter the command:

``show mesh backhaul AP_name``

Note For a 5-GHz backhaul, dynamic frequency selection (DFS) occurs only on 5 GHz and not on 2.4 GHz. The mechanism, which differs for RAP and MAP, is called a coordinated change mechanism.

When 5 GHz is converted to client access from the backhaul or 2.4 GHz is being used as backhaul, DFS works similar to how it works for a local mode AP. DFS is detected on a 5-GHz client access, and the request is sent to the controller for a new channel. Mesh adjacency is not affected for the 2.4-GHz backhaul.

Note Universal client access is available on the 2.4-GHz backhaul.
Universal Client Access

When Universal Client Access is enabled, it allows wireless client association over the backhaul radio. Generally, backhaul radio is a 5-GHz radio for most of the mesh access points except for 1522 where backhaul can be 2.4 GHz. This means that a backhaul radio can carry both backhaul traffic and client traffic.

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

Note
Universal Client Access is disabled by default.

After this feature is enabled, all mesh access points reboot.

This feature is applicable to mesh access points with two or more radios (1552, 1524SB, 1522, Indoor APs in mesh mode) excluding the 1524PS.

Configuring Universal Client Access (GUI)

You will be prompted that the AP will reboot if you enable Universal Client Access.

Figure 10-33 Configuring Universal Client Access Using the GUI

Configuring Universal Client Access (CLI)

Use the following command to enable Universal Client Access:

```
config mesh client-access enable
```
A message similar to the following appears:

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

Universal Client Access on Serial Backhaul Access Points

With universal client access, you can have client access on the backhaul 802.11a radios in addition to the backhaul functionality. This feature is applicable to mesh access points with two or more radios (1552, 1524SB, 1522, Indoor APs in mesh mode) excluding the 1524PS.

The dual 5-GHz Universal Client Access feature is intended for the serial backhaul access point platform, which has three radio slots. The radio in slot 0 operates in the 2.4-GHz band and is used for client access. The radios in slot 1 and slot 2 operate in the 5-GHz band and are primarily used for backhaul. However, with the Universal Client Access feature, clients were allowed to associate over the slot 1 radio. But slot 2 radio was used only for backhaul. With the 7.0 release, client access over the slot 2 radio is allowed with this Dual 5-GHz Universal Access feature.

By default, client access is disabled over both the backhaul radios. Follow the guidelines to enable or disable client access on the radio slots that constitute 5-GHz radios, irrespective of the radios being used as downlinks or uplinks:

- You can enable client access on slot 1 even if client access on slot 2 is disabled.
- You can enable client access on slot 2 only when client access on slot 1 is enabled.
- If you disable client access on slot 1, client access on slot 2 is automatically disabled on the CLI.
- To disable only the extended client access (on the slot 2 radio), use the GUI.
- All the mesh access points reboot whenever client access is enabled or disabled.

The two 802.11a backhaul radios use the same MAC address. There may be instances where a WLAN maps to the same BSSID on more than one slot. Client access on the slot 2 radio is referred to as Extended Universal Access (EUA) in this document.

You can configure Extended Universal Access using one of the following methods:

- Configuring Extended Universal Access (GUI), page 10-67
- Configuring Extended Universal Access (CLI), page 10-70
- Configuring Extended Universal Access from the Wireless Control System (WCS), page 10-71

Configuring Extended Universal Access (GUI)

**Step 1** Choose Controller > Wireless > Mesh.

The Controller GUI when Backhaul Client Access is disabled page appears.
Step 2  Select the **Backhaul Client Access** check box to display the Extended Backhaul Client Access check box.

Step 3  Select the **Extended Backhaul Client Access** check box and click **Apply**.

Step 4  Click **OK**.

**Post-Configuration**

After EUA is enabled, 802.11a radios are displayed.
Slot 2 in the 5-GHz radio in the RAPS (serial backhaul) that is used to extend the backhaul in the DOWNLINK direction is displayed as DOWNLINK ACCESS, where slot 1 in the 5-GHz radio in the RAPS that is used for client access is displayed as ACCESS. Slot 2 in the 5-GHz radio in the MAPS that is used for the UPLINK is displayed as UPLINK ACCESS, and slot 1 in the MAPS is used for the DOWNLINK ACCESS with an omnidirectional antenna that also provides the client access.

Create WLAN on the WLC with the appropriate SSID mapped to the correct interface (VLAN). After you create a WLAN, it is applied to all the radios by default. If you want to enable client access only on 802.11a radios, choose only the appropriate radio policy from the list.
Figure 10-37 Radio Policy Selection

Configuring Extended Universal Access (CLI)

- Go to the Controller prompt and enter the `config mesh client-access enable extended` command.

A message similar to the following appears:

Enabling client access on both backhaul slots
Same BSSIDs will be used on both slots
All Mesh Serial Backhaul APs will be rebooted
Are you sure you want to start? (y/N)

- Enter the `show mesh client-access` command to know the status of the backhaul with client access and the backhaul with client access extended.

A message similar to the following appears:

Backhaul with client access status: enabled
Backhaul with client access extended status(3 radio AP): enabled

- There is no explicit command to disable client access only on slot 2 (EUA). You have to disable client access on both the backhaul slots by entering this command:

`config mesh client-access disable`

A message similar to the following appears:

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

- You can disable EUA from the GUI without disturbing client access on the slot 1 radio, but all 1524SB access points will be rebooted.

It is possible to enable client access only on slot 1 and not on slot 2 by entering this command:

`config mesh client-access enable`

A message similar to the following appears:

All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
Configuring Extended Universal Access from the Wireless Control System (WCS)

Step 1  Choose Controllers > Controller IP Address > Mesh > Mesh Settings.

The WCS Mesh page when Backhaul Client Access is disabled.

Step 2  Select the Client Access on Backhaul Link check box to display the Extended Backhaul Client Access check box.

Step 3  Select the Extended Backhaul Client Access check box and click Apply. A message appears indicating the possible results of enabling the Extended Backhaul Client Access.

Step 4  Click OK to continue.

Configuring Ethernet VLAN Tagging

Ethernet VLAN tagging allows specific application traffic to be segmented within a wireless mesh network and then forwarded (bridged) to a wired LAN (access mode) or bridged to another wireless mesh network (trunk mode).

A typical public safety access application that uses Ethernet VLAN tagging is the placement of video surveillance cameras at various outdoor locations within a city. Each of these video cameras has a wired connection to a MAP. The video of all these cameras is then streamed across the wireless backhaul to a central command station on a wired network.
Ethernet VLAN tagging allows Ethernet ports to be configured as normal, access, or trunk in both indoor and outdoor implementations:

- **Normal mode**—In this mode, the Ethernet port does not accept or send any tagged packets. Tagged frames from clients are dropped.

  Use the normal mode in applications when only a single VLAN is in use or there is no need to segment traffic in the network across multiple VLANs.

- **Note** When VLAN Transparent is disabled, the default Ethernet port mode is normal. VLAN Transparent must be disabled for VLAN tagging to operate and to allow configuration of Ethernet ports. To disable VLAN Transparent, which is a global parameter, see the “Configuring Global Mesh Parameters” section on page 10-31.
• **Access Mode**—In this mode, only untagged packets are accepted. All incoming packets are tagged with user-configured VLANs called access-VLANs.

  Use the access mode for applications in which information is collected from devices connected to the MAP, such as cameras or PCs, and then forwarded to the RAP. The RAP then applies tags and forwards traffic to a switch on the wired network.

• **Trunk mode**—This mode requires the user to configure a native VLAN and an allowed VLAN list (no defaults). In this mode, both tagged and untagged packets are accepted. Untagged packets are accepted and are tagged with the user-specified native VLAN. Tagged packets are accepted if they are tagged with a VLAN in the allowed VLAN list.

  Use the trunk mode for bridging applications such as forwarding traffic between two MAPs that reside on separate buildings within a campus.

Ethernet VLAN tagging operates on Ethernet ports that are not used as backhauls.

---

**Note**

In the controller releases prior to 7.2, the Root Access Point (RAP) native VLAN is forwarded out of Mesh Access Point (MAP) Ethernet ports with Mesh Ethernet Bridging and VLAN Transparent enabled.

In the 7.2 and later controller releases, the Root Access Point (RAP) native VLAN is not forwarded out of Mesh Access Point (MAP) Ethernet ports with Mesh Ethernet Bridging and VLAN Transparent enabled.

This change in behavior increases reliability and minimizes the possibility of forwarding loops on Mesh Backhauls.

### Ethernet VLAN Tagging Guidelines

- For security reasons, the Ethernet port on a mesh access point (RAP and MAP) is disabled by default. It is enabled by configuring Ethernet bridging on the mesh access point port.

- Ethernet bridging must be enabled on all the mesh access points in the mesh network to allow Ethernet VLAN tagging to operate.

- VLAN mode must be set as non-VLAN transparent (global mesh parameter). See the “Configuring Global Mesh Parameters (CLI)” section on page 10-36. VLAN transparent is enabled by default. To set as non-VLAN transparent, you must deselect the VLAN transparent option in the global mesh parameters page.
VLAN tagging can only be configured on Ethernet interfaces as follows:

- On AP1500s, three of the four ports can be used as secondary Ethernet interfaces: port 0-PoE in, port 1-PoE out, and port 3-fiber. Port 2-cable cannot be configured as a secondary Ethernet interface.

- In Ethernet VLAN tagging, port 0-PoE in on the RAP is used to connect to the trunk port of the switch of the wired network. Port 1-PoE out on the MAP is used to connect to external devices such as video cameras.

- Backhaul interfaces (802.11a radios) act as primary Ethernet interfaces. Backhauls function as trunks in the network and carry all VLAN traffic between the wireless and wired network. No configuration of primary Ethernet interfaces is required.

- For indoor mesh networks, the VLAN tagging feature functions as it does for outdoor mesh networks. Any access port that is not acting as a backhaul is secondary and can be used for VLAN tagging.

- VLAN tagging cannot be implemented on RAPs because the RAPs do not have a secondary Ethernet port, and the primary port is used as a backhaul. However, VLAN tagging can be enabled on MAPs with a single Ethernet port because the Ethernet port on a MAP does not function as a backhaul and is therefore a secondary port.

- No configuration changes are applied to any Ethernet interface acting as a backhaul. A warning displays if you attempt to modify the backhaul’s configuration. The configuration is only applied after the interface is no longer acting as a backhaul.
Figure 10-41 Warning Message Displays for Backhaul Configuration Attempts

- No configuration is required to support VLAN tagging on any 802.11a backhaul Ethernet interface within the mesh network as follows:
  - This includes the RAP uplink Ethernet port. The required configuration occurs automatically using a registration mechanism.
  - Any configuration changes to an 802.11a Ethernet link acting as a backhaul are ignored and a warning results. When the Ethernet link no longer functions as a backhaul, the modified configuration is applied.

- VLAN configuration is not allowed on port-02-cable modem port of AP1500s (wherever applicable). VLANs can be configured on ports 0 (PoE-in), 1 (PoE-out), and 3 (fiber).

- Up to 16 VLANs are supported on each sector. The cumulative number of VLANs supported by a RAP’s children (MAP) cannot exceed 16.

- The switch port connected to the RAP must be a trunk:
  - The trunk port on the switch and the RAP trunk port must match.
  - The RAP must always connect to the native VLAN ID 1 on a switch. The RAP’s primary Ethernet interface is by default the native VLAN of 1.
  - The switch port in the wired network that is attached to the RAP (port 0–PoE in) must be configured to accept tagged packets on its trunk port. The RAP forwards all tagged packets received from the mesh network to the wired network.
  - No VLANs, other than those destined for the mesh sector, should be configured on the switch trunk port.

- A configured VLAN on a MAP Ethernet port cannot function as a Management VLAN.

- Configuration is effective only when a mesh access point is in the CAPWAP RUN state and VLAN-Transparent mode is disabled.

- Whenever there roaming or a CAPWAP restart, an attempt is made to apply configuration again.
VLAN Registration

To support a VLAN on a mesh access point, all the uplink mesh access points must also support the same VLAN to allow segregation of traffic that belongs to different VLANs. The activity by which a mesh access point communicates its requirements for a VLAN and gets response from a parent is known as VLAN registration.

Note VLAN registration occurs automatically. No user intervention is required.

VLAN registration is summarized below:

1. Whenever an Ethernet port on a mesh access point is configured with a VLAN, the port requests its parent to support that VLAN.
2. If the parent is able to support the request, it creates a bridge group for the VLAN and propagates the request to its parent. This propagation continues until the RAP is reached.
3. When the request reaches the RAP, it checks whether it is able to support the VLAN request. If yes, the RAP creates a bridge group and a subinterface on its uplink Ethernet interface to support the VLAN request.
4. If the mesh access point is not able to support the VLAN request by its child, at any point, the mesh access point replies with a negative response. This response is propagated to downstream mesh access points until the mesh access point that requested the VLAN is reached.
5. Upon receiving negative response from its parent, the requesting mesh access point defers the configuration of the VLAN. However, the configuration is stored for future attempts. Given the dynamic nature of mesh, another parent and its uplink mesh access points might be able to support it in the case of roaming or a CAPWAP reconnect.

Enabling Ethernet VLAN Tagging (GUI)

You must enable Ethernet bridging before you can configure VLAN tagging. See the “Configuring Ethernet Bridging” procedure on page 10-43.

Step 1 After enabling Ethernet bridging, choose Wireless > All APs.
Step 2 Click the AP name link of the mesh access point on which you want to enable VLAN tagging.
Step 3 On the details page, select the Mesh tab.
Step 4  Select the Ethernet Bridging check box to enable the feature and click Apply.

An Ethernet Bridging section appears at the bottom of the page listing each of the four Ethernet ports of the mesh access point.

- If configuring a MAP access port, click, for example, gigabitEthernet1 (port 1-PoE out).
  a. Choose access from the mode drop-down list.
  b. Enter a VLAN ID. The VLAN ID can be any value between 1 and 4095.
  c. Click Apply.

**Note**  VLAN ID 1 is not reserved as the default VLAN.

**Note**  A maximum of 16 VLANs are supported across all of a RAP’s subordinate MAP.

- If configuring a RAP or MAP trunk port, click gigabitEthernet0 (port 0-PoE in).
a. From the mode drop-down list, choose **trunk**. (See Figure 10-44.)

b. Specify a native VLAN ID for incoming traffic. The native VLAN ID can be any value between 1 and 4095. Do not assign any value assigned to a user-VLAN (access).

c. Click **Apply**.

A trunk VLAN ID field and a summary of configured VLANs appears at the bottom of the screen. The trunk VLAN ID field is for outgoing packets.

d. Specify a trunk VLAN ID for outgoing packets:

   If forwarding untagged packets, do not change the default trunk VLAN ID value of zero. (MAP-to-MAP bridging, campus environment)

   If forwarding tagged packets, enter a VLAN ID (1 to 4095) that is not already assigned. (RAP to switch on wired network).

e. Click **Add** to add the trunk VLAN ID to the allowed VLAN list. The newly added VLAN displays under the Configured VLANs section on the page.

   **Note** To remove a VLAN from the list, select the Remove option from the arrow drop-down list to the right of the desired VLAN.

![Figure 10-44 All APs > AP > VLAN Mappings Page](image)

**Step 5** Click **Apply**.

**Step 6** Click **Save Configuration** to save your changes.

### Configuring Ethernet VLAN Tagging (CLI)

To configure a MAP access port, enter this command:

```
config ap ethernet 1 mode access enable AP1500-MAP 50
```

where **AP1500-MAP** is the variable **AP_name** and **50** is the variable **access_vlan ID**

To configure a RAP or MAP trunk port, enter this command:

```
config ap ethernet 0 mode trunk enable AP1500-MAP 60
```

where **AP1500-MAP** is the variable **AP_name** and **60** is the variable **native_vlan ID**

To add a VLAN to the VLAN allowed list of the native VLAN, enter this command:

```
config ap ethernet 0 mode trunk add AP1500-MAP3 65
```
where AP1500-MAP 3 is the variable AP_name and 65 is the variable VLAN ID

**Viewing Ethernet VLAN Tagging Configuration Details (CLI)**

To view VLAN configuration details for Ethernet interfaces on a specific mesh access point (AP Name) or all mesh access points (summary), enter one of these commands:

```
<Cisco Controller> >show ap config ethernet
sumary         For all APs
<AP Name>      For specific AP
<Cisco Controller> >show ap config ethernet AP-23

Vlan Tagging Information For AP AP-23
  Ethernet 0
    Mode: TRUNK
    Native Vlan 80
    Allowed Vlans: 81 83
  Ethernet 1
    Mode: ACCESS
    Access Vlan 88
  Ethernet 2
    Mode: NORMAL
  Ethernet 3
    Mode: TRUNK
    Native Vlan 83
    Allowed Vlans: 81 87 89
```

To see if VLAN transparent mode is enabled or disabled, enter the following command:
Workgroup Bridge Interoperability with Mesh Infrastructure

A workgroup bridge (WGB) is a small standalone unit that can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB is associated with the root AP through the wireless interface, which means that wired clients get access to the wireless network.

A WGB is used to connect wired networks over a single wireless segment by informing the mesh access point of all the clients that the WGB has on its wired segment via IAPP messages. The data packets for WGB clients contain an additional MAC address in the 802.11 header (4 MAC headers, versus the normal 3 MAC data headers). The additional MAC in the header is the address of the WGB itself. This additional MAC address is used to route the packet to and from the clients.

WGB association is supported on all radios of every mesh access point.
In the current architecture, while an autonomous AP functions as a workgroup bridge, only one radio interface is used for controller connectivity, Ethernet interface for wired client connectivity, and other radio interface for wireless client connectivity. dot11radio 1 (5 GHz) can be used to connect to a controller (using the mesh infrastructure) and Ethernet interface for wired clients. dot11radio 0 (2.4 GHz) can be used for wireless client connectivity. Depending on the requirement, dot11radio 1 or dot11radio 0 can be used for client association or controller connectivity.

With the 7.0 release, a wireless client on the second radio of the WGB is not dissociated by the WGB upon losing its uplink to a wireless infrastructure or in a roaming scenario.

With two radios, one radio can be used for client access and the other radio can be used for accessing the access points. Having two independent radios performing two independent functions provides you better control and lowers the latency. Also, wireless clients on the second radio for the WGB do not get disassociated by the WGB when an uplink is lost or in a roaming scenario. One radio has to be configured as a Root AP (radio role) and the second radio has to be configured as a WGB (radio role).

**Note**

If one radio is configured as a WGB, then the second radio cannot be a WGB or a repeater.

The following features are not supported for use with a WGB:

- FlexConnect
- Idle timeout
- Web authentication—If a WGB associates to a web-authentication WLAN, the WGB is added to the exclusion list, and all of the WGB-wired clients are deleted (web-authentication WLAN is another name for a guest WLAN).
- For wired clients behind the WGB, MAC filtering, link tests, and idle timeout
Configuring Workgroup Bridges

A workgroup bridge (WGB) is used to connect wired networks over a single wireless segment by informing the mesh access point of all the clients that the WGB has on its wired segment via IAPP messages. In addition to the IAPP control messages, the data packets for WGB clients contain an extra MAC address in the 802.11 header (4 MAC headers, versus the normal 3 MAC data headers). The extra MAC in the header is the address of the workgroup bridge itself. This extra MAC address is used to route the packet to and from the clients.

WGB association is supported on both the 2.4-GHz (802.11b/g) and 5-GHz (802.11a) radios on the AP1522, and the 2.4-GHz (802.11b) and 4.9-GHz (public safety) radios on the AP1524PS.

Supported platforms are autonomous WGBs AP1130, AP1140, AP1240, AP1310, and the Cisco 3200 Mobile Router (hereafter referred to as Cisco 3200) which are configured as WGBs can associate with a mesh access point. See the “Cisco Workgroup Bridges” section in Chapter 7 of the Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0 for configuration steps at [http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html](http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html)

Supported Workgroup Bridge Modes and Capacities

The supported WGB modes and capacities are as follows:

- The autonomous access points configured as WGBs must be running Cisco IOS release 12.4.25d-JA or later.

  **Note** If your mesh access point has two radios, you can only configure workgroup bridge mode on one of the radios. We recommend that you disable the second radio. Workgroup bridge mode is not supported on access points with three radios such as the AP1524SB.

- Client mode WGB (BSS) is supported; however, infrastructure WGB is not supported. The client mode WGB is not able to trunk VLAN as in an infrastructure WGB.

- Multicast traffic is not reliably transmitted to WGB because no ACKs are returned by the client. Multicast traffic is unicast to infrastructure WGB, and ACKs are received back.

- If one radio is configured as a WGB in a Cisco IOS access point, then the second radio cannot be a WGB or a repeater.

- Mesh access points can support up to 200 clients including wireless clients, WGB, and wired clients behind the associated WGB.

- Non-Cisco workgroup bridges are supported on Mesh access points.

- A WGB cannot associate with mesh access points if the WLAN is configured with WPA1 (TKIP) +WPA2 (AES), and the corresponding WGB interface is configured with only one of these encryptions (either WPA1 or WPA2):
  - Figure 10-46 displays WPA security settings for WGB (controller GUI).
  - Figure 10-47 displays WPA-2 security settings for WGB (controller GUI).
To view the status of a WGB client, follow these steps:

**Step 1**  Choose **Monitor > Clients** to open the client summary page.

**Step 2**  On the client summary page, click on the MAC address of the client or search for the client using its MAC address.

**Step 3**  In the page that appears, note that the client type is identified as a WGB (far right).

**Step 4**  Click on the MAC address of the client to view configuration details:

- For a wireless client, the page seen in Figure 10-49 appears.
- For a wired client, the page seen in Figure 10-50 appears.
Guidelines and Limitations

- We recommend using a 5-GHz radio for the uplink to Mesh AP infrastructure so you can take advantage of a strong client access on two 5-GHz radios available on mesh access points. A 5-GHz band allows more Effective Isotropic Radiated Power (EIRP) and is less polluted. In a two-radio WGB, configure 5-GHz radio (radio 1) mode as WGB. This radio will be used to access the mesh infrastructure. Configure the second radio 2.4-GHz (radio 0) mode as Root for client access.

- On the Autonomous access points, only one SSID can be assigned to the native VLAN. You cannot have multiple VLANs in one SSID on the autonomous side. SSID to VLAN mapping should be unique because this is the way to segregate traffic on different VLANs. In a unified architecture, multiple VLANs can be assigned to one WLAN (SSID).
Only one WLAN (SSID) for wireless association of the WGB to the access point infrastructure is supported. This SSID should be configured as an infrastructure SSID and should be mapped to the native VLAN.

A dynamic interface should be created in the controller for each VLAN configured in the WGB.

A second radio (2.4-GHz) on the access point should be configured for client access. You have to use the same SSID on both radios and map to the native VLAN. If you create a separate SSID, then it is not possible to map it to a native VLAN, due to the unique VLAN/SSID mapping requirements. If you try to map the SSID to another VLAN, then you do not have multiple VLAN support for wireless clients.

All Layer 2 security types are supported for the WLANs (SSIDs) for wireless client association in WGB.

This feature does not depend on the AP platform. On the controller side, both mesh and nonmesh APs are supported.

There is a limitation of 20 clients in the WGB. The 20-client limitation includes both wired and wireless clients. If the WGB is talking to autonomous access points, then the client limit is very high.

The controller treats the wireless and wired clients behind a WGB in the same manner. Features such as MAC filtering and link test are not supported for wireless WGB clients from the controller.

If required, you can run link tests for a WGB wireless client from an autonomous AP.

Multiple VLANs for wireless clients associated to a WGB are not supported.

Up to 16 multiple VLANs are supported for wired clients behind a WGB from the 7.0 release and later releases.

Roaming is supported for wireless and wired clients behind a WGB. The wireless clients on the other radio will not be dissociated by the WGB when an uplink is lost or in a roaming scenario.

Non-Cisco workgroup bridges are supported on Mesh access points.

We recommend that you configure radio 0 (2.4 GHz) as a Root (one of the mode of operations for Autonomous AP) and radio 1 (5 GHz) as a WGB.

**Example— Configuration of a Workgroup Bridge**

When you configure from the CLI, the following are mandatory:

- dot11 SSID (security for a WLAN can be decided based on the requirement).
- Map the subinterfaces in both the radios to a single bridge group.

**Note**

A native VLAN is always mapped to bridge group 1 by default. For other VLANs, the bridge group number matches the VLAN number; for example, for VLAN 46, the bridge group is 46.

- Map the SSID to the radio interfaces and define the role of the radio interfaces.

In the following example, one SSID (WGBTEST) is used in both radios, and the SSID is the infrastructure SSID mapped to NATIVE VLAN 51. All radio interfaces are mapped to bridge group -1.

```
WGB1# config
WGB1(config)# interface Dot11Radio1.51
WGB1(config-subif)# encapsulation dot1q 51 native
WGB1(config-subif)# bridge-group 1
WGB1(config-subif)# exit
WGB1(config)# interface Dot11Radio0.51
WGB1(config-subif)# encapsulation dot1q 51 native
```
WGB1(config-subif)# bridge-group 1
WGB1(config-subif)# exit
WGB1(config)# dot11 ssid WGBTEST
WGB1(config-ssid)# VLAN 51
WGB1(config-ssid)# authentication open
WGB1(config-ssid)# infrastructure-ssid
WGB1(config-ssid)# exit
WGB1(config)# interface Dot11Radio1
WGB1(config-if)# ssid WGBTEST
WGB1(config-if)# station-role workgroup-bridge
WGB1(config-if)# exit
WGB1(config)# interface Dot11Radio0
WGB1(config-if)# ssid WGBTEST
WGB1(config-if)# station-role root
WGB1(config-if)# exit

You can also use the GUI of an autonomous AP for configuration. From the GUI, subinterfaces are automatically created after the VLAN is defined.

WGB Association Check

Both the WGB association to the controller and the wireless client association to WGB can be verified by entering the `show dot11 associations client` command in autonomous AP.

WGB# show dot11 associations client

802.11 Client Stations on Dot11Radio1:

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>Device</th>
<th>Name</th>
<th>Parent</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0024.130f.920e</td>
<td>209.165.200.225</td>
<td>LWAPP-Parent</td>
<td>RAPSB</td>
<td>-</td>
<td>Assoc</td>
</tr>
</tbody>
</table>

From the controller, choose Monitor > Clients. The WGB and the wireless/wired client behind the WGB are updated and the wireless/wired client are shown as the WGB client, as shown in Figure 10-52, Figure 10-53, and Figure 10-54.
Link Test Result

Figure 10-55 shows the link test results.
A link test can also be run from the controller CLI using this command:

```
linktest client mac address
```

Link tests from the controller are only limited to the WGB, and they cannot be run beyond the WGB from the controller to a wired or wireless client connected to the WGB. You can run link tests for the wireless client connected to the WGB from the WGB itself using the following command:

```
ap# dot11 dot11Radio 0 linktest target client mac
```

Start linktest to 0040.96b8.d462, 100 512 byte packets

```
ap#
```

```
POOR (4% lost) Time (msec) Strength (dBm) SNR Quality Retries

Sent: 100 Avg. 22 -37 -83 48 3 Tot. 34 35

Lost to Tgt: 4 Max. 112 -34 -78 61 10 Max. 10 5

Lost to Src: 4 Min. 0 -40 -87 15 3

Rates (Src/Tgt) 24Mb 0/5 36Mb 25/0 48Mb 73/0 54Mb 2/91
```

Linktest Done in 24.464 msec
WGB Wired/Wireless Client

You can also use the following commands to know the summary of WGBs and clients associated associated with a Cisco lightweight access point:

**show wgb summary**
Number of WGBs: 2

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>AP Name</th>
<th>Status</th>
<th>WLAN</th>
<th>Auth</th>
<th>Protocol</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:1d:70:97:bd:e8</td>
<td>209.165.200.225</td>
<td>c1240</td>
<td>Assoc</td>
<td>2</td>
<td>Yes</td>
<td>802.11a</td>
<td>2</td>
</tr>
<tr>
<td>00:1e:be:27:5f:e2</td>
<td>209.165.200.226</td>
<td>c1240</td>
<td>Assoc</td>
<td>2</td>
<td>Yes</td>
<td>802.11a</td>
<td>5</td>
</tr>
</tbody>
</table>

**show client summary**
Number of Clients: 7

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>AP Name</th>
<th>Status</th>
<th>WLAN/Guest-Lan</th>
<th>Auth</th>
<th>Protocol</th>
<th>Port</th>
<th>Wired</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:24:ca:a9:b4</td>
<td>R14</td>
<td>Associated</td>
<td>1</td>
<td>Yes</td>
<td>N/A</td>
<td>29</td>
<td>No</td>
</tr>
<tr>
<td>00:24:c4:a0:61:3a</td>
<td>R14</td>
<td>Associated</td>
<td>1</td>
<td>Yes</td>
<td>802.11a</td>
<td>29</td>
<td>No</td>
</tr>
<tr>
<td>00:24:c4:a0:61:f4</td>
<td>R14</td>
<td>Associated</td>
<td>1</td>
<td>Yes</td>
<td>802.11a</td>
<td>29</td>
<td>No</td>
</tr>
<tr>
<td>00:24:c4:a0:61:f8</td>
<td>R14</td>
<td>Associated</td>
<td>1</td>
<td>Yes</td>
<td>802.11a</td>
<td>29</td>
<td>No</td>
</tr>
<tr>
<td>00:24:c4:a0:62:0a</td>
<td>R14</td>
<td>Associated</td>
<td>1</td>
<td>Yes</td>
<td>802.11a</td>
<td>29</td>
<td>No</td>
</tr>
<tr>
<td>00:24:c4:a0:62:42</td>
<td>R14</td>
<td>Associated</td>
<td>1</td>
<td>Yes</td>
<td>802.11a</td>
<td>29</td>
<td>No</td>
</tr>
<tr>
<td>00:24:c4:a0:71:d2</td>
<td>R14</td>
<td>Associated</td>
<td>1</td>
<td>Yes</td>
<td>802.11a</td>
<td>29</td>
<td>No</td>
</tr>
</tbody>
</table>

**show wgb detail 00:1e:be:27:5f:e2**
Number of wired client(s): 5

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>AP Name</th>
<th>Mobility</th>
<th>WLAN</th>
<th>Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:16:c7:5d:64:b4:8f</td>
<td>Unknown</td>
<td>c1240</td>
<td>Local</td>
<td>2</td>
<td>No</td>
</tr>
<tr>
<td>00:21:91:7f:82:e9:ae</td>
<td>209.165.200.232</td>
<td>c1240</td>
<td>Local</td>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>00:21:55:00:40:7f:8b</td>
<td>209.165.200.234</td>
<td>c1240</td>
<td>Local</td>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>00:1e:58:31:c7:4a</td>
<td>209.165.200.236</td>
<td>c1240</td>
<td>Local</td>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>00:23:04:9a:0b:12</td>
<td>Unknown</td>
<td>c1240</td>
<td>Local</td>
<td>2</td>
<td>No</td>
</tr>
</tbody>
</table>
Client Roaming

High-speed roaming of Cisco Compatible Extension (CX), version 4 (v4) clients is supported at speeds up to 70 miles per hour in outdoor mesh deployments of AP1522s and AP1524s. An example application might be maintaining communication with a terminal in an emergency vehicle as it moves within a mesh public network.

Three Cisco CX v4 Layer 2 client roaming enhancements are supported:

- **Access point assisted roaming**—Helps clients save scanning time. When a Cisco CX v4 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client’s current SSID(s), and time elapsed since disassociation.

- **Enhanced neighbor list**—Focuses on improving a Cisco CX v4 client’s roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.

- **Roam reason report**—Enables Cisco CX v4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.

> Note

Client roaming is enabled by default.


WGB Roaming Guidelines

- **Configuring a WGB for roaming**—If a WGB is mobile, you can configure it to scan for a better radio connection to a parent access point or bridge. Use the `mobile station period 3 threshold 50` command to configure the workgroup bridge as a mobile station.

  When you enable this setting, the WGB scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using these criteria, a WGB configured as a mobile station searches for a new parent association and roams to a new parent before it loses its current association. When the mobile station setting is disabled (the default setting), a WGB does not search for a new association until it loses its current association.

- **Configuring a WGB for Limited Channel Scanning**—In mobile environments such as railroads, a WGB instead of scanning all the channels is restricted to scan only a set of limited channels to reduce the hand-off delay when the WGB roams from one access point to another. By limiting the number of channels, the WGB scans only those required channels; the mobile WGB achieves and maintains a continuous wireless LAN connection with fast and smooth roaming. This limited channel set is configured using the `ap(config-if)#mobile station scan set of channels`.

  This command invokes scanning to all or specified channels. There is no limitation on the maximum number of channels that can be configured. The maximum number of channels that can be configured is restricted only by the number of channels that a radio can support. When executed, the WGB scans only this limited channel set. This limited channel feature also affects the known channel list that the WGB receives from the access point to which it is currently associated. Channels are added to the known channel list only if they are also part of the limited channel set.
### Configuration Example

This example shows how to configure a roaming configuration:

```
ap(config)# interface dot11radio 1
ap(config-if)# ssid outside
ap(config-if)# packet retries 16
ap(config-if)# station role workgroup-bridge
ap(config-if)# mobile station
ap(config-if)# mobile station period 3 threshold 50
```

Use the `no mobile station scan` command to restore scanning to all the channels.

**Table 10-10** identifies mesh access points and their respective frequency bands that support WGB.

### Table 10-10  WGB Interoperability Chart

<table>
<thead>
<tr>
<th>RAP/MAP</th>
<th>W GB</th>
<th>4.9 GHz (5, 10, 20 MHz)</th>
<th>5 GHz</th>
<th>2.4 GHz</th>
<th>5 GHz</th>
<th>2.4 GHz</th>
<th>5 GHz</th>
<th>2.4 GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backhaul</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1552/1552</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1524SB/1524SB</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1524PS/1524PS</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1522/1522</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1524SB/1522</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1524PS/1522</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1522/1524SB</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1522/1524PS</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1240/1130</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Troubleshooting Tips

If a wireless client is not associated with a WGB, use the following steps to troubleshoot the problem:

1. Verify the client configuration and ensure that the client configuration is correct.
2. Check the `show bridge` command output in autonomous AP, and confirm that the AP is reading the client MAC address from the right interface.
3. Confirm that the subinterfaces corresponding to specific VLANs in different interfaces are mapped to the same bridge group.
4. If required, clear the bridge entry using the `clear bridge` command (this command will remove all wired and wireless clients associated in a WGB and make them associate again).
5. Check the `show dot11 association` command output and confirm that the WGB is associated with the controller.
6. Ensure that the WGB has not exceeded its 20-client limitation.

In a normal scenario, if the `show bridge` and `show dot11 association` command outputs are as expected, wireless client association should be successful.
Configuring Voice Parameters in Indoor Mesh Networks

You can configure call admission control (CAC) and QoS on the controller to manage voice and video quality on the mesh network.

The indoor mesh access points are 802.11e capable, and QoS is supported on the local 2.4-GHz access radio and the 5-GHz backhaul radio. CAC is supported on the backhaul and the CCXv4 clients (which provides CAC between the mesh access point and the client).

Note: Voice is supported only on indoor mesh networks. Voice is supported on a best-effort basis in the outdoors in a mesh network.

CAC

CAC enables a mesh access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi Multimedia (WMM) protocol deployed in CCXv3 ensures sufficient QoS as long as the wireless LAN is not congested. However, to maintain QoS under differing network loads, CAC in CCXv4 or later is required.


Two types of CAC are available for access points: bandwidth-based CAC and load-based CAC. All calls on a mesh network are bandwidth-based, so mesh access points use only bandwidth-based CAC.

Bandwidth-based, or static CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new call. Each access point determines whether it is capable of accommodating a particular call by looking at the bandwidth available and compares it against the bandwidth required for the call. If there is not enough bandwidth available to maintain the maximum allowed number of calls with acceptable quality, the mesh access point rejects the call.

QoS and DSCP Marking

Cisco supports 802.11e on the local access and on the backhaul. Mesh access points prioritize user traffic based on classification, and therefore all user traffic is treated on a best-effort basis.

Resources available to users of the mesh vary, according to the location within the mesh, and a configuration that provides a bandwidth limitation in one point of the network can result in an oversubscription in other parts of the network.

Similarly, limiting clients on their percentage of RF is not suitable for mesh clients. The limiting resource is not the client WLAN, but the resources available on the mesh backhaul.

Similar to wired Ethernet networks, 802.11 WLANs employ Carrier Sense Multiple Access (CSMA), but instead of using collision detection (CD), WLANs use collision avoidance (CA), which means that instead of each station trying to transmit as soon as the medium is free, WLAN devices will use a collision avoidance mechanism to prevent multiple stations from transmitting at the same time.
The collision avoidance mechanism uses two values called CWmin and CWmax. CW stands for *contention window*. The CW determines what additional amount of time an endpoint should wait, after the interframe space (IFS), to attend to transmit a packet. Enhanced distributed coordination function (EDCF) is a model that allows end devices that have delay-sensitive multimedia traffic to modify their CWmin and CWmax values to allow for statically greater (and more frequent) access to the medium.

Cisco access points support EDCF-like QoS. This provides up to eight queues for QoS.

These queues can be allocated in several different ways, as follows:

- Based on TOS / DiffServ settings of packets
- Based on Layer 2 or Layer 3 access lists
- Based on VLAN
- Based on dynamic registration of devices (IP phones)

AP1500s, with Cisco controllers, provide a minimal integrated services capability at the controller, in which client streams have maximum bandwidth limits, and a more robust differentiated services (diffServ) capability based on the IP DSCP values and QoS WLAN overrides.

When the queue capacity has been reached, additional frames are dropped (tail drop).

**Encapsulations**

Several encapsulations are used by the mesh system. These encapsulations include CAPWAP control and data between the controller and RAP, over the mesh backhaul, and between the mesh access point and its client(s). The encapsulation of bridging traffic (noncontroller traffic from a LAN) over the backhaul is the same as the encapsulation of CAPWAP data.

There are two encapsulations between the controller and the RAP. The first is for CAPWAP control, and the second is for CAPWAP data. In the control instance, CAPWAP is used as a container for control information and directives. In the instance of CAPWAP data, the entire packet, including the Ethernet and IP headers, is sent in the CAPWAP container.

**Figure 10-56 Encapsulations**

![Diagram showing encapsulations between Controller and RAP](image)

For the backhaul, there is only one type of encapsulation, encapsulating MESH traffic. However, two types of traffic are encapsulated: bridging traffic and CAPWAP control and data traffic. Both types of traffic are encapsulated in a proprietary mesh header.
In the case of bridging traffic, the entire packet Ethernet frame is encapsulated in the mesh header (see Figure 10-57).

All backhaul frames are treated identically, regardless of whether they are MAP to MAP, RAP to MAP, or MAP to RAP.

**Figure 10-57 Encapsulating Mesh Traffic**

Queuing on the Mesh Access Point

The mesh access point uses a high speed CPU to process ingress frames, Ethernet, and wireless on a first-come, first-serve basis. These frames are queued for transmission to the appropriate output device, either Ethernet or wireless. Egress frames can be destined for either the 802.11 client network, the 802.11 backhaul network, or Ethernet.

AP1500s support four FIFOs for wireless client transmissions. These FIFOs correspond to the 802.11e platinum, gold, silver, and bronze queues, and obey the 802.11e transmission rules for those queues. The FIFOs have a user configurable queue depth.

The backhaul (frames destined for another outdoor mesh access point) uses four FIFOs, although user traffic is limited to gold, silver, and bronze. The platinum queue is used exclusively for CAPWAP control traffic and voice, and has been reworked from the standard 802.11e parameters for CWmin, CWmax, and so on, to provide more robust transmission but higher latencies.

The 802.11e parameters for CWmin, CWmax, and so on, for the gold queue have been reworked to provide lower latency at the expense of slightly higher error rate and aggressiveness. The purpose of these changes is to provide a channel that is more conducive to video applications.

Frames that are destined for Ethernet are queued as FIFO, up to the maximum available transmit buffer pool (256 frames). There is support for a Layer 3 IP Differentiated Services Code Point (DSCP), so marking of the packets is there as well.

In the controller to RAP path for the data traffic, the outer DSCP value is set to the DSCP value of the incoming IP frame. If the interface is in tagged mode, the controller sets the 802.1Q VLAN ID and derives the 802.1p UP (outer) from 802.1p UP incoming and the WLAN default priority ceiling. Frames with VLAN ID 0 are not tagged.
For CAPWAP control traffic the IP DSCP value is set to 46, and the 802.1p user priority is set to 7. Prior to transmission of a wireless frame over the backhaul, regardless of node pairing (RAP/MAP) or direction, the DSCP value in the outer header is used to determine a backhaul priority. The following sections describe the mapping between the four backhaul queues the mesh access point uses and the DSCP values shown in Backhaul Path QoS (see Table 10-11).

### Table 10-11 Backhaul Path QoS

<table>
<thead>
<tr>
<th>DSCP Value</th>
<th>Backhaul Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>2, 4, 6, 8 to 23</td>
<td>Bronze</td>
</tr>
<tr>
<td>26, 32 to 63</td>
<td>Gold</td>
</tr>
<tr>
<td>46 to 56</td>
<td>Platinum</td>
</tr>
<tr>
<td>All others including 0</td>
<td>Silver</td>
</tr>
</tbody>
</table>

The platinum backhaul queue is reserved for CAPWAP control traffic, IP control traffic, and voice packets. DHCP, DNS, and ARP requests are also transmitted at the platinum QoS level. The mesh software inspects each frame to determine whether it is a CAPWAP control or IP control frame in order to protect the platinum queue from use by non-CAPWAP applications.

For a MAP to the client path, there are two different procedures, depending on whether the client is a WMM client or a normal client. If the client is a WMM client, the DSCP value in the outer frame is examined, and the 802.11e priority queue is used (see Table 10-12).

### Table 10-12 MAP to Client Path QoS

<table>
<thead>
<tr>
<th>DSCP Value</th>
<th>Backhaul Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>2, 4, 6, 8 to 23</td>
<td>Bronze</td>
</tr>
<tr>
<td>26, 32 to 45, 47</td>
<td>Gold</td>
</tr>
<tr>
<td>46, 48 to 63</td>
<td>Platinum</td>
</tr>
<tr>
<td>All others including 0</td>
<td>Silver</td>
</tr>
</tbody>
</table>

If the client is not a WMM client, the WLAN override (as configured at the controller) determines the 802.11e queue (bronze, gold, platinum, or silver), on which the packet is transmitted.

For a client of a mesh access point, there are modifications made to incoming client frames in preparation for transmission on the mesh backhaul or Ethernet. For WMM clients, a MAP illustrates the way in which the outer DSCP value is set from an incoming WMM client frame (see Figure 10-59).
The minimum value of the incoming 802.11e user priority and the WLAN override priority is translated using the information listed in Table 10-13 to determine the DSCP value of the IP frame. For example, if the incoming frame has as its value a priority indicating the gold priority, but the WLAN is configured for the silver priority, the minimum priority of silver is used to determine the DSCP value.

If there is no incoming WMM priority, the default WLAN priority is used to generate the DSCP value in the outer header. If the frame is an originated CAPWAP control frame, the DSCP value of 46 is placed in the outer header.

With the 5.2 code enhancements, DSCP information is preserved in an AWPP header.

All wired client traffic is restricted to a maximum 802.1p UP value of 5, except DHCP/DNS and ARP packets, which go through the platinum queue.

The non-WMM wireless client traffic gets the default QoS priority of its WLAN. The WMM wireless client traffic may have a maximum 802.11e value of 6, but it must be below the QoS profile configured for its WLAN. If admission control is configured, WMM clients must use TSPEC signaling and get admitted by CAC.

The CAPWAPP data traffic carries wireless client traffic and has the same priority and treatment as wireless client traffic.

Now that the DSCP value is determined, the rules described earlier for the backhaul path from the RAP to the MAP are used to further determine the backhaul queue on which the frame is transmitted. Frames transmitted from the RAP to the controller are not tagged. The outer DSCP values are left intact, as they were first constructed.

### Bridging Backhaul Packets

Bridging services are treated a little differently from regular controller-based services. There is no outer DSCP value in bridging packets because they are not CAPWAP encapsulated. Therefore, the DSCP value in the IP header as it was received by the mesh access point is used to index into the table as described in the path from the mesh access point to the mesh access point (backhaul).

---

**Table 10-13 DSCP to Backhaul Queue Mapping**

<table>
<thead>
<tr>
<th>DSCP Value</th>
<th>802.11e UP</th>
<th>Backhaul Queue</th>
<th>Packet Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>2, 4, 6, 8 to 23</td>
<td>1, 2</td>
<td>Bronze</td>
<td>Lowest priority packets, if any</td>
</tr>
<tr>
<td>26, 32 to 34</td>
<td>4, 5</td>
<td>Gold</td>
<td>Video packets</td>
</tr>
<tr>
<td>46 to 56</td>
<td>6, 7</td>
<td>Platinum</td>
<td>CAPWAP control, AWPP, DHCP/DNS, ARP packets, voice packets</td>
</tr>
<tr>
<td>All others including 0</td>
<td>0, 3</td>
<td>Silver</td>
<td>Best effort, CAPWAP data packets</td>
</tr>
</tbody>
</table>

**Figure 10-59 MAP to RAP Path**

![Figure 10-59 MAP to RAP Path](image-url)
Bridging Packets from and to a LAN

Packets received from a station on a LAN are not modified in any way. There is no override value for the LAN priority. Therefore, the LAN must be properly secured in bridging mode. The only protection offered to the mesh backhaul is that non-CAPWAP control frames that map to the platinum queue are demoted to the gold queue.

Packets are transmitted to the LAN precisely as they are received on the Ethernet ingress at entry to the mesh.

The only way to integrate QoS between Ethernet ports on AP1500 and 802.11a is by tagging Ethernet packets with DSCP. AP1500s take the Ethernet packet with DSCP and places it in the appropriate 802.11e queue.

AP1500s do not tag DSCP itself:

- On the ingress port, the AP1500 sees a DSCP tag, encapsulates the Ethernet frame, and applies the corresponding 802.11e priority.
- On the egress port, the AP1500 decapsulates the Ethernet frame, and places it on the wire with an untouched DSCP field.

Ethernet devices, such as video cameras, should have the capability to mark the bits with DSCP value to take advantage of QoS.

Note: QoS only is relevant when there is congestion on the network.

Guidelines For Using Voice on the Mesh Network

- Voice is supported only on indoor mesh networks in release 5.2, 6.0, 7.0, and 7.0.116.0. For outdoors, voice is supported on a best-effort basis on a mesh infrastructure.
- When voice is operating on a mesh network, calls must not traverse more than two hops. Each sector must be configured to require no more than two hops for voice.
- RF considerations for voice networks are as follows:
  - Coverage hole of 2 to 10 percent
  - Cell coverage overlap of 15 to 20 percent
  - Voice needs RSSI and SNR values that are at least 15 dB higher than data requirements
  - RSSI of -67 dBm for all data rates should be the goal for 11b/g/n and 11a/n
  - SNR should be 25 dB for the data rate used by client to connect to the AP
  - Packet error rate (PER) should be configured for a value of one percent or less
  - Channel with the lowest utilization (CU) must be used
- On the 802.11a/n (or 802.11b/g/n) > Global parameters page, you should do the following:
  - Enable dynamic target power control (DTPC).
  - Disable all data rates less than 11 Mbps.
- On the 802.11a/n or 802.11b/g/n > Voice parameters page, you should do the following:
  - Load-based CAC must be disabled.
  - Enable admission control (ACM) for CCXv4 or v5 clients that have WMM enabled. Otherwise, bandwidth-based CAC does not operate properly.
- Set the maximum RF bandwidth to 50 percent.
- Set the reserved roaming bandwidth to 6 percent.
- Enable traffic stream metrics.

On the 802.11a/n or 802.11b/g/n > EDCA parameters page, you should do the following:
- Set the EDCA profile for the interface as voice optimized.
- Disable low latency MAC.

On the QoS > Profile page, you should do the following:
- Create a voice profile and select 802.1Q as the wired QoS protocol type.

On the WLANs > Edit > QoS page, you should do the following:
- Select a QoS of platinum for voice and gold for video on the backhaul.
- Select allowed as the WMM policy.

On the WLANs > Edit > QoS page, you should do the following:
- Select CCKM for authorization (auth) key management (mgmt) if you want to support fast roaming. See the “Client Roaming” section on page 10-90.

On the x > y page, you should do the following:
- Disable voice active detection (VAD).

Voice Call Support in a Mesh Network

Table 10-14 shows the actual calls in a clean, ideal environment.

<table>
<thead>
<tr>
<th>No. of Calls</th>
<th>802.11a Radio</th>
<th>802.11b/g Radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAP</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>MAP1</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>MAP2</td>
<td>4</td>
<td>8</td>
</tr>
</tbody>
</table>

Table 10-15 shows the actual calls in a clean, ideal environment.

<table>
<thead>
<tr>
<th>No. of Calls</th>
<th>802.11a/n Radio 20 MHz</th>
<th>802.11a/n Radio 40 MHz</th>
<th>802.11b/g/n Backhaul Radio 20 MHz</th>
<th>802.11b/g/n Backhaul Radio 40 MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAP</td>
<td>20</td>
<td>35</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>MAP1 (First Hop)</td>
<td>10</td>
<td>20</td>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td>MAP2 (Second Hop)</td>
<td>8</td>
<td>15</td>
<td>10</td>
<td>15</td>
</tr>
</tbody>
</table>

1. Traffic was bidirectional 64K voice flows. VoCoder type: G.711, PER <= 1%. Network setup was daisy-chained with no calls traversing more than 2 hops. No external interference.
While making a call, observe the MOS score of the call on the 7921 phone (see Table 10-16). A MOS score between 3.5 and 4 is acceptable.

<table>
<thead>
<tr>
<th>MOS rating</th>
<th>User satisfaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; 4.3</td>
<td>Very satisfied</td>
</tr>
<tr>
<td>4.0</td>
<td>Satisfied</td>
</tr>
<tr>
<td>3.6</td>
<td>Some users dissatisfied</td>
</tr>
<tr>
<td>3.1</td>
<td>Many users dissatisfied</td>
</tr>
<tr>
<td>&lt; 2.58</td>
<td>——</td>
</tr>
</tbody>
</table>

**Viewing the Voice Details for Mesh Networks (CLI)**

Use the commands in this section to view details on voice and video calls on the mesh network:

*Note* See Figure 10-60 when using the CLI commands and viewing their output.

- To view the total number of voice calls and the bandwidth used for voice calls on each RAP, enter this command:
  ```
  show mesh cac summary
  ```
Information similar to the following appears:

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Slot#</th>
<th>Radio</th>
<th>BW Used/Max</th>
<th>Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB_RAP1</td>
<td>0</td>
<td>11b/g</td>
<td>0/23437</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0/23437</td>
<td>0</td>
</tr>
<tr>
<td>SB_MAP1</td>
<td>0</td>
<td>11b/g</td>
<td>0/23437</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0/23437</td>
<td>0</td>
</tr>
<tr>
<td>SB_MAP2</td>
<td>0</td>
<td>11b/g</td>
<td>0/23437</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0/23437</td>
<td>0</td>
</tr>
<tr>
<td>SB_MAP3</td>
<td>0</td>
<td>11b/g</td>
<td>0/23437</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0/23437</td>
<td>0</td>
</tr>
</tbody>
</table>

- To view the mesh tree topology for the network and the bandwidth utilization (used/maximum available) of voice calls and video links for each mesh access point and radio, enter this command:

  `show mesh cac bwused {voice | video} AP_name`

Information similar to the following appears:

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Slot#</th>
<th>Radio</th>
<th>BW Used/Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB_RAP1</td>
<td>0</td>
<td>11b/g</td>
<td>1016/23437</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>3048/23437</td>
</tr>
<tr>
<td>SB_MAP1</td>
<td>0</td>
<td>11b/g</td>
<td>0/23437</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>3048/23437</td>
</tr>
<tr>
<td>SB_MAP2</td>
<td>0</td>
<td>11b/g</td>
<td>2032/23437</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>3048/23437</td>
</tr>
<tr>
<td>SB_MAP3</td>
<td>0</td>
<td>11b/g</td>
<td>0/23437</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0/23437</td>
</tr>
</tbody>
</table>

**Note** The bars (|) to the left of the AP Name field indicate the number of hops that the MAP is from its RAP.

**Note** When the radio type is the same, the backhaul bandwidth utilization (bw used/max) at each hop is identical. For example, mesh access points map1, map2, map3, and rap1 are all on the same radio backhaul (802.11a) and are using the same bandwidth (3048). All of the calls are in the same interference domain. A call placed anywhere in that domain affects the others.

- To view the mesh tree topology for the network and display the number of voice calls that are in progress by mesh access point radio, enter this command:

  `show mesh cac access AP_name`

Information similar to the following appears:

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Slot#</th>
<th>Radio</th>
<th>Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB_RAP1</td>
<td>0</td>
<td>11b/g</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0</td>
</tr>
<tr>
<td>SB_MAP1</td>
<td>0</td>
<td>11b/g</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0</td>
</tr>
<tr>
<td>SB_MAP2</td>
<td>0</td>
<td>11b/g</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0</td>
</tr>
<tr>
<td>SB_MAP3</td>
<td>0</td>
<td>11b/g</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0</td>
</tr>
</tbody>
</table>
Note  Each call received by a mesh access point radio causes the appropriate calls summary column to increment by one. For example, if a call is received on the 802.11b/g radio on map2, then a value of one is added to the existing value in that radio’s calls column. In this case, the new call is the only active call on the 802.11b/g radio of map2. If one call is active when a new call is received, the resulting value is two.

• To view the mesh tree topology for the network and display the voice calls that are in progress, enter this command:

  `show mesh cac callpath AP_name`

  Information similar to the following appears:

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Slot#</th>
<th>Radio</th>
<th>Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB_RAP1</td>
<td>0</td>
<td>11b/g</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>1</td>
</tr>
<tr>
<td>SB_MAP1</td>
<td>0</td>
<td>11b/g</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>1</td>
</tr>
<tr>
<td>SB_MAP2</td>
<td>0</td>
<td>11b/g</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>1</td>
</tr>
<tr>
<td>SB_MAP3</td>
<td>0</td>
<td>11b/g</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0</td>
</tr>
</tbody>
</table>

Note  The calls column for each mesh access point radio in a call path increments by one. For example, for a call that initiates at map2 (show mesh cac call path SB_MAP2) and terminates at rap1 by way of map1, one call is added to the map2 802.11b/g and 802.11a radio calls column, one call to the map1 802.11a backhaul radio calls column, and one call to the rap1 802.11a backhaul radio calls column.

• To view the mesh tree topology of the network, the voice calls that are rejected at the mesh access point radio due to insufficient bandwidth, and the corresponding mesh access point radio where the rejection occurred, enter this command:

  `show mesh cac rejected AP_name`

  Information similar to the following appears:

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Slot#</th>
<th>Radio</th>
<th>Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB_RAP1</td>
<td>0</td>
<td>11b/g</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0</td>
</tr>
<tr>
<td>SB_MAP1</td>
<td>0</td>
<td>11b/g</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0</td>
</tr>
<tr>
<td>SB_MAP2</td>
<td>0</td>
<td>11b/g</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0</td>
</tr>
<tr>
<td>SB_MAP3</td>
<td>0</td>
<td>11b/g</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>11a</td>
<td>0</td>
</tr>
</tbody>
</table>

Note  If a call is rejected at the map2 802.11b/g radio, its calls column increments by one.

• To view the number of bronze, silver, gold, platinum, and management queues active on the specified access point, enter this command. The peak and average length of each queue are shown as well as the overflow count.
show mesh queue-stats AP_name

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Queue Type</th>
<th>Overflows</th>
<th>Peak length</th>
<th>Average length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silver</td>
<td>0</td>
<td>1</td>
<td>0.000</td>
</tr>
<tr>
<td>Gold</td>
<td>0</td>
<td>4</td>
<td>0.004</td>
</tr>
<tr>
<td>Platinum</td>
<td>0</td>
<td>4</td>
<td>0.001</td>
</tr>
<tr>
<td>Bronze</td>
<td>0</td>
<td>0</td>
<td>0.000</td>
</tr>
<tr>
<td>Management</td>
<td>0</td>
<td>0</td>
<td>0.000</td>
</tr>
</tbody>
</table>

Overflows—The total number of packets dropped due to queue overflow.

Peak Length—The peak number of packets waiting in the queue during the defined statistics time interval.

Average Length—The average number of packets waiting in the queue during the defined statistics time interval.

**Enabling Mesh Multicast Containment for Video**

You can use the controller CLI to configure three mesh multicast modes to manage video camera broadcasts on all mesh access points. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

Mesh multicast modes determine how bridging-enabled access points MAP and RAP send multicasts among Ethernet LANs within a mesh network. Mesh multicast modes manage non-CAPWAP multicast traffic only. CAPWAP multicast traffic is governed by a different mechanism.

The three mesh multicast modes are as follows:

- **Regular mode**—Data is multicast across the entire mesh network and all its segments by bridging-enabled RAP and MAP.

- **In-only mode**—Multicast packets received from the Ethernet by a MAP are forwarded to the RAP’s Ethernet network. No additional forwarding occurs, which ensures that non-CAPWAP multicasts received by the RAP are not sent back to the MAP Ethernet networks within the mesh network (their point of origin), and MAP to MAP multicasts do not occur because they are filtered out.

  **Note** When an HSRP configuration is in operation on a mesh network, we recommend the In-Out multicast mode be configured.

- **In-out mode**—The RAP and MAP both multicast but in a different manner:
  - In-out mode is the default mode.
  - If multicast packets are received at a MAP over Ethernet, they are sent to the RAP; however, they are not sent to other MAP over Ethernet, and the MAP to MAP packets are filtered out of the multicast.
  - If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks. When the in-out mode is in operation, it is important to properly partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment and then sent back into the network.
Note If 802.11b clients need to receive CAPWAP multicasts, then multicast must be enabled globally on the controller as well as on the mesh network (using the `config network multicast global enable` CLI command). If multicast does not need to extend to 802.11b clients beyond the mesh network, the global multicast parameter should be disabled (using the `config network multicast global disable` command).

### Enabling Multicast on a Mesh Network (CLI)

To enable multicast mode on the mesh network to receive multicasts from beyond the mesh networks, enter these commands:

```
config network multicast global enable
config mesh multicast {regular | in | in-out}
```

To enable multicast mode only the mesh network (multicasts do not need to extend to 802.11b clients beyond the mesh network), enter these commands:

```
config network multicast global disable
config mesh multicast {regular | in | in-out}
```

**Note** Multicast for mesh networks cannot be enabled using the controller GUI.

### IGMP Snooping

IGMP snooping delivers improved RF usage through selective multicast forwarding and optimizes packet forwarding in voice and video applications.

A mesh access point transmits multicast packets only if a client is associated with the mesh access point that is subscribed to the multicast group. So, when IGMP snooping is enabled, only that multicast traffic relevant to given hosts is forwarded.

To enable IGMP snooping on the controller, enter this command:

```
configure network multicast igmp snooping enable
```

A client sends an IGMP `join` that travels through the mesh access point to the controller. The controller intercepts the `join` and creates a table entry for the client in the multicast group. The controller then proxies the IGMP `join` through the upstream switch or router.

You can query the status of the IGMP groups on a router by entering this command:

```
router# show ip gmp groups
```

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Interface</th>
<th>Uptime</th>
<th>Expires</th>
<th>Last Reporter</th>
</tr>
</thead>
<tbody>
<tr>
<td>233.0.0.1</td>
<td>Vlan119</td>
<td>00:01:52</td>
<td>10.1.1.130</td>
<td></td>
</tr>
</tbody>
</table>

For Layer 3 roaming, an IGMP query is sent to the client’s WLAN. The controller modifies the client’s response before forwarding and changes the source IP address to the controller’s dynamic interface IP address.

The network hears the controller’s request for the multicast group and forwards the multicast to the new controller.

For more information about video, see the following:
Locally Significant Certificates for Mesh APs

Until the 7.0 release, mesh APs supported only the Manufactured Installed Certificate (MIC) to authenticate and get authenticated by controllers to join the controller. You might have had to have your own public key infrastructure (PKI) to control CAs, to define policies, to define validity periods, to define restrictions and usages on the certificates that are generated, and get these certificates installed on the APs and controllers. After these customer-generated or locally significant certificates (LSCs) are present on the APs and controllers, the devices start using these LSCs, to join, authenticate, and derive a session key. Cisco supported normal APs from the 5.2 release and later releases and extended the support for mesh APs as well from the 7.0 release.

With the 7.0.116.0 release, the following functionality has been added:

- Graceful fallback to MIC if APs are unable to join the controller with LSC certificates—Local APs try to join a controller with an LSC for the number of times that are configured on the controller (the default value is 3). After these trials, the AP deletes the LSC and tries to join a controller with an MIC.

Mesh APs try to join a controller with an LSC until its lonely timer expires and the AP reboots. The lonely timer is set for 40 minutes. After the reboot, the AP tries to join a controller with an MIC. If the AP is again not able to join a controller with an MIC in 40 minutes, the AP reboots and then tries to join a controller with an LSC.

Note

An LSC in mesh APs is not deleted. An LSC is deleted in mesh APs only when the LSC is disabled on the controller, which causes the APs to reboot.

- Over the air provisioning of MAPs.

Guidelines and Limitations

- This feature does not remove any preexisting certificates from an AP. It is possible for an AP to have both LSC and MIC certificates.

- After an AP is provisioned with an LSC, it does not read in its MIC certificate on boot-up. A change from an LSC to an MIC will require the AP to reboot. APs do it for a fallback if they cannot be joined with an LSC.

- Provisioning an LSC on an AP does not require an AP to turn off its radios, which is vital for mesh APs, which may get provisioned over-the-air.

- Because mesh APs need a dot1x authentication, a CA and ID certificate is required on the server (in the controller or third-party server depending on the configuration).

- LSC provisioning can happen over Ethernet and over-the-air in case of MAPs. You must connect the mesh RAP to the controller through Ethernet and get the LSC certificate provisioned. After the RAP gets the LSC certificate, MAPs connected to this RAP are provisioned with LSC certificates over the air. After the LSC becomes the default, an AP can be connected over-the-air to the controller using the LSC certificate.
Differences Between LSCs for Mesh APs and Normal APs

CAPWAP APs use LSC for DTLS setup during a JOIN irrespective of the AP mode. Mesh APs also use the certificate for mesh security, which involves a dot1x authentication with the controller (or an external AAA server), through the parent AP. After the mesh APs are provisioned with an LSC, they need to use the LSC for this purpose because MIC will not be read in.

Mesh APs use a statically configured dot1x profile to authenticate. This profile is hardcoded to use "cisco" as the certificate issuer. This profile needs to be made configurable so that vendor certificates can be used for mesh authentication (enter the `config local-auth eap-profile cert-issuer vendor "prfMaP1500LIEAuth93"` command).

You must enter the `config mesh lsc enable/disable` command to enable or disable an LSC for mesh APs. This command will cause all the mesh APs to reboot.

Certificate Verification Process in LSC AP

LSC-provisioned APs have both LSC and MIC certificates, but the LSC certificate will be the default one. The verification process consists of the following two steps:

1. The controller sends the AP the MIC device certificate, which the AP verifies with the MIC CA.
2. The AP sends the LSC device certificate to the controller, which the controller verifies with the LSC CA.

Configuring an LSC (CLI)

**Step 1** Enable LSC and provision the LSC CA certificate in the controller.

**Step 2** Enter this command:

`config local-auth eap-profile cert-issuer vendor prfMaP1500LIEAuth93`

**Step 3** Turn on the feature by entering this command:

`config mesh lsc {enable | disable}`

**Step 4** Install the CA and ID cert on the controller (or any other authentication server) from the same certificate server.

**Step 5** Connect the mesh AP through Ethernet and provision for an LSC certificate.

**Step 6** Let the mesh AP get a certificate and join the controller using the LSC certificate. See Figure 10-61 and Figure 10-62.
LSC-Related Commands

The following commands are related to LSCs:

- **config certificate lsc (enable | disable)**
  - *enable*—To enable an LSC on the system.
  - *disable*—To disable an LSC on the system. Use this keyword to remove the LSC device certificate and send a message to an AP, to do the same and disable an LSC, so that subsequent joins could be made using the MIC/SSC. The removal of the LSC CA cert on the WLC should be done explicitly by using the CLI to accommodate any AP that has not transitioned back to the MIC/SSC.

- **config certificate lsc ca-server URL-Path**
This command configures the URL to the CA server for getting the certificates. The URL contains either the domain name or the IP address, port number (typically=80), and the CGI-PATH. The following format is an example:

```
http://ipaddr:port/cgi-path
```

Only one CA server is allowed to be configured. The CA server has to be configured to provision an LSC.

- **config certificate lsc ca-server delete**

  This command deletes the CA server configured on the WLC.

- **config certificate lsc ca-cert {add | delete}**

  This command adds or deletes the LSC CA certificate into/from the WLC's CA certificate database as follows:
  - **add**—Queries the configured CA server for a CA certificate using the SSCEP getca operation, and gets into the WLC and installs it permanently into the WLC database. If installed, this CA certificate is used to validate the incoming LSC device certificate from the AP.
  - **delete**—Deletes the LSC CA certificate from the WLC database.

- **config certificate lsc subject-params Country State City Orgn Dept Email**

  This command configures the parameters for the device certificate that will be created and installed on the controller and the AP.

  All of these strings have 64 bytes, except for the Country that has a maximum of 3 bytes. The Common Name will be autogenerated using its Ethernet MAC address. This should be given prior to the creation of the controller device certificate request.

  The above parameters are sent as an LWAPP payload to the AP, so that the AP can use these parameters to generate the certReq. The CN is autogenerated on the AP using the current MIC/SSC "Cxxxx-MacAddr" format, where xxxx is the product number.

- **config certificate lsc other-params keysize validity**

  The keysize and validity configurations have defaults. Therefore, it is not mandatory to configure them.

  1. The keysize can be from 360 to 2048 (the default is 2048 bits).
  2. The validity period can be configured from 1 to 20 years (the default is 10 years).

- **config certificate lsc ap-provision {enable | disable}**

  This command enables or disables the provisioning of the LSCs on the APs if the APs just joined using the SSC/MIC. If enabled, all APs that join and do not have the LSC will get provisioned.

  If disabled, no more automatic provisioning will be done. This command does not affect the APs, which already have LSCs in them.

- **config certificate lsc ra-cert {add | delete}**

  This command is recommended when the CA server is a Cisco IOS CA server. The WLC can use the RA to encrypt the certificate requests and make communication more secure. RA certificates are not currently supported by other external CA servers, such as MSFT.

  - **add**—Queries the configured CA server for an RA certificate using the SCEP operation and installs it into the WLC Database. This keyword is used to get the certReq signed by the CA.
  - **delete**—Deletes the LSC RA certificate from the WLC database.

- **config auth-list ap-policy lsc {enable | disable}**
After getting the LSC, an AP tries to join the WLC. Before the AP tries to join the WLC, this command must be executed on the WLC console. Execution of this command is mandatory. By default, the **config auth-list ap-policy lsc** command is in the disabled state, and in the disabled state, the APs are not allowed to join the WLC using the LSC.

- **config auth-list ap-policy mic {enable | disable}**

After getting the MIC, an AP tries to join the WLC. Before the AP tries to join the WLC, this command must be executed on the WLC console. Execution of this command is mandatory. By default, the **config auth-list ap-policy mic** command is in the enabled state. If an AP cannot join because of the enabled state, this log message in the WLC side is displayed: LSC/MIC AP is not allowed to join by config.

### Controller CLI show Commands

The following are the WLC **show** commands:

- **show certificate lsc summary**

  This command displays the LSC certificates installed on the WLC. It would be the CA certificate, device certificate, and optionally, an RA certificate if the RA certificate has also been installed. It also indicates if an LSC is enabled or not.

- **show certificate lsc ap-provision**

  This command displays the status of the provisioning of the AP, whether it is enabled or disabled, and whether a provision list is present or not.

- **show certificate lsc ap-provision details**

  This command displays the list of MAC addresses present in the AP provisioning lists.

### Controller GUI Security Settings

Although the settings are not directly related to the feature, it may help you in achieving the desired behavior with respect to APs provisioned with an LSC.

Figure 10-63 shows three possible cases for mesh AP MAC authorization and EAP.
Case 1—Local MAC Authorization and Local EAP Authentication
Add the MAC address of RAP/MAP to the controller MAC filter list.
Example:
```
config macfilter mac-delimiter colon
config macfilter add 00:0b:85:60:92:30 0 management
```

Case 2—External MAC Authorization and Local EAP authentication
Enter the following command on the WLC:
```
config mesh security rad-mac-filter enable
```
or
Check only the external MAC filter authorization on the GUI page and follow these guidelines:
- Do not add the MAC address of the RAP/MAP to the controller MAC filter list.
- Configure the external radius server details on the WLC.
- Enter the `config macfilter mac-delimiter colon` command configuration on the WLC.
- Add the MAC address of the RAP/MAP in the external radius server in the following format:
  ```
  ```

Case 3—External EAP authentication
Configure the external radius server details on the WLC and apply the following configuration on the controller:
```
config mesh radius-server index enable
config mesh security force-ext-auth enable
```
Add the user ID and password on the AAA server in the `<platform name string>-<Ethernet mac address hex string>` format for EAP Authentication.
If it is a Cisco IOS AP, it should be in the following format:

username: c1240-112233445566 and password: c1240-112233445566 for 1240 platform APs

username: c1520-112233445566 and password: c1520-112233445566 for 1520 platform APs

For 1510 VxWorks-based AP, it should be in the following format:

username: 112233445566 and password: 112233445566

Deployment Guidelines

- When using local authorization, the controller should be installed with the vendor’s CA and device certificate.
- When using an external AAA server, the controller should be installed with the vendor’s CA and device certificate.
- Mesh security should be configured to use ‘vendor’ as the cert-issuer.
- MAPs cannot move from an LSC to an MIC when they fall back to a backup controller.
- The config mesh lsc {enable | disable} command is required to enable or disable an LSC for mesh APs. This command causes all the mesh APs to reboot. Currently, disabling this command may also reboot nonmesh APs.

Slot Bias Options

This section contains the following topics:

- Information About Slot Bias Options, page 10-110
- Disabling Slot Bias, page 10-110
- Guidelines and Limitations, page 10-111
- Commands Related to Slot Bias, page 10-111

Information About Slot Bias Options

When a 1524SB AP is switched on, either slot 1 or slot 2 can be used for an uplink depending on the strength of the signal. AWPP treats both slots equally. For a MAP, slot 2 is the preferred (biased) uplink slot, that is, the slot that is used to connect to the parent AP. Slot 1 is the preferred downlink slot. When both radio slots are available for use and if slot 1 is used for an uplink backhaul, a 15-minute timer is started. At the end of 15 minutes, the AP scans for a channel in slot 2 so that slot 2 might be used for an uplink backhaul again. This process is called slot bias.

We recommend that you use a directional antenna on slot 2 for a proper linear functionality. We also recommend that you ensure that slot 2 is selected for a strong uplink. However, there may be some scenarios where directional antennas are used on both the backhaul radios for mobility. When the AP is powered on, the parent can be selected in either direction. If slot 1 is selected, the AP should not go to the scanning mode after 15 minutes, that is, you should disable the slot bias.

Disabling Slot Bias

You can use the config mesh slot-bias disable to disable slot bias so that the APs can be stable on slot 1.

To disable slot bias, enter this command:
Chapter 10      Controlling Mesh Access Points

Configuring Advanced Features

config mesh slot-bias disable

Note

The slot bias is enabled by default.

Guidelines and Limitations

- The **config mesh slot-bias disable** command is a global command and is applicable to all 1524SB APs associated with the same controller.
- Slot bias is applicable only when both slot 1 and slot 2 are usable. If a slot radio does not have a channel that is available because of dynamic frequency selection (DFS), the other slot takes up both the uplink and downlink roles.
- If slot 2 is not available because of hardware issues, slot bias functions normally. Take corrective action by disabling the slot bias or fixing the antenna.
- A 15-minute timer is initiated (slot bias) only when slot 1 and slot 2 are usable (have channels to operate).
- The 15-minute timer is not initiated if slot 2 cannot find any channels because of DFS, which results in slot 1 taking over the uplink and the downlink.
- Slot 2 takes over slot 1 if slot 1 does not have any channels to operate because of DFS.
- If slot 2 has a hardware failure, then slot bias is initiated, and slot 1 is selected for uplinking.
- Disabling slot bias enables you to take preventive action for a smooth operation.

Commands Related to Slot Bias

- To see which slot is being used for an uplink or a downlink, enter this command:

```
show mesh config
```

Mesh Range....................................... 12000
Mesh Statistics update period.................... 3 minutes
Backhaul with client access status.............. enabled
Backhaul with extended client access status..... disabled
Background Scanning State........................ enabled
Backhaul Amsdu State............................. enabled
Mesh Security
  Security Mode.................................. EAP
  External-Auth................................... disabled
  Use MAC Filter in External AAA server......... disabled
  Force External Authentication.................. disabled
Mesh Alarm Criteria
  Max Hop Count.................................. 4
  Recommended Max Children for MAP.............. 10
  Recommended Max Children for RAP.............. 20
  Low Link SNR.................................... 12
  High Link SNR.................................. 60
  Max Association Number......................... 10
  Association Interval................................ 60 minutes
  Parent Change Numbers......................... 3
  Parent Change Interval......................... 60 minutes
Mesh Multicast Mode.............................. In-Out
Mesh Full Sector DFS............................. enabled
Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
Mesh DCA channels for serial backhaul APs........ disabled
Mesh Slot Bias.................................... disabled
To verify that slot 1 is being used for an uplink, do the following:

a. Enable debugging on the AP by entering this command in the controller:
   
   ```
   debug ap enable AP_name
   ```

b. Enter these commands in the controller:

   ```
   debug ap command show mesh config AP_name
   debug ap command show mesh adjacency parent AP_name
   ```

**Preferred Parent Selection**

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

**Guidelines and Limitations**

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

**Note**

Slot bias and preferred parent selection features are independent of each other. However, with the preferred parent configured, the connection is made to the parent using slot 1 or slot 2, whichever the AP sees first. If slot 1 is selected for the uplink in a MAP, then slot bias occurs. We recommend that you disable slot bias if you already know that slot 1 is going to be selected.

**Configuring a Preferred Parent**

To configure a preferred parent, enter this command:

```
config mesh parent preferred AP_name MAC
```

where:

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

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

```
config mesh parent preferred MAP1SB 00:24:13:0f:92:0f
```

### Related Commands

These commands are related to preferred parent selection:

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

  ```
  config mesh parent preferred AP_name none
  ```

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

  ```
  show ap config general AP_name
  ```

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

```
show ap config general MAP1SB
```

```
Cisco AP Identifier.............................. 9
Cisco AP Name..................................... MAP1SB
Country code..................................... US - United States
Regulatory Domain allowed by Country........... 802.11bg:-A 802.11a:-A
AP Country code.................................. US - United States
AP Regulatory Domain............................ 802.11bg:-A 802.11a:-A
Switch Port Number............................. 1
MAC Address..................................... 12:12:12:12:12:12
IP Address Configuration....................... DHCP
IP Address....................................... 209.165.200.225
IP NetMask....................................... 255.255.255.224
CAPWAP Path MTU.................................. 1485
Domain...........................................
Name Server.....................................
Telnet State..................................... Disabled
Ssh State........................................ Disabled
Cisco AP Location............................... default location
Cisco AP Group Name............................ default-group
Primary Cisco Switch Name...................... 4404
Primary Cisco Switch IP Address................ 209.165.200.230
Secondary Cisco Switch Name.....................
Secondary Cisco Switch IP Address............... Not Configured
Tertiary Cisco Switch Name...................... 4404
Tertiary Cisco Switch IP Address................ 3.3.3.3
Administrative State........................... ADMIN_ENABLED
Operation State................................. REGISTERED
Mirroring Mode................................. Disabled
AP Mode......................................... Local
Public Safety.................................... Global: Disabled, Local: Disabled
AP subMode...................................... WIPS
Remote AP Debug............................... Disabled
S/W Version.................................... 5.1.0.0
```
Co-Channel Interference

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

Viewing Mesh Statistics for a Mesh Access Point

This section describes how to use the controller GUI or CLI to view mesh statistics for specific mesh access points.

Note

You can modify the Statistics Timer interval setting on the All APs > Details page of the controller GUI.

Viewing Mesh Statistics for a Mesh Access Point (GUI)

Step 1

Choose Wireless > Access Points > All APs to open the All APs page.
Step 2 To view statistics for a specific mesh access point, hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Statistics**. The **All APs > AP Name > Statistics** page for the selected mesh access point appears.

This page shows the role of the mesh access point in the mesh network, the name of the bridge group to which the mesh access point belongs, the backhaul interface on which the access point operates, and the number of the physical switch port. It also displays a variety of mesh statistics for this mesh access point.
### Table 10-17  Mesh Access Point Statistics

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mesh Node Stats</strong></td>
<td>Malformed Neighbor Packets</td>
<td>The number of malformed packets received from the neighbor. Examples of malformed packets include malicious floods of traffic such as malformed or short DNS packets and malformed DNS replies.</td>
</tr>
<tr>
<td></td>
<td>Poor Neighbor SNR Reporting</td>
<td>The number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.</td>
</tr>
<tr>
<td></td>
<td>Excluded Packets</td>
<td>The number of packets received from excluded neighbor mesh access points.</td>
</tr>
<tr>
<td></td>
<td>Insufficient Memory Reporting</td>
<td>The number of insufficient memory conditions.</td>
</tr>
<tr>
<td></td>
<td>Rx Neighbor Requests</td>
<td>The number of broadcast and unicast requests received from the neighbor mesh access points.</td>
</tr>
<tr>
<td></td>
<td>Rx Neighbor Responses</td>
<td>The number of responses received from the neighbor mesh access points.</td>
</tr>
<tr>
<td></td>
<td>Tx Neighbor Requests</td>
<td>The number of unicast and broadcast requests sent to the neighbor mesh access points.</td>
</tr>
<tr>
<td></td>
<td>Tx Neighbor Responses</td>
<td>The number of responses sent to the neighbor mesh access points.</td>
</tr>
<tr>
<td></td>
<td>Parent Changes Count</td>
<td>The number of times a mesh access point (child) moves to another parent.</td>
</tr>
<tr>
<td></td>
<td>Neighbor Timeouts Count</td>
<td>The number of neighbor timeouts.</td>
</tr>
<tr>
<td><strong>Queue Stats</strong></td>
<td>Gold Queue</td>
<td>The average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval.</td>
</tr>
<tr>
<td></td>
<td>Silver Queue</td>
<td>The average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval.</td>
</tr>
<tr>
<td></td>
<td>Platinum Queue</td>
<td>The average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval.</td>
</tr>
<tr>
<td></td>
<td>Bronze Queue</td>
<td>The average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval.</td>
</tr>
<tr>
<td></td>
<td>Management Queue</td>
<td>The average and peak number of packets waiting in the management queue during the defined statistics time interval.</td>
</tr>
<tr>
<td>Statistics</td>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mesh Node</td>
<td>Transmitted Packets</td>
<td>The number of packets transmitted during security negotiations by the selected mesh access point.</td>
</tr>
<tr>
<td></td>
<td>Received Packets</td>
<td>The number of packets received during security negotiations by the selected mesh access point.</td>
</tr>
<tr>
<td></td>
<td>Association Request</td>
<td>The number of association request failures that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Requests</td>
<td>The number of association request timeouts that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Successful</td>
<td>The number of successful association requests that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>The number of failed authentication requests that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Request Failures</td>
<td>The number of authentication request timeouts that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Requests</td>
<td>The number of authentication request timeouts that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Successful</td>
<td>The number of successful authentication requests between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Reassociation Request</td>
<td>The number of failed reassociation requests between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Failures</td>
<td>The number of reassociation request timeouts between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Requests</td>
<td>The number of reassociation request timeouts between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Successful</td>
<td>The number of successful reassociation requests between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Reauthentication</td>
<td>The number of failed reauthentication requests between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Request Failures</td>
<td>The number of reauthentication request timeouts that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Requests</td>
<td>The number of reauthentication request timeouts that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Successful</td>
<td>The number of successful reauthentication requests that occur between the selected mesh access point and its parent.</td>
</tr>
<tr>
<td></td>
<td>Unknown Association</td>
<td>The number of unknown association requests received by the parent mesh access point from its child. The unknown association requests</td>
</tr>
<tr>
<td></td>
<td>Requests</td>
<td>often occur when a child is an unknown neighbor mesh access point.</td>
</tr>
<tr>
<td></td>
<td>Invalid Association</td>
<td>The number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This</td>
</tr>
<tr>
<td></td>
<td>Requests</td>
<td>state may occur when the selected child is a valid neighbor but is not in a state that allows association.</td>
</tr>
</tbody>
</table>
Table 10-17  Mesh Access Point Statistics (continued)

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mesh Node Security Stats</td>
<td>Unknown Reauthentication Requests</td>
<td>The number of unknown reauthentication requests received by the parent mesh access point node from its child. This state may occur when a child mesh access point is an unknown neighbor.</td>
</tr>
<tr>
<td></td>
<td>Invalid Reauthentication Requests</td>
<td>The number of invalid reauthentication requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reauthentication.</td>
</tr>
<tr>
<td></td>
<td>Unknown Reassociation Requests</td>
<td>The number of unknown reassociation requests received by the parent mesh access point from a child. This state may occur when a child mesh access point is an unknown neighbor.</td>
</tr>
<tr>
<td></td>
<td>Invalid Reassociation Requests</td>
<td>The number of invalid reassociation requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reassociation.</td>
</tr>
</tbody>
</table>

Viewing Mesh Statistics for an Mesh Access Point (CLI)

Use these commands to view mesh statistics for a specific mesh access point using the controller CLI:

- To view packet error statistics, a count of failures, timeouts, and successes with respect to associations and authentications, and reassociations and reauthentications for a specific mesh access point, enter this command:

  `show mesh security-stats AP_name`

Information similar to the following appears:

```
AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
-------------------------------
  x Packets 14, Rx Packets 19, Rx Error Packets 0

Parent-Side Statistics:
-------------------------------
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0

Child-Side Statistics:
-------------------------------
Association Failures 0
Association Timeouts 0
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Assocation Failures 0
Re-Assocation Timeouts 0
```
To view the number of packets in the queue by type, enter this command:

```
show mesh queue-stats AP_name
```

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Queue Type</th>
<th>Overflows</th>
<th>Peak length</th>
<th>Average length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silver</td>
<td>0</td>
<td>1</td>
<td>0.000</td>
</tr>
<tr>
<td>Gold</td>
<td>0</td>
<td>4</td>
<td>0.004</td>
</tr>
<tr>
<td>Platinum</td>
<td>0</td>
<td>4</td>
<td>0.001</td>
</tr>
<tr>
<td>Bronze</td>
<td>0</td>
<td>0</td>
<td>0.000</td>
</tr>
<tr>
<td>Management</td>
<td>0 0</td>
<td>0</td>
<td>0.000</td>
</tr>
</tbody>
</table>

Overflows—The total number of packets dropped due to queue overflow.

Peak Length—The peak number of packets waiting in the queue during the defined statistics time interval.

Average Length—The average number of packets waiting in the queue during the defined statistics time interval.

**Viewing Neighbor Statistics for a Mesh Access Point**

This section describes how to use the controller GUI or CLI to view neighbor statistics for a selected mesh access point. It also describes how to run a link test between the selected mesh access point and its parent.

**Viewing Neighbor Statistics for a Mesh Access Point (GUI)**

1. Choose **Wireless > Access Points > All APs** to open the All APs page.

2. To view neighbor statistics for a specific mesh access point, hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Neighbor Information**. The All APs > Access Point Name > Neighbor Info page for the selected mesh access point appears.
Step 3  To perform a link test between the mesh access point and its parent or children, follow these steps:
   a. Hover the mouse over the blue drop-down arrow of the parent or desired child and choose **Link Test**. A pop-up window appears.
   b. Click **Submit** to start the link test. The link test results appear on the Mesh > Link Test Results page.
Chapter 10  Controlling Mesh Access Points

Configuring Advanced Features

Figure 10-69 Mesh > Link Test Results Page

Figure 10-70 All APs > Access Point Name > Link Details > Neighbor Name page

Step 4
To view the details for any of the mesh access points on this page, follow these steps:

a. Hover the mouse over the blue drop-down arrow for the desired mesh access point and choose Details. The All APs > Access Point Name > Link Details > Neighbor Name page appears.

b. Click Back to return to the All APs > Access Point Name > Neighbor Info page.

Step 5
To view statistics for any of the mesh access points on this page, follow these steps:

a. Hover the mouse over the blue drop-down arrow for the desired mesh access point and choose Stats. The All APs > Access Point Name > Mesh Neighbor Stats page appears.
Figure 10-71  All APs > Access Point Name > Mesh Neighbor Stats Page

b. Click Back to return to the All APs > Access Point Name > Neighbor Info page.

Viewing the Neighbor Statistics for a Mesh Access Point (CLI)

Use these commands to view neighbor statistics for a specific mesh access point using the controller CLI.

- To view the mesh neighbors for a specific mesh access point, enter this command:
  
  \[ \text{show mesh neigh \{detail | summary\} AP\_Name} \]

  Information similar to the following appears when you request a summary display:

<table>
<thead>
<tr>
<th>AP Name/Radio Mac</th>
<th>Channel</th>
<th>Snr-Up</th>
<th>Snr-Down</th>
<th>Link-Snr</th>
<th>Flags</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>mesh-45-rap1</td>
<td>165</td>
<td>15</td>
<td>18</td>
<td>16</td>
<td>0x86b</td>
<td>UPDATED NEIGH PARENT BEACON</td>
</tr>
<tr>
<td>00:0B:85:80:ED:D0</td>
<td>149</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>0x1a60</td>
<td>NEED UPDATE BEACON DEFAULT</td>
</tr>
<tr>
<td>00:17:94:FE:C3:5F</td>
<td>149</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0x860</td>
<td>BEACON</td>
</tr>
</tbody>
</table>

- To view the channel and signal-to-noise ratio (SNR) details for a link between a mesh access point and its neighbor, enter this command:
  
  \[ \text{show mesh path AP\_Name} \]

  Information similar to the following appears:

<table>
<thead>
<tr>
<th>AP Name/Radio Mac</th>
<th>Channel</th>
<th>Snr-Up</th>
<th>Snr-Down</th>
<th>Link-Snr</th>
<th>Flags</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>mesh-45-rap1</td>
<td>165</td>
<td>15</td>
<td>18</td>
<td>16</td>
<td>0x86b</td>
<td>UPDATED NEIGH PARENT BEACON</td>
</tr>
<tr>
<td>00:0B:85:80:ED:D0</td>
<td>149</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>0x1a60</td>
<td>NEED UPDATE BEACON DEFAULT</td>
</tr>
<tr>
<td>00:17:94:FE:C3:5F</td>
<td>149</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0x860</td>
<td>BEACON</td>
</tr>
</tbody>
</table>

- To view the percentage of packet errors for packets transmitted by the neighbor mesh access point, enter this command:
  
  \[ \text{show mesh per-stats AP\_Name} \]

  Information similar to the following appears:

  Neighbor MAC Address 00:0B:85:80:ED:D0
  Total Packets transmitted: 104833
  Total Packets transmitted successfully: 104833
  Total Packets retried for transmission: 33028

  Neighbor MAC Address 00:0B:85:80:ED:D0
  Total Packets transmitted: 0
  Total Packets transmitted successfully: 0
  Total Packets retried for transmission: 0
Packet error rate percentage = 1 – (number of successfully transmitted packets/number of total packets transmitted).

Converting Indoor Access Points to Mesh Access Points

**Step 1** Convert the autonomous access point (k9w7 image) to a lightweight access point.

For information about this process, see this URL: http://cisco-images.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html.

**Step 2** Convert the lightweight access point to either a mesh access point (MAP) or root access point (RAP) as follows:

**Note** Indoor mesh access points (1130 and 1240) can function as either a RAP or a MAP. By default, all are configured as MAPs.

- To convert the access point to a mesh access point using the controller CLI, perform one of the following:
  - To convert from a lightweight access point to a MAP, enter this command:
    ```
    config ap mode bridge Cisco_AP
    ```
    The mesh access point reloads.
  - To convert from a lightweight access point to a RAP, enter these CLI commands:
    ```
    config ap mode bridge Cisco_AP
    config ap role rootAP Cisco_AP
    ```
    The mesh access point reloads and is configured to operate as a RAP.

- To convert the access point to a mesh access point using the GUI, follow these steps:
  a. Choose Wireless and click on the AP Name link for the 1130 or 1240 indoor access point you want to convert.
  b. At the General Properties panel, choose Bridge from the AP Mode drop-down list.
     The access point reboots.
  c. At the Mesh panel, choose either RootAP or MeshAP from the AP Role drop-down list.
  d. Click Apply to commit your changes.
  e. Click Save Configuration to save your changes.

Changing MAP and RAP Roles for Indoor Mesh Access Points

Cisco 1130 and 1240 series indoor mesh access points can function as either RAPs or MAPs.
Changing MAP and RAP Roles for Indoor Mesh Access Points (GUI)

**Step 1** Choose **Wireless > Access Points > All APs** to open the All APs page.

**Step 2** Click the name of the 1130 or 1240 series access point that you want to change.

**Step 3** Click the **Mesh** tab.

**Step 4** From the AP Role drop-down list, choose **MeshAP** or **RootAP** to specify this access point as a MAP or RAP, respectively.

**Step 5** Click **Apply** to commit your changes. The access point reboots.

**Step 6** Click **Save Configuration** to save your changes.

---

**Note**

We recommend that you use a Fast Ethernet connection between the MAP and controller when changing from a MAP to RAP.

---

**Note**

After a RAP-to-MAP conversion, the MAP’s connection to the controller is a wireless backhaul rather than a Fast Ethernet connection. You must ensure that the Fast Ethernet connection of the RAP being converted is disconnected before the MAP starts up so that the MAP can join over the air.

---

**Note**

We recommend that your power source for MAPs is either a power supply or power injector. We do not recommend that you use PoE as a power source for MAPs.

---

Changing MAP and RAP Roles for Indoor Mesh Access Points (CLI)

**Step 1** Change the role of an indoor access point from MAP to RAP or from RAP to MAP by entering this command:

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

The access point reboots after you change the role.

**Step 2** Save your changes by entering this command:

```
save config
```

Converting Indoor Mesh Access Points to Nonmesh Lightweight Access Points (1130AG, 1240AG)

The access point reboots after you enter the conversion commands in the controller CLI or perform the steps on the controller or the Cisco WCS.
Note We recommend that you use a Fast Ethernet connection to the controller for the conversion from a mesh (bridge) to nonmesh (local) access point. If the backhaul is a radio, after the conversion, you must enable Ethernet and then reload the access image.

Note When a root access point is converted back to a lightweight access point, all of its subordinate mesh access points lose connectivity to the controller. A mesh access point is unable to service its clients until the mesh access point is able to connect to a different root access point in the vicinity. Likewise, clients might connect to a different mesh access point in the vicinity to maintain connectivity to the network.

- To convert an indoor mesh access point (MAP or RAP) to a nonmesh lightweight access point using the controller CLI, enter this command.
  
  `config ap mode local Cisco_AP`

  The access point reloads.

- To convert an indoor mesh access point (MAP or RAP) to a nonmesh lightweight access point using the GUI, follow these steps:
  a. Choose Wireless and click on the AP Name link for the 1130 or 1240 indoor access point you want to convert.
  b. At the General Properties panel, choose Local from the AP Mode drop-down list.
  c. Click Apply to apply changes.
  d. Click Save Configuration to save your changes.

- To convert an indoor mesh access point (MAP or RAP) to a nonmesh lightweight access point using Cisco WCS, follow these steps:
  a. Choose Configure > Access Points and click on the AP Name link for the 1130 or 1240 indoor access point you want to convert.
  b. At the General Properties panel, choose Local as the AP Mode (left side).
  c. Click Save.

Configuring Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers

Outdoor access points (1522, 1524PS) can interoperate with the Cisco 3200 Series Mobile Access Router (MAR) on the public safety channel (4.9 GHz) as well as the 2.4-GHz access and 5-GHz backhaul.

The Cisco 3200 creates an in-vehicle network in which devices such as PCs, surveillance cameras, digital video recorders, printers, PDAs, and scanners can share wireless networks such as cellular or WLAN-based services back to the main infrastructure. Data that is collected from in-vehicle deployments, such
as a police car can be integrated into the overall wireless infrastructure. For specific interoperability
details between series 1130, 1240, and 1520 mesh access points and series 3200 mobile access routers,
see Table 10-18.

### Guidelines and Limitations

- Client access must be enabled on the backhaul (Mesh global parameter).
- Public Safety must be enabled globally on all mesh access points (MAPs) in the mesh network.
- Channel number assignments on the 1522 or 1524PS must match those on the Cisco 3200 radio
  interfaces:
  - Channels 20 (4950 GHz) through 26 (4980 GHz) and sub-band channels 1 through 19 (5 and 10
    MHz) are used for MAR interoperability. This configuration change is made on the controller.
    No changes are made to the access point configuration.
  - Channel assignments are made only to the RAP. Updates to the MAP are propagated by the RAP.
  - Cisco MAR 3200s can scan channels within but not across the 5-, 10-, or 20-MHz bands.

### Enabling Mesh Access Points to Operate with Cisco 3200 Series Mobile Access
Routers (GUI)

#### Step 1
Enable the backhaul for client access by choosing **Wireless > Mesh** to open the Mesh page.

#### Step 2
Select the **Backhaul Client Access** check box to allow wireless client association over the 802.11a radio.
Step 3  Click **Apply** to commit your changes.

Step 4  When prompted to allow a reboot of all the mesh access points on the network, click **OK**.

Step 5  Choose **Wireless > Access Points > Radios > 802.11a/n** to open the 802.11a/n Radios page.

Step 6  Hover your cursor over the blue drop-down arrow for the appropriate RAP and choose **Configure**. The 802.11a/n (4.9 GHz) > Configure page appears.

**Figure 10-72  802.11 a/n (4.9GHz) > Configure Page**

Step 7  Under the RF Channel Assignment section, choose the **WLC Controlled** option for Assignment Method and choose a channel between 1 and 26.

Step 8  Click **Apply** to commit your changes.

Step 9  Click **Save Configuration** to save your changes.

---

**Enabling Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers (CLI)**

Step 1  Enable client access mode on the 1522 and 1524PS mesh access points by entering this command:

```
config mesh client-access enable
```

Step 2  Enable public safety on a global basis by entering this command:

```
config mesh public-safety enable all
```

Step 3  Enable the public safety channels by entering these commands:

- For the 1522 access point, enter these commands:

```
config 802.11a disable Cisco_MAP
```
config 802.11a channel ap Cisco_MAP channel_number
config 802.11a enable Cisco_MAP

• For the 1524PS, enter these commands:
  config 802.11–a49 disable Cisco_MAP
  config 802.11–a49 channel ap Cisco_MAP channel_number
  config 802.11–a49 enable Cisco_MAP

Note  Enter the config 802.11–a58 enable Cisco_MAP command to enable a 5-GHz radio.

Note  For both the 1522 and 1524PS mesh access points, valid values for the channel number is 1 through 26.

Step 4  Save your changes by entering this command:
  save config

Step 5  Verify your configuration by entering these commands:
  show mesh public-safety
  show mesh client-access
  show ap config 802.11a summary (for 1522 access points only)
  show ap config 802.11–a49 summary (for 1524PS access points only)

Note  Enter the show config 802.11-a58 summary command to view configuration details for a 5-GHz radio.
Managing Controller Software and Configurations

This chapter contains these sections:
- Upgrading the Controller Software, page 11-1
- Predownloading an Image to an Access Point, page 11-10
- Transferring Files to and from a Controller, page 11-15
- Saving Configurations, page 11-33
- Editing Configuration Files, page 11-34
- Clearing the Controller Configuration, page 11-35
- Erasing the Controller Configuration, page 11-35
- Resetting the Controller, page 11-36

Upgrading the Controller Software

This section contains the following topics:
- Information About Upgrading the Controller Software, page 11-1
- Guidelines and Limitations, page 11-2
- Upgrading Controller Software, page 11-5

Information About Upgrading the Controller Software

When you upgrade the controller’s software, the software on the controller’s associated access points is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession. Up to 10 access points can be concurrently upgraded from the controller.

Note
The Cisco 5500 Series Controllers can download the 6.0 software to 100 access points simultaneously.
Upgrading the Controller Software

Caution
Do not power down the controller or any access point during this process; otherwise, you might corrupt the software image. Upgrading a controller with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported in software release 4.0.206.0 and later releases, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Note
In controller software release 5.2 or later releases, the WLAN override feature is not available from both the controller GUI and CLI. If your controller is configured for WLAN override and you upgrade to controller software release 5.2 or later releases, the controller deletes the WLAN configuration and broadcasts all WLANs. You can specify that only certain WLANs be transmitted by configuring access point groups. Each access point advertises only the enabled WLANs that belong to its access point group.

Guidelines and Limitations

- Ensure that you have a TFTP or FTP server available for the software upgrade. Follow these guidelines when setting up a TFTP or FTP server:
  - Controller software release 6.0 is greater than 32 MB; you must make sure that your TFTP server supports files that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd32 and the TFTP server is within WCS. If you attempt to download the 6.0 controller software and your TFTP server does not support files of this size, the following error message appears: “TFTP failure while storing in flash.”
  - If you are upgrading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.
- You can upgrade or downgrade the controller software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to software release 6.0. shows the upgrade path that you must follow prior to downloading software release 6.0.
- The Cisco 5500 Series Controllers can run only controller software release 6.0 or later releases.
- When you upgrade the controller to an intermediate software release, wait until all of the access points joined to the controller are upgraded to the intermediate release before you install the 6.0 software. In large networks, it may take some time to download the software on each access point.
- In software releases 6.0.186.0 and later releases, you can download the upgrade image to the controller, and then download the image to the access points while the network is still up. New CLI and controller GUI functionality allow you to specify the boot image for both devices and to reset the access points when the controller resets. When both devices are up, the access points discover and rejoin the controller. See the “Predownloading an Image to an Access Point” section on page 11-10 for more information about predownloading images to access points.
We recommend that you install the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file on all controller platforms. This file resolves CSCsm03461 and is necessary to view the version information for ER.aes files in the output of the `show sysinfo` command. If you do not install this ER.aes file, your controller does not obtain the fix for this defect, and “N/A” appears in the text box Recovery Image Version or Emergency Image Version text box in the output of this command.

You cannot install the Cisco Unified Wireless Network Controller Boot Software 7.0.116.0 ER.aes file on Cisco 5500 Controller platform.

The ER.aes files are independent from the controller software files. You can run any controller software file with any ER.aes file. However, installing the latest boot software file (7.0.116.0 ER.aes) ensures that the boot software modifications in all of the previous and current boot software ER.aes files are installed.

If you require a downgrade from one release to another, you may lose the configuration from your current release. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.

Do not upgrade a controller using a wireless client as the TFTP or FTP server if the client is associated to the same controller that is being upgraded. If you try upgrading a Wireless LAN Controller using an associated client, the upgrade will fail. The controller will not attempt to contact the TFTP server to download the image. The TFTP server can be located on a client that is not associated to the same controller to which it is associated. This is applicable on all controller platforms.

Ensure that you comply with the following rules before you upgrade your controller in a mesh network:

- You can upgrade from all mesh releases to controller software release 6.0 without any configuration file loss. See Table 11-1 for the available upgrade paths.

**Note** If you downgrade to a mesh release, you must then reconfigure the controller. We recommend that you save the configuration from the mesh release before upgrading to release 6.0 for the first time. You can reapply the configuration if you need to downgrade.

- You cannot downgrade from controller software release 6.0 to a mesh release (4.1.190.5, 4.1.191.22M, or 4.1.192.xxM) without experiencing a configuration loss.

- Predownloading a 7.2 or later version of an image on a Cisco Aironet 1240 access point is not supported when upgrading from a previous controller release. If predownloading is attempted to the Cisco Aironet 1240 access point, the AP gets disconnected.

- Configuration files are in the binary state immediately after upgrade from a mesh release to controller software release 6.0. After reset, the XML configuration file is selected.

- Do not edit XML files.

### Table 11-1 Upgrade Compatibility Matrix for Controller Mesh and Non-Mesh Releases

<table>
<thead>
<tr>
<th>Upgrade to 6.0</th>
<th>4.1.192.35M</th>
<th>4.1.192.36M</th>
<th>4.1.192.37M</th>
<th>4.1.192.38M</th>
<th>4.1.192.39M</th>
<th>4.1.192.40M</th>
<th>4.1.192.41M</th>
<th>4.1.192.42M</th>
<th>4.1.192.43M</th>
<th>4.1.192.44M</th>
<th>4.1.192.45M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade from</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.192.35M</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cisco Wireless LAN Controller Configuration Guide
### Table 11-1 Upgrade Compatibility Matrix for Controller Mesh and Non-Mesh Releases (continued)

| Upgrade to | 6.0 | 5.2 | 4.1.191.24M | 4.1.190.5 | 4.1.185.0 | 4.1.181.0 | 4.1.171.0 | 4.0.219.0 | 4.0.217.204 | 4.0.217.0 | 4.0.216.0 | 4.0.206.0 | 4.0.179.11 | 4.0.179.8 | 4.0.155.5 | 4.0.155.0 | 3.2.195.10 | 3.2.193.5 | 3.2.171.6 | 3.2.171.5 | 3.2.150.10 | 3.2.150.6 |
|------------|-----|-----|-------------|-----------|-----------|-----------|-----------|-----------|-------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| 4.1.192.22M| Y   | Y   | Y           |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.1.191.24M| Y   | –   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.1.190.5  | Y   | Y   | –           |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.1.185.0  | Y   | Y   | –           |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.1.181.0  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.1.171.0  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.0.219.0  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.0.217.204| Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.0.217.0  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.0.216.0  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.0.206.0  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.0.179.11 | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.0.179.8  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.0.155.5  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 4.0.155.0  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 3.2.195.10 | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 3.2.193.5  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 3.2.171.6  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 3.2.171.5  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 3.2.150.10 | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
| 3.2.150.6  | Y   | Y   |             |           |           |           |           |           |              |           |           |           |           |           |           |           |           |           |           |           |           |           |
Upgrading Controller Software

Note
Do not install the 6.0 controller software file and the 5.2.157.0 ER.aes boot software file at the same time. Install one file and reboot the controller and then install the other file and reboot the controller.

This section contains the following topics:

- Upgrading Controller Software (GUI), page 11-5
- Upgrading Controller Software (CLI), page 11-7

Upgrading Controller Software (GUI)

Step 1
Upload your controller configuration files to a server to back them up.

Note
We highly recommend that you back up the configuration files of the controller before you upgrade the controller software. See the “Uploading and Downloading Configuration Files” section on page 11-28 for instructions.

Step 2
Obtain the 6.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file from the Software Center on Cisco.com as follows:

- Click this URL to go to the Software Center:
b. Choose Wireless Software.

c. Choose Wireless LAN Controllers.

d. Choose Standalone Controllers or Integrated Controllers and Controller Modules.

e. Choose a controller series.

f. If necessary, choose a controller model.

g. If you chose Standalone Controllers in Step d., choose Wireless LAN Controller Software.

h. If you chose the Cisco Catalyst 6500 series switch 7600 Series Wireless Services Module (WiSM) in Step e., choose Wireless Services Modules (WiSM) Software.

i. Choose a controller software release. The software releases are labeled as follows to help you determine which release to download:

   • Early Deployment (ED)—These software releases provide new features, new hardware platform support, and bug fixes.

   • Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.

   • Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

j. Choose a software release number.

k. Click the filename (filename.aes).

l. Click Download.

m. Read Cisco’s End User Software License Agreement and then click Agree.

n. Save the file to your hard drive.

o. Repeat steps a. through n. to download the remaining file (either the 6.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 3 Copy the controller software file (filename.aes) and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file to the default directory on your TFTP or FTP server.

Step 4 Disable the controller 802.11a and 802.11b/g networks.

Step 5 Disable any WLANs on the controller.

Step 6 Choose Commands > Download File to open the Download File to Controller page.

Figure 11-1  Download File to Controller Page

Step 7 From the File Type drop-down list, choose Code.
Step 8  From the Transfer Mode drop-down list, choose TFTP or FTP.

Step 9  In the IP Address text box, enter the IP address of the TFTP or FTP server.

   If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

Step 10 Enter the maximum number of times that the TFTP server attempts to download the software in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the software in the Timeout text box.

Step 11 In the File Path text box, enter the directory path of the software.

Step 12 In the File Name text box, enter the name of the controller software file (filename.aes).

Step 13 If you are using an FTP server, follow these steps:

   a. In the Server Login Username text box, enter the username to log into the FTP server.

   b. In the Server Login Password text box, enter the password to log into the FTP server.

   c. In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 14 Click Download to download the software to the controller. A message appears indicating the status of the download.

   Note  You can schedule a reboot at a specified time. See “Setting a Reboot Time” section on page 11-14.

Step 15 To install the remaining file (either the 6.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 16 Reenable the WLANs.

Step 17 For Cisco WiSMs, reenable the controller port channel on the Catalyst switch.

Step 18 Reenable your 802.11a and 802.11b/g networks.

Step 19 (Optional) Reload your latest configuration file to the controller.

Step 20 Verify that the 6.0 controller software is installed on your controller by choosing Monitor on the controller GUI and looking at the Software Version text box under Controller Summary.

Step 21 Verify that the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file is installed on your controller by choosing Monitor to open the Summary page and looking at the text box Recovery Image Version or Emergency Image Version text box.

   Note  If a Cisco Unified Wireless Network Controller Boot Software ER.aes file is not installed, the text box Recovery Image Version or Emergency Image Version text box shows “N/A.”

Upgrading Controller Software (CLI)

Step 1  Upload your controller configuration files to a server to back them up.
Upgrading the Controller Software

We highly recommend that you back up the configuration files of the controller before you upgrade the controller software. See the “Uploading and Downloading Configuration Files” section on page 11-28 for instructions.

**Step 2** Obtain the 6.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file from the Software Center on Cisco.com as follows:

a. Click this URL to go to the Software Center:
   

b. Choose Wireless Software.

c. Choose Wireless LAN Controllers.


e. Choose the name of a controller.

f. Choose Wireless LAN Controller Software.

g. Choose a controller software release.

h. Click the filename (filename.aes).

i. Click Download.

j. Read Cisco’s End User Software License Agreement and then click Agree.

k. Save the file to your hard drive.

l. Repeat steps a. to k. to download the remaining file (either the 6.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

**Step 3** Copy the controller software file (filename.aes) and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file to the default directory on your TFTP or FTP server.

**Step 4** Disable the controller 802.11a and 802.11b/g networks.

**Step 5** For Cisco WiSMs, shut down the controller port channel on the Catalyst switch to allow the controller to reboot before the access points start downloading the software.

**Step 6** Disable any WLANs on the controller (using the `config wlan disable wlan_id` command).

**Step 7** Log into the controller CLI.

**Step 8** Enter the `ping server-ip-address` command to verify that the controller can contact the TFTP or FTP server.

**Step 9** View current download settings by entering the `transfer download start` command. Answer n to the prompt to view the current download settings.

Information similar to the following appears:

```
Mode:........................................... TFTP
Data Type:........................................ Code
TFTP Server IP:................................. xxx.xxx.xxx.xxx
TFTP Packet Timeout:......................... 6
TFTP Max Retries:............................. 10
TFTP Path:...................................... <directory path>
TFTP Filename:............................... xxx.aes

This may take some time.
Are you sure you want to start? (y/N) n
Transfer Canceled
```
**Step 10**

Change the download settings, if necessary by entering these commands:

- `transfer download mode {tftp | ftp}
- `transfer download datatype code
- `transfer download serverip server-ip-address
- `transfer download filename filename
- `transfer download path server-path-to-file

**Note**

Pathnames on a TFTP or FTP server are relative to the server’s default or root directory. For example, in the case of the Solaris TFTP server, the path is “/”.

If you are using a TFTP server, also enter these commands:

- `transfer download tftpMaxRetries retries
- `transfer download tftpPktTimeout timeout

**Note**

The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the `retries` parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the `timeout` parameter.

If you are using an FTP server, also enter these commands:

- `transfer download username username
- `transfer download password password
- `transfer download port port

**Note**

The default value for the `port` parameter is 21.

**Step 11**

View the current updated settings by entering the `transfer download start` command. Answer `y` to the prompt to confirm the current download settings and start the software download.

Information similar to the following appears:

```
Mode........................................... TFTP
Data Type...................................... Code
TFTP Server IP.................................. xxx.xxx.xxx.xxx
TFTP Packet Timeout......................... 6
TFTP Max Retries.............................. 10
TFTP Path...................................... <directory path>
TFTP Filename.................................. xxx.aes

Are you sure you want to start? (y/n) y
TFTP Code transfer starting.
TFTP receive complete... extracting components.
Writing new bootloader to flash.
Making backup copy of RTOS.
Writing new RTOS to flash.
Making backup copy of Code.
Writing new Code to flash.
TFTP File transfer operation completed successfully.
Please restart the switch (reset system) for update to complete.
```
Predownloading an Image to an Access Point

This section contains the following topics:

- Information About Predownloading an Image to an Access Point, page 11-10
- Access Point Predownload Process, page 11-11
- Guidelines and Limitations, page 11-12
- Predownloading an Image to an Access Point, page 11-12

Information About Predownloading an Image to an Access Point

To minimize a network outages, you can now download an upgrade image to the access point from the controller without resetting the access point or losing network connectivity. Previously, you would download an upgrade image to the controller and reset it, which causes the access point to go into discovery mode. After the access point discovers the controller with the new image, the access point downloads the new image, resets, goes into discovery mode, and rejoins the controller.
You can now download the upgrade image to the controller and then download the image to the access point while the network is still up. You can also schedule a reboot of the controller and access points, either after a specified amount of time or at a specific date and time. When both devices are up, the access point discovers and rejoins the controller.

**Note**

These access point models do not support predownloading of images: 1120, 1230, and 1310.

---

### Access Point Predownload Process

The access point predownload feature works as below:

- The controller image is downloaded.
  - The downloaded image becomes the backup image on the controller. Change the current boot image as the backup image using the `config boot backup` command. This ensures that if a system failure occurs, the controller boots with the last working image of the controller.
  - User predownloads the upgraded image using the `config ap image predownload primary all` command. The upgrade image gets downloaded as the backup up image on the access points. This can be verified using the `show ap image all` command.
  - User manually changes the boot image to primary using `config boot primary` command and reboot the controller for the upgrade image to get activated.
    - or
  - User issues scheduled reboot with `swap` keyword. For more information see “Setting a Reboot Time” section on page 11-14. Here the `swap` keyword has the following importance: The swapping happens to the primary and backup images on access point, and the currently active image on controller with the backup image.
  - When the controller reboots, the access points get disassociated and eventually they come up with upgrade image. Once the controller responds to the discovery request sent by access points with its discovery response packet, the access point sends a join request.

- The actual upgrade of the images occur. The following sequence of actions occur.
  - During boot time, the access point sends a join request.
  - Controller responds with the join response along with the image version the controller is running.
  - The access point compares its running image with the running image on the controller. If the versions match, the access point joins the controller.
  - If the versions do not match, the access point compares the version of the backup image and if they match, the access point swaps the primary and backup images and reloads and subsequently joins the controller.
  - If the primary image of the access point is the same as the controllers’, the access point reloads and joins the controller.
  - If none of the above conditions are true, the access point sends an image data request to the controller, downloads the latest image, reloads and joins the controller.
Guidelines and Limitations

- The maximum number of concurrent predownloads is limited to half the number of concurrent normal image downloads. This limitation allows new access points to join the controller during image downloading.

  If you reach the predownload limit, then the access points that cannot get an image sleep for a time between 180 to 600 seconds and then reattempt the predownload.

- Before you enter the predownload command, you should change the active controller boot image to the backup image. This step ensures that if the controller reboots for some reason, it comes back up with the earlier running image, not the partially downloaded upgrade image.

- Access points with 16-MB total available memory (1130 and 1240 access points) may not have enough free memory to download an upgrade image and may automatically delete crash info files, radio files, and any backup images to free up space. However, this limitation does not affect the predownload process because the predownload image replaces any backup image on the access point.

- When the system time is changed by using the `config time` command, the time set for scheduled reset will not be valid and the scheduled system reset will be canceled. You are given an option either to cancel the scheduled reset before configuring the time or retain the scheduled reset and not configure the time.

- All the primary, secondary, and tertiary controllers should run the same images as the primary and backup images. That is, the primary image of all three controllers should be X and the secondary image of all three controllers should be Y or the feature will not be effective.

- At the time of the reset, if any AP is downloading the controller image, the scheduled reset is canceled. The following message appears with the reason why the scheduled reset was canceled:

  ```
  %OSAPI-3-RESETSYSTEM_FAILED: osapi_task.c:4458 System will not reset as software is being upgraded.
  ```

Predownloading an Image to an Access Point

This section contains the following topics:

- Configuring Predownload Image to Access Points- Global Configuration (GUI), page 11-12
- Predownloading an Image to Access Points (CLI), page 11-13

Configuring Predownload Image to Access Points- Global Configuration (GUI)

**Step 1**
Obtain the upgrade image and copy the image to the controller by performing Step 1 through Step 14 in the “Upgrading Controller Software (GUI)” section on page 11-5.

**Step 2**
To configure the predownloading of access point images globally, choose Wireless > Access Points > Global Configuration to open the Global Configuration page.

**Step 3**
In the AP Image Pre-download section, perform one of the following:

- To instruct all the access points to predownload a primary image from the controller, click Download Primary under the AP Image Pre-download.
- To instruct all the access points to swap their primary and backup images, click Interchange Image.
- To download an image from the controller and store it as a backup image, click Download Backup.
• To abort the predownload operation, click **Abort Predownload**.

**Step 4** Click **OK** to confirm the action.

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

---

### Configuring Predownload Image to an Access Point (GUI)

**Step 1** Obtain the upgrade image and copy the image to the controller by performing **Step 1** through **Step 14** in the “Upgrading Controller Software (GUI)” section on page 11-5.

**Step 2** To configure the predownloading of access point images globally, choose **Wireless > All APs > AP_Name** to open the All AP Details page.

**Step 3** Click the **Advanced** tab.

**Step 4** Under the AP Image download section, perform one of the following:

- To instruct this access point to predownload a primary image from the controller, click **Download Primary** under the AP Image Pre-download.
- To instruct this access point to swap their primary and backup images, click **Interchange Image**.
- To download an image from the controller and store it as a backup image, click **Download Backup**.
- To abort the predownload operation on this access point, click **Abort Predownload**.

**Step 5** Click **OK** to confirm the action.

**Step 6** Click **Apply** to commit your changes.

---

### Predownloading an Image to Access Points (CLI)

Using the CLI, you can predownload an image to a specific access point or to all access points. The process includes three steps:

1. Obtaining the upgrade image.
2. Specify access points that will receive the predownload image.
3. Set a reboot time for the controller and the access points.

**Obtaining the Upgrade Image**

To obtain the upgrade image and copy the image to the controller, follow **Step 1** through **Step 11** in the “Upgrading Controller Software (CLI)” section on page 11-7.

**Specifying Access Points for Predownload**

Use one of these commands to specify access points for predownload:

- Specify access points for predownload by entering this command:

  ```
  config ap image predownload {primary | backup} {ap_name | all}
  ```

  The primary image is the new image; the backup image is the existing image. Access points always boot with the primary image.
• Swap an access point’s primary and backup images by entering this command:

```bash
config ap image swap {ap_name | all}
```

• Display detailed information on access points specified for predownload by entering this command:

```bash
show ap image {all | ap-name}
```

Information similar to the following appears:

```
Total number of APs........................................ 7
Number of APs
  Initiated.................................................. 4
  Predownloading............................................ 0
  Completed predownloading............................... 3
  Not Supported............................................. 0
  Failed to Predownload.................................... 0
```

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Primary Image</th>
<th>Backup Image</th>
<th>Predownload Status</th>
<th>Predownload Version</th>
<th>Next Retry Time</th>
<th>Retry Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP1140-1</td>
<td>7.0.56.0</td>
<td>6.0.183.38</td>
<td>Complete</td>
<td>6.0.183.38</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>AP1140-2</td>
<td>7.0.56.0</td>
<td>6.0.183.58</td>
<td>Initiated</td>
<td>6.0.183.38</td>
<td>23:46:43</td>
<td>1</td>
</tr>
<tr>
<td>AP1130-2</td>
<td>7.0.56.0</td>
<td>6.0.183.38</td>
<td>Complete</td>
<td>6.0.183.38</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>AP1130-3</td>
<td>7.0.56.0</td>
<td>6.0.183.58</td>
<td>Initiated</td>
<td>6.0.183.38</td>
<td>23:43:25</td>
<td>1</td>
</tr>
<tr>
<td>AP1130-4</td>
<td>7.0.56.0</td>
<td>6.0.183.38</td>
<td>Complete</td>
<td>6.0.183.38</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>AP1130-5</td>
<td>7.0.56.0</td>
<td>6.0.183.58</td>
<td>Initiated</td>
<td>6.0.183.38</td>
<td>23:43:00</td>
<td>1</td>
</tr>
<tr>
<td>AP1130-6</td>
<td>7.0.56.0</td>
<td>6.0.183.58</td>
<td>Initiated</td>
<td>6.0.183.38</td>
<td>23:41:33</td>
<td>1</td>
</tr>
</tbody>
</table>

The output lists access points that are specified for predownloading and provides for each access point, primary and secondary image versions, the version of the predownload image, the predownload retry time (if necessary), and the number of predownload attempts. The output also includes the predownload status for each device. The status of the access points is as follows:

• None—The access point is not scheduled for predownload.
• Predownloading—The access point is predownloading the image.
• Not supported—The access point (1120, 1230, and 1310) does not support predownloading.
• Initiated—The access point is waiting to get the predownload image because the concurrent download limit has been reached.
• Failed—The access point has failed 64 predownload attempts.
• Complete—The access point has completed predownloading.

### Setting a Reboot Time

Use one of these commands to schedule a reboot of the controller and access points:

• Specify the amount of time delay before the devices reboot by entering this command:

```bash
reset system in HH:MM:SS image {swap | no-swap} reset-aps [save-config]
```

Note: The `swap` operand in the `reset` command will result in the swapping of the primary and backup images on both the controller and the access point.

The controller sends a reset message to all joined access points, and then the controller resets.

• Specify a date and time for the devices to reboot by entering this command:
**reset system at YYYY-MM-DD HH:MM:SS image {swap | no-swap} reset-aps [save-config]**

The controller sends a reset message to all joined access points, and then the controller resets.

**Note**
The `swap` operand in the `reset` command will result in the swapping of the primary and backup images on both the controller and the access point.

- Set up an SNMP trap message that announces the upcoming reset by entering this command:
  ```
  reset system notify-time minutes
  ```
  The controller sends the announcement trap *the configured number of minutes* before the reset.

- Cancel the scheduled reboot by entering this command:
  ```
  reset system cancel
  ```

**Note**
If you configure reset times and then use the `config time` command to change the system time on the controller, the controller notifies you that any scheduled reset times will be canceled and must be reconfigured after you set the system time.

Use the `show reset` command to display scheduled resets.

Information similar to the following appears:

```
System reset is scheduled for Apr 08 01:01:01 2010.
Current local time and date is Apr 07 02:57:44 2010.
A trap will be generated 10 minutes before each scheduled system reset.
Use 'reset system cancel' to cancel the reset.
Configuration will be saved before the system reset.
```

## Transferring Files to and from a Controller

Controllers have built-in utilities for uploading and downloading various files. Follow the instructions in these sections to import files using either the controller GUI or CLI:

- **Downloading a Login Banner File**, page 11-15
- **Downloading Device Certificates**, page 11-19
- **Downloading CA Certificates**, page 11-22
- **Uploading PACs**, page 11-25
- **Uploading and Downloading Configuration Files**, page 11-28

### Downloading a Login Banner File

This section contains the following topics:

- **Information About Downloading a Login Banner File**, page 11-16
- **Downloading a Login Banner File**, page 11-16
- **Clearing the Login Banner (GUI)**, page 11-18
Information About Downloading a Login Banner File

In controller software release 6.0 or later releases, you can download a login banner file using either the GUI or the CLI. The login banner is the text that appears on the page before user authentication when you access the controller GUI or CLI using Telnet, SSH, or a console port connection.

You save the login banner information as a text (*.txt) file. The text file cannot be larger than 1296 characters and cannot have more than 16 lines of text.

Note
The ASCII character set consists of printable and nonprintable characters. The login banner supports only printable characters.

Here is an example of a login banner:

> Welcome to the Cisco Wireless Controller!
> Unauthorized access prohibited.
> Contact sysadmin@corp.com for access.

Follow the instructions in this section to download a login banner to the controller through the GUI or CLI. However, before you begin, make sure that you have a TFTP or FTP server available for the file download. Follow these guidelines when setting up a TFTP or FTP server:

- If you are downloading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Note
Clearing the controller configuration does not remove the login banner. See the “Clearing the Login Banner (GUI)” section on page 11-18 for information about clearing the login banner using the controller GUI or CLI.

Note
The controller can have only one login banner file. If you download another login banner file to the controller, the first login banner file is overwritten.

Downloading a Login Banner File

This section contains the following topics:

- Downloading a Login Banner File (GUI), page 11-16
- Downloading a Login Banner File (CLI), page 11-17

Downloading a Login Banner File (GUI)

Step 1 Copy the login banner file to the default directory on your TFTP or FTP server.

Step 2 Choose Commands > Download File to open the Download File to Controller page.
Step 3  From the File Type drop-down list, choose Login Banner.

Step 4  From the Transfer Mode drop-down list, choose TFTP or FTP.

Step 5  In the IP Address text box, enter the IP address of the TFTP or FTP server.
        If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

Step 6  Enter the maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout text box.

Step 7  In the File Path text box, enter the directory path of the login banner file.

Step 8  In the File Name text box, enter the name of the login banner text (*.txt) file.

Step 9  If you are using an FTP server, follow these steps:
        a. In the Server Login Username text box, enter the username to log into the FTP server.
        b. In the Server Login Password text box, enter the password to log into the FTP server.
        c. In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 10 Click Download to download the login banner file to the controller. A message appears indicating the status of the download.

---

**Downloading a Login Banner File (CLI)**

Step 1  Log into the controller CLI.

Step 2  Specify the transfer mode used to download the config file by entering this command:
        `transfer download mode {tftp | ftp}`

Step 3  Download the controller login banner by entering this command:
        `transfer download datatype login-banner`

Step 4  Specify the IP address of the TFTP or FTP server by entering this command:
        `transfer download serverip server-ip-address`
Step 5 Specify the name of the config file to be downloaded by entering this command:

`transfer download path server-path-to-file`

Step 6 Specify the directory path of the config file by entering this command:

`transfer download filename filename.txt`

Step 7 If you are using a TFTP server, enter these commands:

- `transfer download tftpMaxRetries retries`
- `transfer download tftpPktTimeout timeout`

| Note | The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the `retries` parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the `timeout` parameter. |

Step 8 If you are using an FTP server, enter these commands:

- `transfer download username username`
- `transfer download password password`
- `transfer download port port`

| Note | The default value for the `port` parameter is 21. |

Step 9 View the download settings by entering the `transfer download start` command. Answer `y` when prompted to confirm the current settings and start the download process.

Information similar to the following appears:

```
Mode............................................. TFTP
Data Type........................................ Login Banner
TFTP Server IP.................................. 10.10.10.10
TFTP Packet Timeout.............................. 6
TFTP Max Retries................................. 10
TFTP Path........................................ /
TFTP Filename.................................... banner.txt

This may take some time.
Are you sure you want to start? (y/N) y

TFTP Login Banner transfer starting.

TFTP receive complete... checking login banner.
Successfully installed new login banner file
```

### Clearing the Login Banner (GUI)

Step 1 Choose Commands > Login Banner to open the Login Banner page.
Transferring Files to and from a Controller

Step 2 Click **Clear**.
Step 3 When prompted, click **OK** to clear the banner.

To clear the login banner from the controller using the controller CLI, enter the `clear login-banner` command.

**Downloading Device Certificates**

This section contains the following topics:

- Information About Downloading Device Certificates, page 11-19
- Guidelines and Limitations, page 11-19
- Downloading Device Certificates, page 11-20

**Information About Downloading Device Certificates**

Each wireless device (controller, access point, and client) has its own device certificate. For example, the controller is shipped with a Cisco-installed device certificate. This certificate is used by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific device certificate, it must be downloaded to the controller.

*Note* See the “Configuring Local EAP” section on page 7-36 for information on configuring local EAP.

Follow the instructions in this section to download a vendor-specific device certificate to the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP or FTP server available for the certificate download.

**Guidelines and Limitations**

- If you are downloading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
Transferring Files to and from a Controller

- A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.
- All certificates downloaded to the controller must be in PEM format.

**Downloading Device Certificates**

This section contains the following topics:
- Downloading Device Certificates (GUI), page 11-20
- Downloading Device Certificates (CLI), page 11-21

**Downloading Device Certificates (GUI)**

**Step 1**  Copy the device certificate to the default directory on your TFTP or FTP server.

**Step 2**  Choose **Commands > Download File** to open the Download File to Controller page.

**Figure 11-4   Download File to Controller Page**

**Step 3**  From the File Type drop-down list, choose **Vendor Device Certificate**.

**Step 4**  In the Certificate Password text box, enter the password that was used to protect the certificate.

**Step 5**  From the Transfer Mode drop-down list, choose **TFTP** or **FTP**.

**Step 6**  In the IP Address text box, enter the IP address of the TFTP or FTP server.

If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

**Step 7**  Enter the maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout text box.

**Step 8**  In the File Path text box, enter the directory path of the certificate.

**Step 9**  In the File Name text box, enter the name of the certificate.

**Step 10**  If you are using an FTP server, follow these steps:

a. In the Server Login Username text box, enter the username to log into the FTP server.
b. In the Server Login Password text box, enter the password to log into the FTP server.
c. In the Server Port Number text box, enter the port number on the FTP server through which the
download occurs. The default value is 21.

Step 11 Click Download to download the device certificate to the controller. A message appears indicating the
status of the download.

Step 12 After the download is complete, choose Commands > Reboot > Reboot.

Step 13 If prompted to save your changes, click Save and Reboot.

Step 14 Click OK to confirm your decision to reboot the controller.

---

**Downloading Device Certificates (CLI)**

Step 1 Log on to the controller CLI.

Step 2 Specify the transfer mode used to download the config file by entering this command:

```
transfer download mode {tftp | ftp}
```

Step 3 Specify the type of the file to be downloaded by entering this command:

```
transfer download datatype eapdevcert
```

Step 4 Specify the certificate’s private key by entering this command:

```
transfer download certpassword password
```

Step 5 Specify the IP address of the TFTP or FTP server by entering this command:

```
transfer download serverip server-ip-address
```

Step 6 Specify the name of the config file to be downloaded by entering this command:

```
transfer download path server-path-to-file
```

Step 7 Specify the directory path of the config file by entering this command:

```
transfer download filename filename.pem
```

Step 8 If you are using a TFTP server, enter these commands:

- `transfer download tftpMaxRetries retries`
- `transfer download tftpPktTimeout timeout`

*Note* The default values of 10 retries and a 6-second timeout should work correctly without any
adjustment. However, you can change these values. To do so, enter the maximum number of
times that the TFTP server attempts to download the software for the `retries` parameter and the
amount of time (in seconds) that the TFTP server attempts to download the software for the
`timeout` parameter.

Step 9 If you are using an FTP server, enter these commands:

- `transfer download username username`
- `transfer download password password`
- `transfer download port port`
Step 10  View the updated settings by entering the `transfer download start` command. Answer `y` when prompted to confirm the current settings and start the download process.

Information similar to the following appears:

```
Mode........................................... TFTP
Data Type................................... Vendor Dev Cert
TFTP Server IP.............................. 10.10.10.4
TFTP Packet Timeout......................... 6
TFTP Max Retries............................... 10
TFTP Path................................... /tftpboot/
TFTP Filename................................ filename.pem
```

This may take some time.

Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.
Certificate installed.
Reboot the switch to use the new certificate.

Step 11  Reboot the controller by entering this command:
```
reset system
```

---

**Downloading CA Certificates**

This section contains the following topics:

- Information About Downloading CA Certificates, page 11-22
- Guidelines and Limitations, page 11-22
- Downloading CA Certificates, page 11-23

**Information About Downloading CA Certificates**

Controllers and access points have a Certificate Authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate may be used by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific CA certificate, it must be downloaded to the controller.

Note  See the “Configuring Local EAP” section on page 7-36 for information about configuring local EAP.

**Guidelines and Limitations**

- Ensure that you have a TFTP or FTP server available for the certificate download. Follow these guidelines when setting up a TFTP or FTP server:
- If you are downloading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

- All certificates downloaded to the controller must be in PEM format.

**Downloading CA Certificates**

This section contains the following topics:

- Downloading CA Certificates (GUI), page 11-23
- Downloading CA Certificates (CLI), page 11-24

**Downloading CA Certificates (GUI)**

**Step 1** Copy the CA certificate to the default directory on your TFTP or FTP server.

**Step 2** Choose Commands > Download File to open the Download File to Controller page.

**Step 3** From the File Type drop-down list, choose Vendor CA Certificate.

**Step 4** From the Transfer Mode drop-down list, choose TFTP or FTP.

**Step 5** In the IP Address text box, enter the IP address of the TFTP or FTP server.

If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

**Step 6** Enter the maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout text box.

**Step 7** In the File Path text box, enter the directory path of the certificate.

**Step 8** In the File Name text box, enter the name of the certificate.
Step 9  If you are using an FTP server, follow these steps:
   a. In the Server Login Username text box, enter the username to log into the FTP server.
   b. In the Server Login Password text box, enter the password to log into the FTP server.
   c. In the Server Port Number text box, enter the port number on the FTP server through which the
      download occurs. The default value is 21.

Step 10 Click **Download** to download the CA certificate to the controller. A message appears indicating the
 status of the download.

Step 11 After the download is complete, choose **Commands > Reboot > Reboot**.

Step 12 If prompted to save your changes, click **Save and Reboot**.

Step 13 Click **OK** to confirm your decision to reboot the controller.

### Downloading CA Certificates (CLI)

Step 1 Log on to the controller CLI.

Step 2 Specify the transfer mode used to download the config file by entering this command:

```
transfer download mode {tftp | ftp}
```

Step 3 Specify the type of the file to be downloaded by entering this command:

```
transfer download datatype eapdevcert
```

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:

```
transfer download serverip server-ip-address
```

Step 5 Specify the directory path of the config file by entering this command:

```
transfer download path server-path-to-file
```

Step 6 Specify the name of the config file to be downloaded by entering this command:

```
transfer download filename filename.pem
```

Step 7 If you are using a TFTP server, enter these commands:

- `transfer download tftpMaxRetries retries`
- `transfer download tftpPktTimeout timeout`

**Note** The default values of 10 retries and a 6-second timeout should work correctly without any
adjustment. However, you can change these values. To do so, enter the maximum number of
times that the TFTP server attempts to download the software for the `retries` parameter and the
amount of time (in seconds) that the TFTP server attempts to download the software for the
`timeout` parameter.

Step 8 If you are using an FTP server, enter these commands:

- `transfer download username username`
- `transfer download password password`
- `transfer download port port`
Note
The default value for the port parameter is 21.

**Step 9**
View the updated settings by entering the `transfer download start` command. Answer `y` when prompted to confirm the current settings and start the download process.

Information similar to the following appears:

```
Mode............................... TFTP
Data Type........................... Vendor CA Cert
TFTP Server IP..................... 10.10.10.4
TFTP Packet Timeout................ 6
TFTP Max Retries................... 10
TFTP Path........................../tftpboot/username/
TFTP Filename...................... filename.pem
```

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP CA cert transfer starting.
Certificate installed.
Reboot the switch to use the new certificate.

**Step 10**
Reboot the controller by entering the `reset system` command.

---

**Uploading PACs**

This section contains the following topics:

- Information About Uploading PACs, page 11-25
- Guidelines and Limitations, page 11-25
- Uploading PACs, page 11-26

---

### Information About Uploading PACs

Protected access credentials (PACs) are credentials that are either automatically or manually provisioned and used to perform mutual authentication with a local EAP authentication server during EAP-FAST authentication. When manual PAC provisioning is enabled, the PAC file is manually generated on the controller.

**Note**
See the “Configuring Local EAP” section on page 7-36 for information on configuring local EAP.

---

### Guidelines and Limitations

- Ensure you have a TFTP or FTP server available for the PAC upload. Follow these guidelines when setting up a TFTP or FTP server:
  - If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are uploading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.

- A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

**Uploading PACs**

This section contains the following topics:

- Uploading PACs (GUI), page 11-26
- Uploading PACs (CLI), page 11-27

**Uploading PACs (GUI)**

**Step 1** Choose **Commands > Upload File** to open the Upload File from Controller page.

**Figure 11-6 Upload File from Controller Page**

- **Step 2** From the File Type drop-down list, choose **PAC (Protected Access Credential)**.
- **Step 3** In the User text box, enter the name of the user who will use the PAC.
- **Step 4** In the Validity text box, enter the number of days for the PAC to remain valid. The default setting is zero (0).
- **Step 5** In the Password and Confirm Password text boxes, enter a password to protect the PAC.
- **Step 6** From the Transfer Mode drop-down list, choose **TFTP** or **FTP**.
- **Step 7** In the IP Address text box, enter the IP address of the TFTP or FTP server.
- **Step 8** In the File Path text box, enter the directory path of the PAC.
- **Step 9** In the File Name text box, enter the name of the PAC file. PAC files have a .pac extension.
- **Step 10** If you are using an FTP server, follow these steps:
  a. In the Server Login Username text box, enter the username to log into the FTP server.
  b. In the Server Login Password text box, enter the password to log into the FTP server.
c. In the Server Port Number text box, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 11 Click Upload to upload the PAC from the controller. A message appears indicating the status of the upload.

Step 12 Follow the instructions for your wireless client to load the PAC on your client devices. Make sure to use the password that you entered above.

### Uploading PACs (CLI)

1. Log on to the controller CLI.
2. Specify the transfer mode used to upload the config file by entering this command:
   ```
   transfer upload mode {tftp | ftp}
   ```
3. Upload a Protected Access Credential (PAC) by entering this command:
   ```
   transfer upload datatype pac
   ```
4. Specify the identification of the user by entering this command:
   ```
   transfer upload pac username validity password
   ```
5. Specify the IP address of the TFTP or FTP server by entering this command:
   ```
   transfer upload serverip server-ip-address
   ```
6. Specify the directory path of the config file by entering this command:
   ```
   transfer upload path server-path-to-file
   ```
7. Specify the name of the config file to be uploaded by entering this command:
   ```
   transfer upload filename manual.pac
   ```
8. If you are using an FTP server, enter these commands:
   ```
   * transfer upload username username
   * transfer upload password password
   * transfer upload port port
   ```
   **Note** The default value for the `port` parameter is 21.

9. View the updated settings by entering the `transfer upload start` command. Answer y when prompted to confirm the current settings and start the upload process.

Information similar to the following appears:

```
Mode.................. TFTP
TFTP Server IP........ 10.10.10.4
TFTP Path............... /tftpboot/username/
TFTP Filename........... manual.pac
Data Type................ PAC
PAC User................ username
PAC Validity............ 10 days
PAC Password............ password

Are you sure you want to start? (y/N) y
```
PAC transfer starting.

File transfer operation completed successfully.

Step 10  Follow the instructions for your wireless client to load the PAC on your client devices. Make sure to use the password that you entered above.

Uploading and Downloading Configuration Files

This section contains the following topics:

- Information About Uploading and Downloading Configuration Files, page 11-28
- Guidelines and Limitations, page 11-28
- Uploading Configuration Files, page 11-29
- Downloading Configuration Files, page 11-31

Information About Uploading and Downloading Configuration Files

We recommend that you upload your controller’s configuration file to a server to back it up. If you lose your configuration, you can then download the saved configuration to the controller.

Caution

Do not download a configuration file to your controller that was uploaded from a different controller platform.

In controller software release 4.2 or later releases, the controller’s bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in a binary format. Therefore, you cannot download a binary configuration file onto a controller running software release 4.2 or later releases. However, when you upgrade a controller from a previous software release to 4.2 or later releases, the configuration file is migrated and converted to XML.

Guidelines and Limitations

- Any CLI with an invalid value is filtered out and set to default by the XML validation engine. Validation occurs during bootup. A configuration may be rejected if the validation fails. A configuration may fail if you have an invalid CLI. For example, if you have a CLI where you try to configure a WLAN without adding appropriate commands to add the WLAN.

- A configuration may be rejected if the dependencies are not addressed. For example, if you try to configure dependent parameters without using the add command. The XML validation may succeed but the configuration download infrastructure will immediately reject the configuration with no validation errors.

- An invalid configuration can be verified by using the show invalid-config command. The show invalid-config command reports the configuration that is rejected by the controller either as part of download process or by XML validation infrastructure.

- Controller software release 5.2 or later releases enable you to read and modify the configuration file. See the “Editing Configuration Files” section on page 11-34 for details. Controller software releases prior to 5.2 do not allow configuration files to be modified. If you attempt to make changes to a 4.2,
5.0, or 5.1 configuration file and then download the file to a controller, the controller displays a cyclic redundancy checksum (CRC) error while it is rebooting and returns the configuration parameters to their default values.

**Uploading Configuration Files**

This section contains the following topics:

- Uploading Configuration Files (GUI), page 11-29
- Uploading Configuration Files (CLI), page 11-30

**Uploading Configuration Files (GUI)**

**Step 1**  
Choose **Commands > Upload File** to open the Upload File from Controller page.

**Figure 11-7  Upload File from Controller Page**

![Upload File from Controller Page](image)

**Step 2**  
From the File Type drop-down list, choose **Configuration**.

**Step 3**  
Encrypt the configuration file by selecting the **Configuration File Encryption** check box and entering the encryption key in the Encryption Key text box.

**Step 4**  
From the Transfer Mode drop-down list, choose **TFTP** or **FTP**.

**Step 5**  
In the IP Address text box, enter the IP address of the TFTP or FTP server.

**Step 6**  
In the File Path text box, enter the directory path of the configuration file.

**Step 7**  
In the File Name text box, enter the name of the configuration file.

**Step 8**  
If you are using an FTP server, follow these steps:

- In the Server Login Username text box, enter the username to log into the FTP server.
- In the Server Login Password text box, enter the password to log into the FTP server.
- In the Server Port Number text box, enter the port number on the FTP server through which the upload occurs. The default value is 21.

**Step 9**  
Click **Upload** to upload the configuration file to the TFTP or FTP server. A message appears indicating the status of the upload. If the upload fails, repeat this procedure and try again.
Uploading Configuration Files (CLI)

Step 1 Specify the transfer mode used to upload the configuration file by entering this command:
```
transfer upload mode {tftp | ftp}
```

Step 2 Specify the type of file to be uploaded by entering this command:
```
transfer upload datatype config
```

Step 3 Encrypt the configuration file by entering these commands:
```
   transfer encrypt enable
   transfer encrypt set-key key, where key is the encryption key used to encrypt the file.
```

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:
```
transfer upload serverip server-ip-address
```

Step 5 Specify the directory path of the configuration file by entering this command:
```
transfer upload path server-path-to-file
```

Step 6 Specify the name of the configuration file to be uploaded by entering this command:
```
transfer upload filename filename
```

Step 7 If you are using an FTP server, enter these commands to specify the username and password used to log into the FTP server and the port number through which the upload occurs:
```
   transfer upload username username
   transfer upload password password
   transfer upload port port
```

   Note The default value for the port parameter is 21.

Step 8 Initiate the upload process by entering this command:
```
transfer upload start
```

Step 9 When prompted to confirm the current settings, answer y.

Information similar to the following appears:
```
Mode............................................. TFTP
TFTP Server IP.................................. 10.10.10.4
TFTP Path........................................ Config/
TFTP Filename.................................... AS_4402_4_2_55_8_Config.xml
Data Type........................................ Config File
Encryption....................................... Disabled

*******************************************************************************
*** WARNING: Config File Encryption Disabled ***
*******************************************************************************

Are you sure you want to start? (y/N) y

File transfer operation completed successfully.

If the upload fails, repeat this procedure and try again.
**Transferring Files to and from a Controller**

**Chapter 11      Managing Controller Software and Configurations**

**Transferring Files to and from a Controller**

**Downloading Configuration Files**

This section contains the following topics:

- **Downloading Configuration Files (GUI), page 11-31**
- **Downloading Configuration Files (CLI), page 11-32**

**Downloading Configuration Files (GUI)**

**Step 1** Choose **Commands > Download File** to open the Download File to Controller page.

**Step 2** From the File Type drop-down list, choose **Configuration**.

**Step 3** If the configuration file is encrypted, select the **Configuration File Encryption** check box and enter the encryption key used to decrypt the file in the Encryption Key text box.

**Note** The key that you enter here should match the one entered during the upload process.

**Step 4** From the Transfer Mode drop-down list, choose **TFTP** or **FTP**.

**Step 5** In the IP Address text box, enter the IP address of the TFTP or FTP server.

If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

**Step 6** Enter the maximum number of times that the TFTP server attempts to download the configuration file in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the configuration file in the Timeout text box.

**Step 7** In the File Path text box, enter the directory path of the configuration file.

**Step 8** In the File Name text box, enter the name of the configuration file.

**Step 9** If you are using an FTP server, follow these steps:

a. In the Server Login Username text box, enter the username to log into the FTP server.
b. In the Server Login Password text box, enter the password to log into the FTP server.

c. In the Server Port Number text box, enter the port number on the FTP server through which the
download occurs. The default value is 21.

**Step 10** Click **Download** to download the file to the controller. A message appears indicating the status of the
download, and the controller reboots automatically. If the download fails, repeat this procedure and try
again.

---

**Downloading Configuration Files (CLI)**

***Note***
The controller does not support incremental configuration downloads. The configuration file contains all
mandatory commands (all interface address commands, mgmtuser with read-write permission
commands, and interface port or LAG enable or disable commands) required to successfully complete
the download. For example, if you download only the `config time ntp server index server_address`
command as part of the configuration file, the download fails. Only the commands present in the
configuration file are applied to the controller, and any configuration in the controller prior to the
download is removed.

---

**Step 1** Specify the transfer mode used to download the configuration file by entering this command:

```plaintext
transfer download mode {tftp | ftp}
```

**Step 2** Specify the type of file to be downloaded by entering this command:

```plaintext
transfer download datatype config
```

**Step 3** If the configuration file is encrypted, enter these commands:

- `transfer encrypt enable`
- `transfer encrypt set-key key`, where `key` is the encryption key used to decrypt the file

***Note***
The key that you enter here should match the one entered during the upload process.

**Step 4** Specify the IP address of the TFTP or FTP server by entering this command:

```plaintext
transfer download serverip server-ip-address
```

**Step 5** Specify the directory path of the configuration file by entering this command:

```plaintext
transfer download path server-path-to-file
```

**Step 6** Specify the name of the configuration file to be downloaded by entering this command:

```plaintext
transfer download filename filename
```

**Step 7** If you are using a TFTP server, enter these commands:

- `transfer download tftpMaxRetries retries`
- `transfer download tftpPktTimeout timeout`
Saving Configurations

Controllers contain two kinds of memory: volatile RAM and NVRAM. At any time, you can save the configuration changes from active volatile RAM to nonvolatile RAM (NVRAM) using one of these commands:

- **save config**—Saves the configuration from volatile RAM to NVRAM without resetting the controller.
- **reset system**—Prompts you to confirm that you want to save configuration changes before the controller reboots.
• **logout**—Prompts you to confirm that you want to save configuration changes before you log out.

## Editing Configuration Files

When you save the controller’s configuration, the controller stores it in XML format in flash memory. Controller software release 5.2 or later releases enable you to easily read and modify the configuration file by converting it to CLI format. When you upload the configuration file to a TFTP or FTP server, the controller initiates the conversion from XML to CLI. You can then read or edit the configuration file in a CLI format on the server. When you are finished, you download the file back to the controller, where it is reconverted to an XML format and saved.

### Step 1
Upload the configuration file to a TFTP or FTP server by performing one of the following:

- Upload the file using the controller GUI. Follow the instructions in the “Uploading Configuration Files (GUI)” section on page 11-29.
- Upload the file using the controller CLI. Follow the instructions in the “Uploading Configuration Files (CLI)” section on page 11-30.

### Step 2
Read or edit the configuration file on the server. You can modify or delete existing CLI commands and add new CLI commands to the file.

**Note**
To edit the configuration file, you can use either Notepad or WordPad on Windows or the VI editor on Linux.

### Step 3
Save your changes to the configuration file on the server.

### Step 4
Download the configuration file to the controller by performing one of the following:

- Download the file using the controller GUI. Follow the instructions in the “Downloading Configuration Files (GUI)” section on page 11-31.
- Download the file using the controller CLI. Follow the instructions in the “Downloading Configuration Files (CLI)” section on page 11-32.

The controller converts the configuration file to an XML format, saves it to flash memory, and then reboots using the new configuration. CLI commands with known keywords and proper syntax are converted to XML while improper CLI commands are ignored and saved to flash memory. Any CLI commands that have invalid values are replaced with default values. To see any ignored commands or invalid configuration values, enter this command:

`show invalid-config`

**Note**
You cannot execute this command after the `clear config` or `save config` command.

### Step 5
If the downloaded configuration contains a large number of invalid CLI commands, you might want to upload the invalid configuration to the TFTP or FTP server for analysis. To do so, perform one of the following:

- Upload the invalid configuration using the controller GUI. Follow the instructions in the “Uploading Configuration Files (GUI)” section on page 11-29 but choose **Invalid Config** from the File Type drop-down list in Step 2 and skip Step 3.
Clearing the Controller Configuration

Step 1 Clear the configuration by entering this command:

```
clear config
```
Enter y at the confirmation prompt to confirm the action.

Step 2 Reboot the system by entering this command:

```
reset system
```
Enter n to reboot without saving configuration changes. When the controller reboots, the configuration wizard starts automatically.

Step 3 Follow the instructions in the “Configuring the Controller Using the GUI Configuration Wizard” section on page 3-1 to complete the initial configuration.

Erasing the Controller Configuration

Step 1 Reset the configuration by entering this command:

```
reset system
```
At the confirmation prompt, enter y to save configuration changes to NVRAM. The controller reboots.

Step 2 When you are prompted for a username, restore the factory-default settings by entering this command:

```
recover-config
```
The controller reboots and the configuration wizard starts automatically.

Step 3 Follow the instructions in the “Configuring the Controller Using the GUI Configuration Wizard” section on page 3-1 to complete the initial configuration.
Resetting the Controller

You can reset the controller and view the reboot process on the CLI console using one of the following two methods:

- Turn the controller off and then turn it back on.
- On the CLI, enter `reset system`. At the confirmation prompt, enter `y` to save configuration changes to NVRAM. The controller reboots.

When the controller reboots, the CLI console displays the following reboot information:

- Initializing the system.
- Verifying the hardware configuration.
- Loading microcode into memory.
- Verifying the operating system software load.
- Initializing with its stored configurations.
- Displaying the login prompt.
Managing User Accounts

This chapter contains these sections:
- Creating Guest User Accounts, page 12-1
- Obtaining a Web Authentication Certificate, page 12-6
- Web Authentication Process, page 12-9
- Choosing the Default Web Authentication Login Page, page 12-12
- Choosing a Customized Web Authentication Login Page from an External Web Server, page 12-19
- Downloading a Customized Web Authentication Login Page, page 12-21
- Assigning Login, Login Failure, and Logout Pages per WLAN, page 12-25
- Configuring Wired Guest Access, page 12-28
- Supporting IPv6 Client Guest Access, page 12-37

Creating Guest User Accounts

This section contains the following topics:
- Information About Creating Guest Accounts, page 12-1
- Guidelines and Limitations, page 12-2
- Creating a Lobby Ambassador Account, page 12-2
- Viewing Guest User Accounts, page 12-5

Information About Creating Guest Accounts

The controller can provide guest user access on WLANs. The first step in creating guest user accounts is to create a lobby administrator user, also known as a lobby ambassador account. Once this account has been created, a lobby ambassador can create and manage guest user accounts on the controller. The lobby ambassador has limited configuration privileges and access only to the web pages used to manage the guest accounts.

The lobby ambassador can specify the amount of time that the guest user accounts remain active. After the specified time elapses, the guest user accounts expire automatically.
Guidelines and Limitations

The local user database is limited to a maximum of 2048 entries, which is also the default value. This database is shared by local management users (including lobby ambassadors), local network users (including guest users), MAC filter entries, exclusion list entries, and access point authorization list entries. Together they cannot exceed the configured maximum value.

Creating a Lobby Ambassador Account

This section contains the following topics:
- Creating a Lobby Ambassador Account (GUI), page 12-2
- Creating a Lobby Ambassador Account (CLI), page 12-3
- Creating Guest User Accounts as a Lobby Ambassador (GUI), page 12-3

Creating a Lobby Ambassador Account (GUI)

Step 1 Choose Management > Local Management Users to open the Local Management Users page.

This page lists the names and access privileges of the local management users.

Note If you want to delete any of the user accounts from the controller, hover your cursor over the blue drop-down arrow and choose Remove. However, deleting the default administrative user prohibits both GUI and CLI access to the controller. Therefore, you must create a user with administrative privileges (ReadWrite) before you remove the default user.

Step 2 Click New to create a lobby ambassador account. The Local Management Users > New page appears.

Step 3 In the User Name text box, enter a username for the lobby ambassador account.

Note Management usernames must be unique because they are stored in a single database.

Step 4 In the Password and Confirm Password text boxes, enter a password for the lobby ambassador account.
Creating Guest User Accounts

Chapter 12  Managing User Accounts

Creating Guest User Accounts

Note

Passwords are case sensitive. The settings for the management User Details parameters depends on the settings that you make in the Password Policy page. The following requirements are enforced on the password:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain a management username or the reverse letters of a username.
- The password should not contain words like Cisco, oscic, admin, nimda, or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

Step 5

Choose **LobbyAdmin** from the User Access Mode drop-down list. This option enables the lobby ambassador to create guest user accounts.

Note

The **ReadOnly** option creates an account with read-only privileges, and the **ReadWrite** option creates an administrative account with both read and write privileges.

Step 6

Click **Apply** to commit your changes. The new lobby ambassador account appears in the list of local management users.

Step 7

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

Creating a Lobby Ambassador Account (CLI)

To create a lobby ambassador account use the following command:

```
config mgmtuser add lobbyadmin_username lobbyadmin_pwd lobby-admin
```

Note

Replacing **lobby-admin** with **read-only** creates an account with read-only privileges. Replacing **lobby-admin** with **read-write** creates an administrative account with both read and write privileges.

Creating Guest User Accounts as a Lobby Ambassador (GUI)

Step 1

Log into the controller as the lobby ambassador, using the username and password. The Lobby Ambassador Guest Management > Guest Users List page appears.
Creating Guest User Accounts

Chapter 12  Managing User Accounts

Creating Guest User Accounts

Figure 12-2  Lobby Ambassador Guest Management > Guest Users List Page

Step 2  Click New to create a guest user account. The Lobby Ambassador Guest Management > Guest Users List > New page appears.

Step 3  In the User Name text box, enter a name for the guest user. You can enter up to 24 characters.

Step 4  Perform one of the following:

- If you want to generate an automatic password for this guest user, select the Generate Password check box. The generated password is entered automatically in the Password and Confirm Password text boxes.

- If you want to create a password for this guest user, leave the Generate Password check box unselected and enter a password in both the Password and Confirm Password text boxes.

Note  Passwords can contain up to 24 characters and are case sensitive.

Step 5  From the Lifetime drop-down lists, choose the amount of time (in days, hours, minutes, and seconds) that this guest user account is to remain active. A value of zero (0) for all four text boxes creates a permanent account.

Default: 1 day

Range: 5 minutes to 30 days

Note  The smaller of this value or the session timeout for the guest WLAN, which is the WLAN on which the guest account is created, takes precedence. For example, if a WLAN session timeout is due to expire in 30 minutes but the guest account lifetime has 10 minutes remaining, the account is deleted in 10 minutes upon guest account expiry. Similarly, if the WLAN session timeout expires before the guest account lifetime, the client experiences a recurring session timeout that requires reauthentication.

Note  You can change a guest user account with a nonzero lifetime to another lifetime value at any time while the account is active. However, to make a guest user account permanent using the controller GUI, you must delete the account and create it again. If desired, you can use the config netuser lifetime user_name 0 command to make a guest user account permanent without deleting and recreating it.

Step 6  From the WLAN SSID drop-down list, choose the SSID that will be used by the guest user. The only WLANs that are listed are those WLANs for which Layer 3 web authentication has been configured.
Step 7  In the Description text box, enter a description of the guest user account. You can enter up to 32 characters.

Step 8  Click Apply to commit your changes. The new guest user account appears in the list of guest users on the Guest Users List page.

From this page, you can see all of the guest user accounts, their WLAN SSID, and their lifetime. You can also edit or remove a guest user account. When you remove a guest user account, all of the clients that are using the guest WLAN and are logged in using that account’s username are deleted.

Step 9  Repeat this procedure to create any additional guest user accounts.

Viewing Guest User Accounts

This section contains the following topics:

- Viewing the Guest Accounts (GUI), page 12-5
- Viewing the Guest Accounts (CLI), page 12-6

Viewing the Guest Accounts (GUI)

To view guest user accounts using the controller GUI, choose Security > AAA > Local Net Users. The Local Net Users page appears.

From this page, you can see all of the local net user accounts (including guest user accounts) and can edit or remove them as desired. When you remove a guest user account, all of the clients that are using the guest WLAN and are logged in using that account’s username are deleted.
Viewing the Guest Accounts (CLI)

To see all of the local net user accounts (including guest user accounts) using the controller CLI, enter this command:

```
show netuser summary
```

Additional References

- Creating a Lobby Ambassador Account (GUI), page 12-2
- Creating a Lobby Ambassador Account (CLI), page 12-3

Obtaining a Web Authentication Certificate

This section contains the following topics:

- Information About Web Authentication Certificate, page 12-6
- Support for Chained Certificate, page 12-6
- Obtaining Web Authentication Certificates, page 12-6

Information About Web Authentication Certificate

The controller’s operating system automatically generates a fully functional web authentication certificate, so you do not need to do anything in order to use certificates with Layer 3 web authentication. However, if desired, you can prompt the operating system to generate a new web authentication certificate, or you can download an externally generated SSL certificate.

Support for Chained Certificate

In controller versions earlier than 5.1.151.0, web authentication certificates can be only device certificates and should not contain the CA roots chained to the device certificate (no chained certificates).

With controller version 5.1.151.0 and later, the controller allows for the device certificate to be downloaded as a chained certificate (up to a level of 2) for web authentication. Wildcard certificates are also supported. For more information about chained certificates, see the Generate CSR for Third-Party Certificates and Download Chained Certificates to the WLC document at http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a0080a77592.shtml.

Obtaining Web Authentication Certificates

This section contains the following topics:

- Obtaining a Web Authentication Certificate (GUI), page 12-7
- Obtaining a Web Authentication Certificate (CLI), page 12-8
Obtaining a Web Authentication Certificate (GUI)

**Step 1** Choose Security > Web Auth > Certificate to open the Web Authentication Certificate page.

**Figure 12-4 Web Authentication Certificate Page**

This page shows the details of the current web authentication certificate.

**Step 2** If you want to use a new operating system-generated web authentication certificate, follow these steps:

a. Click Regenerate Certificate. The operating system generates a new web authentication certificate, and a successfully generated web authentication certificate message appears.

b. Reboot the controller to register the new certificate.

**Step 3** If you prefer to use an externally generated web authentication certificate, follow these steps:

a. Verify that the controller can ping the TFTP server.

b. Select the Download SSL Certificate check box.

c. In the Server IP Address text box, enter the IP address of the TFTP server.

The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.
d. Enter the maximum number of times that each download can be attempted in the Maximum Retries text box and the amount of time (in seconds) allowed for each download in the Timeout text box.

e. In the Certificate File Path text box, enter the directory path of the certificate.

f. In the Certificate File Name text box, enter the name of the certificate (certname.pem).

g. In the Certificate Password text box, enter the password for the certificate.

h. Click Apply to commit your changes. The operating system downloads the new certificate from the TFTP server.

i. Reboot the controller to register the new certificate.

---

**Obtaining a Web Authentication Certificate (CLI)**

**Step 1**

See the current web authentication certificate by entering this command:

```
show certificate summary
```

Information similar to the following appears:

```
Web Administration Certificate................... Locally Generated
Web Authentication Certificate.................. Locally Generated
Certificate compatibility mode:............... off
```

**Step 2**

If you want the operating system to generate a new web authentication certificate, follow these steps:

a. To generate the new certificate, enter this command:

```
config certificate generate webauth
```

b. To reboot the controller to register the new certificate, enter this command:

```
reset system
```

**Step 3**

If you prefer to use an externally generated web authentication certificate, follow these steps:

---

**Note**

We recommend that the Common Name (CN) of the externally generated web authentication certificate be 1.1.1.1 (or the equivalent virtual interface IP address) in order for the client’s browser to match the domains of the web authentication URL and the web authentication certificate.

a. Specify the name, path, and type of certificate to be downloaded by entering these commands:

```
transfer download mode tftp
transfer download datatype webauthcert
transfer download serverip server_ip_address
transfer download path server_path_to_file
transfer download filename certname.pem
transfer download certpassword password
transfer download tftpMaxRetries retries
transfer download tftpPktTimeout timeout
```
**Web Authentication Process**

This section contains the following topics:

- Information About Web Authentication Process, page 12-9
- Guidelines and Limitations, page 12-9

**Information About Web Authentication Process**

Web authentication is a Layer 3 security feature that causes the controller to not allow IP traffic (except DHCP-related packets) from a particular client until that client has correctly supplied a valid username and password. When you use web authentication to authenticate clients, you must define a username and password for each client. When the clients attempt to join the wireless LAN, their users must enter the username and password when prompted by a login page.

**Guidelines and Limitations**

When web authentication is enabled (under Layer 3 Security), users might receive a web-browser security alert the first time that they attempt to access a URL.
When clients connect to a WebAuth SSID with a preauthorization ACL configured to allow VPN users, the clients will get disconnected from the SSID every few minutes. Webauth SSIDs must not connect without authenticating on the web page.

After the user clicks Yes to proceed (or if the client’s browser does not display a security alert), the web authentication system redirects the client to a login page (see Figure 12-6).

To prevent the security alert from appearing, follow these steps:

**Step 1** Click **View Certificate** on the Security Alert page.

**Step 2** Click **Install Certificate**.

**Step 3** When the Certificate Import Wizard appears, click **Next**.

**Step 4** Choose **Place all certificates in the following store** and click **Browse**.

**Step 5** At the bottom of the Select Certificate Store page, select the **Show Physical Stores** check box.

**Step 6** Expand the **Trusted Root Certification Authorities** folder and choose **Local Computer**.

**Step 7** Click **OK**.

**Step 8** Choose **Next > Finish**.

**Step 9** When the “The import was successful” message appears, click **OK**.

   d. Because the issuer text box is blank on the controller self-signed certificate, open Internet Explorer, choose **Tools > Internet Options > Advanced**, unselect the **Warn about Invalid Site Certificates** check box under Security, and click **OK**.

**Step 10** Reboot the PC. On the next web authentication attempt, the login page appears.
Chapter 12  Managing User Accounts

Web Authentication Process

Figure 12-6  Default Web Authentication Login Page

The default login page contains a Cisco logo and Cisco-specific text. You can choose to have the web authentication system display one of the following:

- The default login page
- A modified version of the default login page
- A customized login page that you configure on an external web server
- A customized login page that you download to the controller

The “Choosing the Default Web Authentication Login Page” section on page 12-12 provides instructions for choosing how the web authentication login page appears.

When the user enters a valid username and password on the web authentication login page and clicks Submit, the web authentication system displays a successful login page and redirects the authenticated client to the requested URL.
Choosing the Default Web Authentication Login Page

This section contains the following topics:

- Information About Default Web Authentication Login Page, page 12-12
- Guidelines and Limitations, page 12-13
- Choosing the Default Web Authentication Login Page (GUI), page 12-13
- Choosing the Default Web Authentication Login Page (CLI), page 12-14
- Example: Modified Default Web Authentication Login Page Example, page 12-16
- Example: Creating a Customized Web Authentication Login Page, page 12-17

Information About Default Web Authentication Login Page

If you are using a custom web-auth bundle that is served by the internal controller web server, the page should not contain more than 5 elements (including HTML, CSS, and Images). This is because the internal controller web server implements a DoS protection mechanism that limits each client to open a
maximum of 5 (five) concurrent TCP connections depending on the load. Some browsers may try to open more than 5 TCP sessions at the same time (For example Firefox 4) if the page contains more elements and this may result in the page loading slowly depending on how the browser handles the DoS protection.

If you have a complex custom web authentication module, it is recommended that you use an external web-auth config on the controller, where the full login page is hosted at an external web server.

**Guidelines and Limitations**

If you do not want users to connect to a web page using a browser that is configured with SSLv2 only, you can disable SSLv2 for web authentication by entering the `config network secureweb cipher-option sslv2 disable` command. If you enter this command, users must use a browser that is configured to use a more secure protocol such as SSLv3 or later releases. The default value is enabled.

**Choosing the Default Web Authentication Login Page (GUI)**

**Step 1** Choose **Security > Web Auth > Web Login Page** to open the Web Login page.

**Step 2** From the Web Authentication Type drop-down list, choose **Internal (Default)**.

**Step 3** If you want to use the default web authentication login page as is, go to **Step 8**. If you want to modify the default login page, go to **Step 4**.

**Step 4** If you want to hide the Cisco logo that appears in the top right corner of the default page, choose the Cisco Logo **Hide** option. Otherwise, click the **Show** option.

**Step 5** If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter the desired URL in the Redirect URL After Login text box. You can enter up to 254 characters.

**Step 6** If you want to create your own headline on the login page, enter the desired text in the Headline text box. You can enter up to 127 characters. The default headline is “Welcome to the Cisco wireless network.”

**Step 7** If you want to create your own message on the login page, enter the desired text in the Message text box. You can enter up to 2047 characters. The default message is “Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.”

**Step 8** Click **Apply** to commit your changes.
Choosing the Default Web Authentication Login Page

**Step 9** Click **Preview** to view the web authentication login page.

**Step 10** If you are satisfied with the content and appearance of the login page, click **Save Configuration** to save your changes. Otherwise, repeat any of the previous steps as necessary to achieve your desired results.

---

### Choosing the Default Web Authentication Login Page (CLI)

**Step 1** Specify the default web authentication type by entering this command:

```
config custom-web webauth_type internal
```

**Step 2** If you want to use the default web authentication login page as is, go to **Step 8**. If you want to modify the default login page, go to **Step 3**.

**Step 3** To show or hide the Cisco logo that appears in the top right corner of the default login page, enter this command:

```
config custom-web weblogo {enable | disable}
```

**Step 4** If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter this command:

```
config custom-web redirecturl url
```

You can enter up to 130 characters for the URL. To change the redirect back to the default setting, enter the **clear redirecturl** command.

**Step 5** If you want to create your own headline on the login page, enter this command:

```
config custom-web webtitle title
```

You can enter up to 130 characters. The default headline is “Welcome to the Cisco wireless network.” To reset the headline to the default setting, enter the **clear webtitle** command.

**Step 6** If you want to create your own message on the login page, enter this command:

```
config custom-web webmessage message
```

You can enter up to 130 characters. The default message is “Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.” To reset the message to the default setting, enter the **clear webmessage** command.

**Step 7** To enable or disable the web authentication logout popup window, enter this command:

```
config custom-web logout-popup {enable | disable}
```

**Step 8** Enter the **save config** command to save your settings.

**Step 9** Import your own logo into the web authentication login page as follows:

1. Make sure that you have a Trivial File Transfer Protocol (TFTP) server available for the file download. Follow these guidelines when setting up a TFTP server:
   - If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
   - If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
   - A third-party TFTP server cannot run on the same computer as the Cisco WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.
b. Ensure that the controller can contact the TFTP server by entering this command:
   \texttt{ping ip-address}

c. Copy the logo file (in .jpg, .gif, or .png format) to the default directory on your TFTP server. The maximum file size is 30 kilobits. For an optimal fit, the logo should be approximately 180 pixels wide and 360 pixels high.

d. Specify the download mode by entering this command:
   \texttt{transfer download mode tftp}

e. Specify the type of file to be downloaded by entering this command:
   \texttt{transfer download datatype image}

f. Specify the IP address of the TFTP server by entering this command:
   \texttt{transfer download serverip tftp-server-ip-address}

\textbf{Note} Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

g. Specify the download path by entering this command:
   \texttt{transfer download path absolute-tftp-server-path-to-file}

h. Specify the file to be downloaded by entering this command:
   \texttt{transfer download filename \{filename.jpg | filename.gif | filename.png\}}

i. View your updated settings and answer \texttt{y} to the prompt to confirm the current download settings and start the download by entering this command:
   \texttt{transfer download start}

   Information similar to the following appears:
   \begin{verbatim}
   Mode........................................... TFTP
   Data Type...................................... Login Image
   TFTP Server IP................................ x.x.x.x
   TFTP Path..................................... <directory path>
   TFTP Filename..................................... <filename.jpg|.gif|.png>
   This may take some time.
   Are you sure you want to start? (y/n) y
   TFTP Image transfer starting.
   Image installed.
   \end{verbatim}

j. Save your settings by entering this command:
   \texttt{save config}

\textbf{Note} If you ever want to remove this logo from the web authentication login page, enter the \texttt{clear webimage} command.

\textbf{Step 10} Follow the instructions in the “Verifying the Web Authentication Login Page Settings (CLI)” section on page 12-25 to verify your settings.
Example: Modified Default Web Authentication Login Page Example

Figure 12-9 shows an example of a modified default web authentication login page.

These CLI commands were used to create this login page:

- config custom-web weblogo disable
- config custom-web webtitle Welcome to the AcompanyBC Wireless LAN!
- config custom-web webmessage Contact the System Administrator for a Username and Password.
- transfer download start

Information similar to the following appears:

Mode........................................... TFTP
Data Type...................................... Login Image
TFTP Server IP................................. xxx.xxx.xxx.xxx
TFTP Path...................................... /
TFTP Filename..................................... Logo.gif
This may take some time.
Are you sure you want to start? (y/n) y
TFTP Image transfer starting.
Image installed.

- config custom-web redirecturl url

show custom-web
Cisco Logo....................... Disabled
CustomLogo....................... 00_logo.gif
Custom Title..................... Welcome to the AcompanyBC Wireless LAN!
Custom Message ................... Contact the System Administrator for a Username and Password.
Custom Redirect URL........ http://www.AcompanyBC.com
Web Authentication Mode..... Disabled
Web Authentication URL........ Disabled

Example: Creating a Customized Web Authentication Login Page

This section provides information on creating a customized web authentication login page, which can then be accessed from an external web server.

Here is a web authentication login page template. It can be used as a model when creating your own customized page:

```html
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<title>Web Authentication</title>
<script>
function submitAction(){
    var link = document.location.href;
    var searchString = "redirect="
    var equalIndex = link.indexOf(searchString);
    var redirectUrl = "";
    if (equalIndex >= 0) {
        equalIndex += searchString.length;
        redirectUrl += link.substring(equalIndex);
        if(redirectUrl.length > 255)
            redirectUrl = redirectUrl.substring(0,255);
        document.forms[0].redirect_url.value = redirectUrl;
        document.forms[0].buttonClicked.value = 4;
        document.forms[0].submit();
    }

    if(equalIndex >= 0) {
        equalIndex += searchString.length;
        redirectUrl += link.substring(equalIndex);
    }
    if(redirectUrl.length > 255)
        redirectUrl = redirectUrl.substring(0,255);
    document.forms[0].redirect_url.value = redirectUrl;
    document.forms[0].buttonClicked.value = 4;
    document.forms[0].submit();
}

function loadAction(){
    var url = window.location.href;
    var args = new Object();
    var query = location.search.substring(1);
    var pairs = query.split("&");
    for(var i=0;i<pairs.length;i++){
        var pos = pairs[i].indexOf('=');
        if(pos == -1) continue;
        var argname = pairs[i].substring(0,pos);
        var value = pairs[i].substring(pos+1);
        args[argname] = unescape(value);
    }
    document.forms[0].action = args.switch_url;
    document.forms[0].submit();
}
</script>
</head>
<body>

This section provides information on creating a customized web authentication login page, which can then be accessed from an external web server.

Here is a web authentication login page template. It can be used as a model when creating your own customized page:

```html
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<title>Web Authentication</title>
<script>
function submitAction(){
    var link = document.location.href;
    var searchString = "redirect="
    var equalIndex = link.indexOf(searchString);
    var redirectUrl = "";
    if (equalIndex >= 0) {
        equalIndex += searchString.length;
        redirectUrl += link.substring(equalIndex);
        if(redirectUrl.length > 255)
            redirectUrl = redirectUrl.substring(0,255);
        document.forms[0].redirect_url.value = redirectUrl;
        document.forms[0].buttonClicked.value = 4;
        document.forms[0].submit();
    }

    if(equalIndex >= 0) {
        equalIndex += searchString.length;
        redirectUrl += link.substring(equalIndex);
    }
    if(redirectUrl.length > 255)
        redirectUrl = redirectUrl.substring(0,255);
    document.forms[0].redirect_url.value = redirectUrl;
    document.forms[0].buttonClicked.value = 4;
    document.forms[0].submit();
}

function loadAction(){
    var url = window.location.href;
    var args = new Object();
    var query = location.search.substring(1);
    var pairs = query.split("&");
    for(var i=0;i<pairs.length;i++){
        var pos = pairs[i].indexOf('=');
        if(pos == -1) continue;
        var argname = pairs[i].substring(0,pos);
        var value = pairs[i].substring(pos+1);
        args[argname] = unescape(value);
    }
    document.forms[0].action = args.switch_url;
    document.forms[0].submit();
}
</script>
</head>
<body>
```
Choosing the Default Web Authentication Login Page

```javascript
// This is the status code returned from webauth login action
// Any value of status code from 1 to 5 is error condition and user
// should be shown error as below or modify the message as it suits
// the customer
if(args.statusCode == 1){
    alert("You are already logged in. No further action is required on your part.");
}
else if(args.statusCode == 2){
    alert("You are not configured to authenticate against web portal. No further
    action is required on your part.");
}
else if(args.statusCode == 3){
    alert("The username specified cannot be used at this time. Perhaps the username is
    already logged into the system?");
}
else if(args.statusCode == 4){
    alert("The User has been excluded. Please contact the administrator.");
}
else if(args.statusCode == 5){
    alert("Invalid username and password. Please try again.");
}
else if(args.statusCode == 6){
    alert("Invalid email address format. Please try again.");
}
```

```html
<form method="post" action="https://209.165.200.225/login.html">
  <input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0">
  <input TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE="">
  <input TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

  <div align="center">
    <table border="0" cellspacing="0" cellpadding="0">
      <tr> <td>&nbsp;</td></tr>
      <tr align="center" > <td colspan="2">User Name &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="TEXT" name="username" SIZE="25" MAXLENGTH="63" VALUE=""></td>
      </tr>
      <tr align="center" > <td colspan="2">Password &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="Password" name="password" SIZE="25" MAXLENGTH="24"></td>
      </tr>
      <tr align="center">
        <td colspan="2"><input type="button" name="Submit" value="Submit" class='button" onclick='submitAction();'>
      </td>
    </tr>
  </table>
</div>
</form>
</body>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();">
<form method="post" action="https://209.165.200.225/login.html">
  <input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0">
  <input TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE="">
  <input TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

  <div align="center">
    <table border="0" cellspacing="0" cellpadding="0">
      <tr> <td>&nbsp;</td></tr>
      <tr align="center" > <td colspan="2">User Name &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="TEXT" name="username" SIZE="25" MAXLENGTH="63" VALUE=""></td>
      </tr>
      <tr align="center" > <td colspan="2">Password &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="Password" name="password" SIZE="25" MAXLENGTH="24"></td>
      </tr>
      <tr align="center">
        <td colspan="2"><input type="button" name="Submit" value="Submit" class='button" onclick='submitAction();'>
      </td>
    </tr>
  </table>
</div>
</form>
</body>
</html>
```
These parameters are added to the URL when the user’s Internet browser is redirected to the customized login page:

- **ap_mac**—The MAC address of the access point to which the wireless user is associated.
- **switch_url**—The URL of the controller to which the user credentials should be posted.
- **redirect**—The URL to which the user is redirected after authentication is successful.
- **statusCode**—The status code returned from the controller’s web authentication server.
- **wlan**—The WLAN SSID to which the wireless user is associated.

The available status codes are as follows:

- **Status Code 1**: “You are already logged in. No further action is required on your part.”
- **Status Code 2**: “You are not configured to authenticate against web portal. No further action is required on your part.”
- **Status Code 3**: “The username specified cannot be used at this time. Perhaps the username is already logged into the system?”
- **Status Code 4**: “You have been excluded.”
- **Status Code 5**: “The User Name and Password combination you have entered is invalid. Please try again.”

**Note**

For additional information, see the *External Web Authentication with Wireless LAN Controllers Configuration Example* at this URL: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008076f974.shtml

---

**Choosing a Customized Web Authentication Login Page from an External Web Server**

This section contains the following topics:

- **Information About Customized Web Authentication Login Page**, page 12-20
- **Guidelines and Limitations**, page 12-20
- **Choosing a Customized Web Authentication Login Page from an External Web Server (GUI)**, page 12-20
- **Choosing a Customized Web Authentication Login Page from an External Web Server (CLI)**, page 12-21
Information About Customized Web Authentication Login Page

You can customize the web authentication login page to redirect to an external web server. When you enable this feature, the user is directed to your customized login page on the external web server.

Guidelines and Limitations

For Cisco 5500 Series Controllers, and controller network modules, you must configure a preauthentication access control list (ACL) on the WLAN for the external web server and then choose this ACL as the WLAN preauthentication ACL under Security Policies > Web Policy on the WLANs > Edit page.

Choosing a Customized Web Authentication Login Page from An External Web Server

This section contains the following topics:

- Choosing a Customized Web Authentication Login Page from an External Web Server (GUI), page 12-20

Choosing a Customized Web Authentication Login Page from an External Web Server (GUI)

**Step 1** Choose Security > Web Auth > Web Login Page to open the Web Login page.

**Step 2** From the Web Authentication Type drop-down list, choose External (Redirect to external server).

**Step 3** In the URL text box, enter the URL of the customized web authentication login page on your web server. You can enter up to 252 characters.

**Step 4** In the Web Server IP Address text box, enter the IP address of your web server. Your web server should be on a different network from the controller service port network.

**Step 5** Click Add Web Server. This server now appears in the list of external web servers.

**Step 6** Click Apply to commit your changes.
Step 7 If you are satisfied with the content and appearance of the login page, click Save Configuration to save your changes.

Choosing a Customized Web Authentication Login Page from an External Web Server (CLI)

Step 1 Specify the web authentication type by entering this command:
config custom-web webauth_type external

Step 2 Specify the URL of the customized web authentication login page on your web server by entering this command:
config custom-web ext-webauth-url url
You can enter up to 252 characters for the URL.

Step 3 Specify the IP address of your web server by entering this command:
config custom-web ext-webserver {add | delete} server_IP_address

Step 4 Enter the save config command to save your settings.

Step 5 Follow the instructions in the “Verifying the Web Authentication Login Page Settings (CLI)” section on page 12-25 to verify your settings.

Additional References

See Chapter 7, “Configuring Security Solutions,” for more information on ACLs.

Downloading a Customized Web Authentication Login Page

This section contains the following topics:
- Information About Downloading Customized Web Authentication Login Page, page 12-21
- Guidelines and Limitations, page 12-22
- Downloading a Customized Web Authentication Login Page (GUI), page 12-22
- Downloading a Customized Web Authentication Login Page (CLI), page 12-24
- Example: Customized Web Authentication Login Page, page 12-24
- Verifying the Web Authentication Login Page Settings (CLI), page 12-25

Information About Downloading Customized Web Authentication Login Page

You can compress the page and image files used for displaying a web authentication login page into a.tar file for download to a controller. These files are known as the webauth bundle. The maximum allowed size of the files in their uncompressed state is 1 MB. When the .tar file is downloaded from a local TFTP server, it enters the controller’s file system as an untarred file.
Note
If you load a webauth bundle with a .tar compression application that is not GNU compliant, the controller cannot extract the files in the bundle and the following error messages appear: “Extracting error” and “TFTP transfer failed.” Therefore, we recommend that you use an application that complies with GNU standards, such as PicoZip, to compress the .tar file for the webauth bundle.

Note
Configuration backups do not include extra files or components, such as the webauth bundle or external licenses, that you download and store on your controller, so you should manually save external backup copies of those files or components.

Note
If the customized webauth bundle has more than 3 separated elements, we advise you to use an external server to prevent page load issues that may be caused because of TCP rate-limiting policy on the controller.

Guidelines and Limitations

- Name the login page “login.html.” The controller prepares the web authentication URL based on this name. If the server does not find this file after the webauth bundle has been untarred, the bundle is discarded, and an error message appears.
- Include input text boxes for both a username and password.
- Retain the redirect URL as a hidden input item after extracting from the original URL.
- Extract and set the action URL in the page from the original URL.
- Include scripts to decode the return status code.
- Make sure that all paths used in the main page (to refer to images, for example).
- Ensure that no filenames within the bundle are greater than 30 characters.

Additional References

You can download a login page example from Cisco WCS and use it as a starting point for your customized login page. See the “Downloading a Customized Web Auth Page” section in the Using Templates chapter of the Cisco Wireless Control System Configuration Guide, Release 7.0, for instructions.

Downloading a Customized Web Authentication Login Page (GUI)

Step 1
Make sure that you have a TFTP server available for the file download. See the guidelines for setting up a TFTP server in Step 9 of the “Choosing the Default Web Authentication Login Page (GUI)” section on page 12-13.

Step 2
Copy the .tar file containing your login page to the default directory on your TFTP server.

Step 3
Choose Commands > Download File to open the Download File to Controller page.
Step 4  From the File Type drop-down list, choose **Webauth Bundle**.

Step 5  From the Transfer Mode drop-down list, choose **TFTP** or **FTP**.

Step 6  In the IP Address text box, enter the IP address of the TFTP server.

Step 7  If you are using a TFTP server, enter the maximum number of times the controller should attempt to download the `.tar` file in the Maximum Retries text box.

   The range is 1 to 254.

   The default is 10.

Step 8  If you are using a TFTP server, enter the amount of time in seconds before the controller times out while attempting to download the `.tar` file in the Timeout text box.

   The range is 1 to 254 seconds.

   The default is 6 seconds.

Step 9  In the File Path text box, enter the path of the `.tar` file to be downloaded. The default value is “/.”

Step 10  In the File Name text box, enter the name of the `.tar` file to be downloaded.

Step 11  If you are using an FTP server, follow these steps:

   a.  In the Server Login Username text box, enter the username to log into the FTP server.

   b.  In the Server Login Password text box, enter the password to log into the FTP server.

   c.  In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 12  Click **Download** to download the `.tar` file to the controller.

Step 13  Choose **Security > Web Auth > Web Login Page** to open the Web Login page.

Step 14  From the Web Authentication Type drop-down list, choose **Customized (Downloaded)**.

Step 15  Click **Apply** to commit your changes.

Step 16  Click **Preview** to view your customized web authentication login page.

Step 17  If you are satisfied with the content and appearance of the login page, click **Save Configuration** to save your changes.
Downloading a Customized Web Authentication Login Page (CLI)

Step 1  Make sure that you have a TFTP server available for the file download. See the guidelines for setting up a TFTP server in Step 9 of the “Choosing the Default Web Authentication Login Page (CLI)” section on page 12-14.

Step 2  Copy the .tar file containing your login page to the default directory on your TFTP server.

Step 3  Specify the download mode by entering this command:

```
transfer download mode tftp
```

Step 4  Specify the type of file to be downloaded by entering this command:

```
transfer download datatype webauthbundle
```

Step 5  Specify the IP address of the TFTP server by entering this command:

```
transfer download serverip tftp-server-ip-address.
```

Note  Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

Step 6  Specify the download path by entering this command:

```
transfer download path absolute-tftp-server-path-to-file
```

Step 7  Specify the file to be downloaded by entering this command:

```
transfer download filename filename.tar
```

Step 8  View your updated settings and answer y to the prompt to confirm the current download settings and start the download by entering this command:

```
transfer download start
```

Step 9  Specify the web authentication type by entering this command:

```
config custom-web webauth_type customized
```

Step 10  Enter the save config command to save your settings.

Additional References

See the “Web Authentication Process” section on page 12-9.

Example: Customized Web Authentication Login Page

The following figure shows an example of a customized web authentication login page.
Verifying the Web Authentication Login Page Settings (CLI)

Enter the `show custom-web` command to verify your changes to the web authentication login page. This example shows the information that appears when the configuration settings are set to default values:

- **Cisco Logo**: Enabled
- **CustomLogo**: Disabled
- **Custom Title**: Disabled
- **Custom Message**: Disabled
- **Custom Redirect URL**: Disabled
- **Web Authentication Mode**: Disabled
- **Web Authentication URL**: Disabled

Information similar to the following appears:

- **Cisco Logo**: Disabled
- **CustomLogo**: 00_logo.gif
- **Custom Title**: Welcome to the AcompanyBC Wireless LAN!
- **Custom Message**: Contact the System Administrator for a Username and Password.
- **Custom Redirect URL**: 
- **Web Authentication Mode**: Internal
- **Web Authentication URL**: Disabled

Assigning Login, Login Failure, and Logout Pages per WLAN

This section contains the following topics:

- **Information About Assigning Login, Login Failure, and Logout Pages per WLAN**, page 12-26
- **Assigning Login, Login Failure, and Logout Pages per WLAN (GUI)**, page 12-26
- **Assigning Login, Login Failure, and Logout Pages per WLAN (CLI)**, page 12-27
Information About Assigning Login, Login Failure, and Logout Pages per WLAN

You can display different web authentication login, login failure, and logout pages to users per WLAN. This feature enables user-specific web authentication pages to be displayed for a variety of network users, such as guest users or employees within different departments of an organization.

Different login pages are available for all web authentication types (internal, external, and customized). However, different login failure and logout pages can be specified only when you choose customized as the web authentication type.

Assigning Login, Login Failure, and Logout Pages per WLAN (GUI)

Step 1  Choose WLANs to open the WLANs page.
Step 2  Click the ID number of the WLAN to which you want to assign a web login, login failure, or logout page.
Step 3  Choose Security > Layer 3.
Step 4  Make sure that Web Policy and Authentication are selected.
Step 5  Select the Override Global Config check box to override the global authentication configuration web authentication pages.
Step 6  When the Web Auth Type drop-down list appears, choose one of the following options to define the web authentication pages for wireless guest users:

- **Internal**—Displays the default web login page for the controller. This is the default value.
- **Customized**—Displays custom web login, login failure, and logout pages. If you choose this option, three separate drop-down lists appear for login, login failure, and logout page selection. You do not need to define a customized page for all three options. Choose None from the appropriate drop-down list if you do not want to display a customized page for that option.

  **Note**  These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files. For details on downloading custom pages, see the “Downloading a Customized Web Authentication Login Page” section on page 12-21.

- **External**—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

  You can choose specific RADIUS or LDAP servers to provide external authentication on the WLANs > Edit (Security > AAA Servers) page. Additionally, you can define the priority in which the servers provide authentication.

Step 7  If you chose External as the web authentication type in Step 6, choose AAA Servers and choose up to three RADIUS and LDAP servers using the drop-down lists.

  **Note**  The RADIUS and LDAP external servers must already be configured in order to be selectable options on the WLANs > Edit (Security > AAA Servers) page. You can configure these servers on the RADIUS Authentication Servers page and LDAP Servers page.

Step 8  Establish the priority in which the servers are contacted to perform web authentication as follows:
Chapter 12  Managing User Accounts

Assigning Login, Login Failure, and Logout Pages per WLAN

Note
The default order is local, RADIUS, LDAP.

a. Highlight the server type (local, RADIUS, or LDAP) that you want to be contacted first in the box next to the Up and Down buttons.
b. Click Up and Down until the desired server type is at the top of the box.
c. Click the < arrow to move the server type to the priority box on the left.
d. Repeat these steps to assign priority to the other servers.

Step 9  Click Apply to commit your changes.
Step 10  Click Save Configuration to save your changes.

Assigning Login, Login Failure, and Logout Pages per WLAN (CLI)

Step 1  Determine the ID number of the WLAN to which you want to assign a web login, login failure, or logout page by entering this command:
show wlan summary

Step 2  If you want wireless guest users to log into a customized web login, login failure, or logout page, enter these commands to specify the filename of the web authentication page and the WLAN for which it should display:

• config wlan custom-web login-page page_name wlan_id—Defines a customized login page for a given WLAN.
• config wlan custom-web loginfailure-page page_name wlan_id—Defines a customized login failure page for a given WLAN.

Note  To use the controller’s default login failure page, enter the config wlan custom-web loginfailure-page none wlan_id command.

• config wlan custom-web logout-page page_name wlan_id—Defines a customized logout page for a given WLAN.

Note  To use the controller’s default logout page, enter the config wlan custom-web logout-page none wlan_id command.

Step 3  Redirect wireless guest users to an external server before accessing the web login page by entering this command to specify the URL of the external server:
cfg config wlan custom-web ext-webauth-url ext_web_url wlan_id

Step 4  Define the order in which web authentication servers are contacted by entering this command:
cfg config wlan security web-auth server-precedence wlan_id {local | ldap | radius} {local | ldap | radius}
The default order of server web authentication is local, RADIUS and LDAP.
**Configuring Wired Guest Access**

This section contains the following topics:

- Information About Wired Guest Access, page 12-28
- Prerequisites for Configuring Wired Guest Access, page 12-30
- Guidelines and Limitations, page 12-30
- Configuring Wired Guest Access, page 12-31

**Information About Wired Guest Access**

Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or through specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

Wired guest access can be configured in a standalone configuration or in a dual-controller configuration that uses both an anchor controller and a foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

---

**Note**

All external servers must be preconfigured on the controller. You can configure them on the RADIUS Authentication Servers page and the LDAP Servers page.

**Step 5**

Define which web authentication page displays for a wireless guest user by entering this command:

```bash
config wlan custom-web webauth-type {internal | customized | external} wlan_id
```

where

- **internal** displays the default web login page for the controller. This is the default value.
- **customized** displays the custom web login page that was configured in Step 2.

**Note**

You do not need to define the web authentication type in Step 5 for the login failure and logout pages as they are always customized.

- **external** redirects users to the URL that was configured in Step 3.

**Step 6**

Use a WLAN-specific custom web configuration rather than a global custom web configuration by entering this command:

```bash
config wlan custom-web global disable wlan_id
```

**Note**

If you enter the `config wlan custom-web global enable wlan_id` command, the custom web authentication configuration at the global level is used.

**Step 7**

Save your changes by entering this command:

```bash
save config
```
Wired guest access ports initially terminate on a Layer 2 access switch or switch port configured with VLAN interfaces for wired guest access traffic. The wired guest traffic is then trunked from the access switch to a controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch. See Figure 12-13.

**Figure 12-13   Wired Guest Access Example with One Controller**

If two controllers are being used, the foreign controller, which receives the wired guest traffic from the access switch, forwards it to the anchor controller. A bidirectional EoIP tunnel is established between the foreign and anchor controllers to handle this traffic. See Figure 12-14.
**Figure 12-14**  Wired Guest Access Example with Two Controllers

Note

Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

Note

You can specify the amount of bandwidth allocated to a wired guest user in the network by configuring a QoS role and a bandwidth contract. For details on configuring these features. See the “Configuring Quality of Service” section on page 4-66.

**Prerequisites for Configuring Wired Guest Access**

To configure wired guest access on a wireless network, you must perform the following:

1. Configure a dynamic interface (VLAN) for wired guest user access
2. Create a wired LAN for guest user access
3. Configure the controller
4. Configure the anchor controller (if terminating traffic on another controller)
5. Configure security for the guest LAN
6. Verify the configuration

**Guidelines and Limitations**

- Wired guest access is supported only on the following controllers: Cisco 5500 Series and Cisco Flex 7500 Series controllers, the Cisco WiSM, the Cisco WiSM2, and the Catalyst 3750G Integrated Wireless LAN Controller Switch.
- Wired guest access interfaces must be tagged.
- Wired guest access ports must be in the same Layer 2 network as the foreign controller.
- Up to five wired guest access LANs can be configured on a controller. Also in a wired guest access LAN, multiple anchors are supported.
- Layer 3 web authentication and web passthrough are supported for wired guest access clients. Layer 2 security is not supported.
- Do not trunk a wired guest VLAN to multiple foreign controllers, as it might produce unpredictable results.

## Configuring Wired Guest Access

This section contains the following topics:
- Configuring Wired Guest Access (GUI), page 12-31
- Configuring Wired Guest Access (CLI), page 12-34

### Configuring Wired Guest Access (GUI)

**Step 1** Choose **Controller > Interfaces** to create a dynamic interface for wired guest user access. The Interfaces page appears.

**Step 2** Click **New** to open the Interfaces > New page.

**Step 3** Enter a name and VLAN ID for the new interface.

**Step 4** Click **Apply** to commit your changes.

**Step 5** In the Port Number text box, enter a valid port number. You can enter a number between 0 and 25 (inclusive).

**Step 6** Select the **Guest LAN** check box.

**Step 7** Click **Apply** to commit your changes.

**Step 8** To create a wired LAN for guest user access, choose **WLANs**.

**Step 9** Choose **Create New** from the drop-down list and click **Go** on the WLANs page. The WLANs > New page appears.

**Figure 12-15  WLANs > New Page**

**Step 10** From the Type drop-down list, choose **Guest LAN**.

**Step 11** In the Profile Name text box, enter a name that identifies the guest LAN. Do not use any spaces.

**Step 12** From the WLAN ID drop-down list, choose the ID number for this guest LAN.

**Note** You can create up to five guest LANs, so the WLAN ID options are 1 through 5 (inclusive).
Step 13  Click **Apply** to commit your changes. The WLANs > Edit page appears.

Figure 12-16  WLANs > Edit Page

Step 14  Select the **Enabled** check box for the Status parameter.

Step 15  Web authentication (Web-Auth) is the default security policy. If you want to change this to web passthrough, choose the **Security** tab after completing Step 16 and Step 17.

Step 16  From the Ingress Interface drop-down list, choose the VLAN that you created in Step 3. This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 17  From the Egress Interface drop-down list, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.

Step 18  If you want to change the authentication method (for example, from web authentication to web passthrough), choose **Security > Layer 3**. The WLANs > Edit (Security > Layer 3) page appears.

Figure 12-17  WLANs > Edit (Security > Layer 3) Page

Step 19  From the Layer 3 Security drop-down list, choose one of the following:

- **None**—Layer 3 security is disabled.
- **Web Authentication**—Causes users to be prompted for a username and password when connecting to the wireless network. This is the default value.
- **Web Passthrough**—Allows users to access the network without entering a username and password.
Chapter 12      Managing User Accounts

Configuring Wired Guest Access

Step 20   If you choose the Web Passthrough option, an Email Input check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

Step 21   To override the global authentication configuration set on the Web Login page, select the Override Global Config check box.

Step 22   When the Web Auth Type drop-down list appears, choose one of the following options to define the web authentication pages for wired guest users:

- **Internal**—Displays the default web login page for the controller. This is the default value.
- **Customized**—Displays custom web login, login failure, and logout pages. If you choose this option, three separate drop-down lists appear for login, login failure, and logout page selection. You do not need to define a customized page for all three options. Choose None from the appropriate drop-down list if you do not want to display a customized page for that option.

Note   These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files.

- **External**—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

You can choose specific RADIUS or LDAP servers to provide external authentication on the WLANs > Edit (Security > AAA Servers) page. Additionally, you can define the priority in which the servers provide authentication.

Step 23   If you chose External as the web authentication type in Step 22, choose AAA Servers and choose up to three RADIUS and LDAP servers using the drop-down lists.

Note   The RADIUS and LDAP external servers must already be configured in order to be selectable options on the WLANs > Edit (Security > AAA Servers) page. You can configure these servers on the RADIUS Authentication Servers page and LDAP Servers page.

Step 24   To establish the priority in which the servers are contacted to perform web authentication as follows:

Note   The default order is local, RADIUS, LDAP.

a. Highlight the server type (local, RADIUS, or LDAP) that you want to be contacted first in the box next to the Up and Down buttons.

b. Click Up and Down until the desired server type is at the top of the box.

c. Click the < arrow to move the server type to the priority box on the left.

d. Repeat these steps to assign priority to the other servers.

Step 25   Click Apply to commit your changes.

Step 26   Click Save Configuration to save your changes.
Step 27  Repeat this process if a second (anchor) controller is being used in the network.

Configuring Wired Guest Access (CLI)

Step 1  Create a dynamic interface (VLAN) for wired guest user access by entering this command:

```
config interface create interface_name vlan_id
```

Step 2  If link aggregation trunk is not configured, enter this command to map a physical port to the interface:

```
config interface port interface_name primary_port {secondary_port}
```

Step 3  Enable or disable the guest LAN VLAN by entering this command:

```
config interface guest-lan interface_name {enable | disable} [save config]
```

Note  Information on the configured web authentication appears in both the `show run-config` and `show running-config` commands.

Step 4  Display the customized web authentication settings for a specific guest LAN by entering this command:

```
show custom-web {all | guest-lan guest_lan_id}
```

Note  If internal web authentication is configured, the Web Authentication Type displays as internal rather than external (controller level) or customized (WLAN profile level).

Information similar to the following appears for the `show custom-web all` command:

- Radius Authentication Method................... PAP
- Cisco Logo.................................... Enabled
- CustomLogo.................................... None
- Custom Title.................................. None
- Custom Message................................ None
- Custom Redirect URL.......................... None
- Web Authentication Type....................... External
- External Web Authentication URL.............. http:\9.43.0.100\login.html

External Web Server list

<table>
<thead>
<tr>
<th>Index</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9.43.0.100</td>
</tr>
<tr>
<td>2</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>3</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>4</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>5</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>...</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>20</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

Configuration Per Profile:

```
WLAN ID: 1
WLAN Status.............................. Enabled
Web Security Policy..................... Web Based Authentication
Global Status............................ Disabled
WebAuth Type............................. Customized
Login Page................................ login1.html
Loginfailure page name.................. loginfailure1.html
```
Logout page name............................. logout1.html

WLAN ID: 2
WLAN Status................................. Enabled
Web Security Policy.......................... Web Based Authentication
Global Status................................. Disabled
WebAuth Type................................. Internal
Logins failure page name...................... None
Logout page name............................. None

WLAN ID: 3
WLAN Status................................. Enabled
Web Security Policy.......................... Web Based Authentication
Global Status................................. Enabled
WebAuth Type................................. Customized
Login Page.................................... login.html
Logins failure page name...................... LF2.html
Logout page name............................. LG2.html

Information similar to the following appears for the `show custom-web guest-lan guest_lan_id` command:

Guest LAN ID: 1
Guest LAN Status............................. Disabled
Web Security Policy.......................... Web Based Authentication
Global Status................................. Enabled
WebAuth Type................................. Internal
Logins failure page name...................... None
Logout page name............................. None

**Step 5**

Display a summary of the local interfaces by entering this command:

```
show interface summary
```

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Port</th>
<th>VLAN Id</th>
<th>IP Address</th>
<th>Type</th>
<th>Ap Mgr</th>
<th>Guest</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-manager</td>
<td>1</td>
<td>untagged</td>
<td>1.100.163.25</td>
<td>Static</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>management</td>
<td>1</td>
<td>untagged</td>
<td>1.100.163.24</td>
<td>Static</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>service-port</td>
<td>N/A</td>
<td>N/A</td>
<td>172.19.35.31</td>
<td>Static</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>virtual</td>
<td>N/A</td>
<td>N/A</td>
<td>1.1.1.1</td>
<td>Static</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>wired</td>
<td>1</td>
<td>20</td>
<td>10.20.20.8</td>
<td>Dynamic</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>wired-guest</td>
<td>1</td>
<td>236</td>
<td>10.20.236.50</td>
<td>Dynamic</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note** The interface name of the wired guest LAN in this example is `wired-guest` and its VLAN ID is 236.

Display detailed interface information by entering this command:

```
show interface detailed interface_name
```

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>MAC Address</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>wired-guest</td>
<td>00:1a:6d:dd:1e:40</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

Chapter 12      Managing User Accounts

Configuring Wired Guest Access

DHCP Option 82................................... Disabled
Virtual DNS Host Name............................ Disabled
AP Manager....................................... No
Guest Interface.................................. No

Step 6  Display the configuration of a specific wired guest LAN by entering this command:

   show guest-lan guest_lan_id

Information similar to the following appears:

Guest LAN Identifier............................. 1
Profile Name..................................... guestlan
Network Name (SSID).............................. guestlan
Status........................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients.......................... 1
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. Infinity
Interface........................................ wired
Ingress Interface................................. wired-guest
WLAN ACL......................................... unconfigured
DHCP Server...................................... 10.20.236.90
DHCP Address Assignment Required............... Disabled
Quality of Service............................... Silver (best effort)
Security
   Web Based Authentication...................... Enabled
   ACL........................................... Unconfigured
   Web-Passthrough............................... Disabled
   Conditional Web Redirect...................... Disabled
   Auto Anchor................................. Disabled

Mobility Anchor List
GLAN ID IP Address Status
------- --------------- ------

Note  Enter the show guest-lan summary command to see all wired guest LANs configured on the controller.

Step 7  Display the active wired guest LAN clients by entering this command:

   show client summary guest-lan

Information similar to the following appears:

Number of Clients................................ 1
MAC Address   AP Name Status    WLAN  Auth Protocol  Port Wired
------------------- ------- ----------- ----- ----- --------- ----- ------
00:16:36:40:ac:58   N/A   Associated   1    No  802.3  1  Yes

Step 8  Display detailed information for a specific client by entering this command:

   show client detail client_mac

Information similar to the following appears:

Client MAC Address.................................. 00:40:96:b2:a3:44
Client Username..................................... N/A
AP MAC Address.................................... 00:18:74:c7:c0:90
Client State........................................ Associated
Wireless LAN Id................................. 1
BSSID............................................. 00:18:74:c7:c0:9f
Channel........................................... 56
IP Address........................................... 192.168.10.28
Association Id................................. 1
Authentication Algorithm...................... Open System
Supporting IPv6 Client Guest Access

Once a guest user associates, the user is placed in a run state until the client is authenticated. The controller intercepts both IPv4 and IPv6 traffic in this state and redirects it to the virtual IP address of the controller. Once the user is authenticated, the user’s MAC address is moved to the run state and both IPv4 traffic and IPv6 traffic are allowed to pass.

To support the redirection of IPv6-only clients, the controller automatically creates an IPv6 virtual address based on the IPv4 virtual address configured on the controller. The virtual IPv6 address follows the convention of [::ffff:<virtual IPv4 address>]. For example, a virtual IP address of 192.0.2.1 would translate into [::ffff:192.0.2.1]. For an IPv6 captive portal to be displayed, the user must request an IPv6 resolvable DNS entry such as ipv6.google.com, which returns a DNSv6 (AAAA) record.
Configuring Radio Resource Management

This chapter contains these sections:
- Information About Radio Resource Management, page 13-1
- Guidelines and Limitations, page 13-5
- Configuring RRM, page 13-5
- Configuring Off-Channel Scanning Defer, page 13-9
- Configuring RF Groups, page 13-29
- Viewing the RF Group Status, page 13-30
- Configuring RRM Neighbor Discovery Packets, page 13-25
- Overriding RRM, page 13-32
- Configuring Rogue Access Point Detection in RF Groups, page 13-41
- Configuring CCX Radio Management Features, page 13-44

Information About Radio Resource Management

The Radio Resource Management (RRM) software embedded in the controller acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables controllers to continually monitor their associated lightweight access points for the following information:

- Traffic load—The total bandwidth used for transmitting and receiving traffic. It enables wireless LAN managers to track and plan network growth ahead of client demand.
- Interference—The amount of traffic coming from other 802.11 sources.
- Noise—The amount of non-802.11 traffic that is interfering with the currently assigned channel.
- Coverage—The received signal strength (RSSI) and signal-to-noise ratio (SNR) for all connected clients.
- Other — The number of nearby access points.

Using this information, RRM can periodically reconfigure the 802.11 RF network for best efficiency. To do this, RRM performs these functions:

- Radio resource monitoring
- Transmit power control
- Dynamic channel assignment
- Coverage hole detection and correction

### Radio Resource Monitoring

RRM automatically detects and configures new controllers and lightweight access points as they are added to the network. It then automatically adjusts associated and nearby lightweight access points to optimize coverage and capacity.

Lightweight access points can simultaneously scan all valid 802.11a/b/g channels for the country of operation as well as for channels available in other locations. The access points go “off-channel” for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

**Note**

In the presence of voice traffic (in the last 100 ms), the access points defer off-channel measurements.

Each access point spends only 0.2 percent of its time off-channel. This activity is distributed across all access points so that adjacent access points are not scanning at the same time, which could adversely affect wireless LAN performance.

**Note**

When there are numerous rogue access points in the network, the chance of detecting rogues on channels 157 or 161 by a FlexConnect or local mode access point is small. In such cases, the monitor mode AP can be used for rogue detection.

### Transmit Power Control

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. You can choose between two versions of transmit power control: TPCv1 and TPCv2. With TPCv1, typically, power can be kept low to gain extra capacity and reduce interference. transmit power is dynamically adjusted with the goal of minimum interference. TPCv2 is suitable for dense networks. In this mode, there could be higher roaming delays and coverage hole incidents.

The transmit power control (TPC) algorithm both increases and decreases an access point’s power in response to changes in the RF environment. In most instances, TPC seeks to lower an access point's power to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from coverage hole detection, which is primarily concerned with clients. TPC provides enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

**Note**

See Step 6 on page 13-36 for an explanation of the transmit power levels.

### Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings

The TPC algorithm balances RF power in many diverse RF environments. However, it is possible that automatic power control will not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions—for example, when all access points must be mounted in a central hallway, placing the access points close together, but requiring coverage out to the edge of the building.
In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings apply to all access points through RF profiles in a RF network. This can also be set from the TCP Global Settings page.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment text boxes, enter the maximum and minimum transmit power used by RRM on the Tx Power Control page. The range for these parameters is –10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

If you configure a maximum transmit power, RRM does not allow any access point attached to the controller to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm, unless the access point is configured manually.

**Dynamic Channel Assignment**

Two adjacent access points on the same channel can cause either signal contention or signal collision. In a collision, data is not received by the access point. This functionality can become a problem, for example, when someone reading e-mail in a café affects the performance of the access point in a neighboring business. Even though these are completely separate networks, someone sending traffic to the café on channel 1 can disrupt communication in an enterprise using the same channel. Controllers can dynamically allocate access point channel assignments to avoid conflict and to increase capacity and performance. Channels are “reused” to avoid wasting scarce RF resources. In other words, channel 1 is allocated to a different access point far from the café, which is more effective than not using channel 1 altogether.

The controller’s dynamic channel assignment (DCA) capabilities are also useful in minimizing adjacent channel interference between access points. For example, two overlapping channels in the 802.11b/g/n band, such as 1 and 2, cannot both simultaneously use 11/54 Mbps. By effectively reassigning channels, the controller keeps adjacent channels separated.

*Note*

We recommend that you use only non-overlapping channels (1, 6, 11, and so on).

The controller examines a variety of real-time RF characteristics to efficiently handle channel assignments as follows:

- **Access point received energy**—The received signal strength measured between each access point and its nearby neighboring access points. Channels are optimized for the highest network capacity.

- **Noise**—Noise can limit signal quality at the client and access point. An increase in noise reduces the effective cell size and degrades user experience. By optimizing channels to avoid noise sources, the controller can optimize coverage while maintaining system capacity. If a channel is unusable due to excessive noise, that channel can be avoided.

- **802.11 Interference**—Interference is any 802.11 traffic that is not part of your wireless LAN, including rogue access points and neighboring wireless networks. Lightweight access points constantly scan all channels looking for sources of interference. If the amount of 802.11 interference exceeds a predefined configurable threshold (the default is 10 percent), the access point sends an alert to the controller. Using the RRM algorithms, the controller may then dynamically rearrange channel assignments to increase system performance in the presence of the interference. Such an adjustment could result in adjacent lightweight access points being on the same channel, but this setup is preferable to having the access points remain on a channel that is unusable due to an interfering foreign access point.
In addition, if other wireless networks are present, the controller shifts the usage of channels to complement the other networks. For example, if one network is on channel 6, an adjacent wireless LAN is assigned to channel 1 or 11. This arrangement increases the capacity of the network by limiting the sharing of frequencies. If a channel has virtually no capacity remaining, the controller may choose to avoid this channel. In very dense deployments in which all nonoverlapping channels are occupied, the controller does its best, but you must consider RF density when setting expectations.

- Utilization—When utilization monitoring is enabled, capacity calculations can consider that some access points are deployed in ways that carry more traffic than other access points (for example, a lobby versus an engineering area). The controller can then assign channels to improve the access point with the worst performance reported.

- Load—The load is taken into account when changing the channel structure to minimize the impact on clients currently in the wireless LAN. This metric keeps track of every access point’s transmitted and received packet counts to determine how busy the access points are. New clients avoid an overloaded access point and associate to a new access point. This parameter is disabled by default.

The controller combines this RF characteristic information with RRM algorithms to make system-wide decisions. Conflicting demands are resolved using soft-decision metrics that guarantee the best choice for minimizing network interference. The end result is optimal channel configuration in a three-dimensional space, where access points on the floor above and below play a major factor in an overall wireless LAN configuration.

In controller software releases prior to 5.1, only radios using 20-MHz channels are supported by DCA. In controller software release 5.1 or later releases, DCA is extended to support 802.11n 40-MHz channels in the 5-GHz band. 40-MHz channelization allows radios to achieve higher instantaneous data rates (potentially 2.25 times higher than 20-MHz channels). In controller software release 5.1 or later releases, you can choose if DCA works at 20 or 40 MHz.

Note

Radios using 40-MHz channels in the 2.4-GHz band are not supported by DCA.

The RRM startup mode is invoked in the following conditions:

- In a single-controller environment, the RRM startup mode is invoked after the controller is rebooted.
- In a multiple-controller environment, the RRM startup mode is invoked after an RF Group leader is elected.

RRM startup mode runs for 100 minutes (10 iterations at 10-minute intervals). The duration of the RRM startup mode is independent of the DCA interval, sensitivity, and network size. The startup mode consists of 10 DCA runs with high sensitivity (making channel changes easy and sensitive to the environment) to converge to a steady state channel plan. After the startup mode is finished, DCA continues to run at the specified interval and sensitivity.

Coverage Hole Detection and Correction

The RRM coverage hole detection algorithm can detect areas of radio coverage in a wireless LAN that are below the level needed for robust radio performance. This feature can alert you to the need for an additional (or relocated) lightweight access point.

If clients on a lightweight access point are detected at threshold levels (RSSI, failed client count, percentage of failed packets, and number of failed packets) lower than those specified in the RRM configuration, the access point sends a “coverage hole” alert to the controller. The alert indicates the existence of an area where clients are continually experiencing poor signal coverage, without having a viable access point to which to roam. The controller discriminates between coverage holes that can and
cannot be corrected. For coverage holes that can be corrected, the controller mitigates the coverage hole by increasing the transmit power level for that specific access point. The controller does not mitigate coverage holes caused by clients that are unable to increase their transmit power or are statically set to a power level because increasing their downstream transmit power might increase interference in the network.

**Note**

While transmit power control and DCA can operate in multiple-controller environments (based on RF domains), coverage hole detection is performed on a per-controller basis. In controller software release 5.2 or later releases, you can disable coverage hole detection on a per-WLAN basis. See the “Disabling Coverage Hole Detection on a WLAN (GUI)” section on page 8-69 for more information.

### Benefits of RRM

RRM produces a network with optimal capacity, performance, and reliability. It frees you from having to continually monitor the network for noise and interference problems, which can be transient and difficult to troubleshoot. RRM ensures that clients enjoy a seamless, trouble-free connection throughout the Cisco unified wireless network.

RRM uses separate monitoring and control for each deployed network: 802.11a/n and 802.11b/g/n. The RRM algorithms run separately for each radio type (802.11a/n and 802.11b/g/n). RRM uses both measurements and algorithms. RRM measurements can be adjusted using monitor intervals, but they cannot be disabled. RRM algorithms are enabled automatically but can be disabled by statically configuring channel and power assignment. The RRM algorithms run at a specified updated interval, which is 600 seconds by default.

### Guidelines and Limitations

- The OEAP 600 series access points do not support RRM. The radios for the 600 series OEAP access points are controlled through the local GUI of the 600 series access points and not through the wireless LAN controller. Attempting to control the spectrum channel or power, or disabling the radios through the controller will fail to have any effect on the 600 series OEAP.

### Configuring RRM

The controller’s preconfigured RRM settings are optimized for most deployments. However, you can modify the controller’s RRM configuration parameters at any time through either the GUI or the CLI.

**Note**

You can configure these parameters on controllers that are part of an RF group or on controllers that are not part of an RF group.

**Note**

The RRM parameters should be set to the same values on every controller in an RF group. The RF group leader can change as a result of controller reboots or depending on which radios hear each other. If the RRM parameters are not identical for all RF group members, varying results can occur when the group leader changes.
Using the controller GUI, you can configure the following RRM parameters: RF group mode, transmit power control, dynamic channel assignment, coverage hole detection, profile thresholds, monitoring channels, and monitor intervals.

**Configuring the RF Group Mode (GUI)**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Wireless &gt; 802.11a/n or 802.11b/g/n &gt; RRM &gt; RF Grouping to open the 802.11a (or 802.11b/g) RRM &gt; RF Grouping page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the <strong>Group Mode</strong> drop-down box, select the mode you want to configure for this controller. You can configure RF grouping in the following modes:</td>
</tr>
<tr>
<td></td>
<td>• auto—Sets the RF group selection to automatic update mode.</td>
</tr>
<tr>
<td></td>
<td>• leader—Sets the RF group selection to static mode, and sets this controller as the group leader.</td>
</tr>
<tr>
<td></td>
<td>• off—Sets the RF group selection off. Every controller optimizes its own access point parameters.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> A configured static leader cannot become a member of another controller until its mode is set to “auto”.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> A controller with a lower priority cannot assume the role of a group leader if a controller with a higher priority is available. Here priority is related to the processing power of the controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> We recommend that controllers participate in automatic RF grouping. You can override RRM settings without disabling automatic RF group participation. See the “Overriding RRM” section on page 13-32 for instructions.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Apply</strong> to save the configuration and Click <strong>Restart</strong> to restart RRM RF Grouping algorithm.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If you configured RF Grouping mode for this controller as a static leader, you can add group members from the RF Group Members section as follows:</td>
</tr>
<tr>
<td></td>
<td>a. In the Controller Name text box, enter the controller that you want to add as a member to this group.</td>
</tr>
<tr>
<td></td>
<td>b. In the IP Address text box, enter the IP address of the controller.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>Add Member</strong> to add the member to this group.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the member has not joined the static leader, the reason of the failure is shown in parentheses.</td>
</tr>
<tr>
<td></td>
<td>To know more about the number of access points and controllers you can add as members, see “RF Group Leader” section on page 13-27Figure 13-3.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Apply</strong> to save your changes.</td>
</tr>
</tbody>
</table>
Configuring the RF Group Mode (CLI)

**Step 1**  Configure the RF Grouping mode by entering this command:

```
config advanced {802.11a | 802.11b} group-mode {auto | leader | off | restart}
```

- **auto**—Sets the RF group selection to automatic update mode.
- **leader**—Sets the RF group selection to static mode, and sets this controller as the group leader.
- **off**—Sets the RF group selection off. Every controller optimizes its own access point parameters.
- **restart**—Restarts the RF group selection.

**Note**  A configured static leader cannot become a member of another controller until its mode is set to “auto”.

**Note**  A controller with a lower priority cannot assume the role of a group leader if a controller with higher priority is available. Here priority is related to the processing power of the controller.

**Step 2**  Add or remove a controller as a static member of the RF group (if the mode is set to “leader”) by entering the these commands:

```
config advanced {802.11a | 802.11b} group-member add controller_name controller_ip_address
config advanced {802.11a | 802.11b} group-member remove controller_name controller_ip_address
```

**Step 3**  To see RF grouping status, by entering these commands:

```
show advanced {802.11a | 802.11b} group
```

Configuring Transmit Power Control (GUI)

**Step 1**  Choose Wireless > 802.11a/n or 802.11b/g/n > RRM > TPC to open the 802.11a/n (or 802.11b/g/n) > RRM > Tx Power Control (TPC) page.

**Step 2**  Choose the Transmit Power Control version from the following options:

- **Interference Optimal Mode (TPCv2)**—For scenarios where voice calls are extensively used. Transmit power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there could be higher roaming delays and coverage hole incidents.

**Note**  We recommend that you use TCPv2 only in cases where RF issues cannot be resolved by using TCPv1. Please evaluate and test the use of TCPv2 with the assistance of Cisco Services.

- **Coverage Optimal Mode (TCPv1)**—(Default) Offers strong signal coverage and stability.

**Step 3**  Choose one of the following options from the Power Level Assignment Method drop-down list to specify the controller’s dynamic power assignment mode:

- **Automatic**—Causes the controller to periodically evaluate and, if necessary, update the transmit power for all joined access points. This is the default value.
• **On Demand**—Causes the controller to periodically evaluate the transmit power for all joined access points. However, the controller updates the power, if necessary, only when you click **Invoke Power Update Now**.

  **Note**  
  The controller does not evaluate and update the transmit power immediately after you click **Invoke Power Update Now**. It waits for the next 600-second interval. This value is not configurable.

• **Fixed**—Prevents the controller from evaluating and, if necessary, updating the transmit power for joined access points. The power level is set to the fixed value chosen from the drop-down list.

  **Note**  
  The transmit power level is assigned an integer value instead of a value in mW or dBm. The integer corresponds to a power level that varies depending on the regulatory domain, channel, and antennas in which the access points are deployed. See **Step 6 on page 13-36** for information on available transmit power levels.

  **Note**  
  For optimal performance, we recommend that you use the Automatic setting. See the “Disabling Dynamic Channel and Power Assignment Globally for a Controller” section on page 13-39 for instructions if you need to disable the controller’s dynamic channel and power settings.

**Step 4**  
Enter the maximum and minimum power level assignment values in the Maximum Power Level Assignment and Minimum Power Level Assignment text boxes.

The range for the Maximum Power Level Assignment is -10 to 30 dBm.

The range for the Minimum Power Level Assignment is -10 to 30 dBm.

**Step 5**  
In the Power Threshold text box, enter the cutoff signal level used by RRM when determining whether to reduce an access point’s power. The default value for this parameter is –70 dBm for TPCv1 and –67 dBm for TPCv2, but can be changed when access points are transmitting at higher (or lower) than desired power levels.

The range for this parameter is –80 to –50 dBm. Increasing this value (between –65 and –50 dBm) causes the access points to operate at a higher transmit power. Decreasing the value has the opposite effect.

In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.

This page also shows the following nonconfigurable transmit power level parameter settings:

• **Power Neighbor Count**—The minimum number of neighbors an access point must have for the transmit power control algorithm to run.

• **Power Assignment Leader**—The MAC address of the RF group leader, which is responsible for power level assignment.

• **Last Power Level Assignment**—The last time RRM evaluated the current transmit power level assignments.

**Step 6**  
Click **Apply** to commit your changes.

**Step 7**  
Click **Save Configuration** to save your changes.
Configuring Off-Channel Scanning Defer

This section contains the following sections:

- Information About Off-Channel Scanning Defer, page 13-9
- Configuring Off-Channel Scanning Defer for WLANs, page 13-9

Information About Off-Channel Scanning Defer

In deployments with certain power-save clients, you sometimes need to defer RRM's normal off-channel scanning to avoid missing critical information from low-volume clients (for example, medical devices that use power-save mode and periodically send telemetry information). This feature improves the way that QoS interacts with the RRM scan defer feature.

You can use a client's WMM UP marking to configure the access point to defer off-channel scanning for a configurable period of time if it receives a packet marked UP.

Off-Channel Scanning Defer is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off-Channel Scanning Defer is responsible for rogue detection. Devices that need to defer Off-Channel Scanning Defer should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that Off-Channel Defer scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP Off-Channel Scanning Defer, such as monitor access points, or other access points in the same location that do not have this WLAN assigned.

Assignment of a QoS policy (bronze, silver, gold, and platinum) to a WLAN affects how packets are marked on the downlink connection from the access point regardless of how they were received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. The marking results of each QoS policy are as follows:

- Bronze marks all downlink traffic to UP= 1.
- Silver marks all downlink traffic to UP= 0.
- Gold marks all downlink traffic to UP=4.
- Platinum marks all downlink traffic to UP=6.

Configuring Off-Channel Scanning Defer for WLANs

This section contains the following sections:

- Configuring Off-Channel Scanning Defer for a WLAN (GUI), page 13-10
- Configuring Off Channel Scanning Defer for a WLAN (CLI), page 13-10
- Configuring Dynamic Channel Assignment (GUI), page 13-10
- Configuring Coverage Hole Detection (GUI), page 13-14
- Configuring RRM Profile Thresholds, Monitoring Channels, and Monitor Intervals (GUI), page 13-16
- Configuring RRM (CLI), page 13-18
- Viewing RRM Settings (CLI), page 13-22
- Debug RRM Issues (CLI), page 13-25
Configuring Off-Channel Scanning Defer for a WLAN (GUI)

Step 1  Choose WLANs to open the WLANs page.
Step 2  Click the ID number of the WLAN to which you want to configure off-channel scanning Defer.
Step 3  Choose the Advanced tab from the WLANs > Edit page.
Step 4  From the Off Channel Scanning Defer section, set the Scan Defer Priority by clicking on the priority argument.
Step 5  Set the time in milliseconds in the Scan Defer Time text box. Valid values are 100 through 60000. The default value is 100 milliseconds.
Step 6  Click Apply to save your configuration.

Configuring Off Channel Scanning Defer for a WLAN (CLI)

Step 1  Assign a defer-priority for the channel scan by entering this command:
   `config wlan channel-scan defer-priority priority [enable | disable] WLAN-id`
   The valid range for the priority argument is 0 to 7.
   The priority is 0 to 7 (this value should be set to 6 on the client and on the WLAN).
   Use this command to configure the amount of time that scanning will be deferred following an UP packet in the queue.
Step 2  Assign the channel scan defer time (in milliseconds) by entering this command:
   `config wlan channel-scan defer-time msec WLAN-id`
   The time value is in miliseconds (ms) and the valid range is 100 (default) to 60000 (60 seconds). This setting should match the requirements of the equipment on your wireless LAN.
   You can also configure this feature on the controller GUI by selecting WLANs, and either edit an existing WLAN or create a new one.

Configuring Dynamic Channel Assignment (GUI)

To specify the channels that the dynamic channel assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning using the controller GUI, follow these steps:

Note  This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

Step 1  Disable the 802.11a/n or 802.11b/g/n network as follows:
   a. Choose Wireless > 802.11a/n or 802.11b/g/n > Network to open the 802.11a (or 802.11b/g) Global Parameters page.
   b. Unselect the 802.11a (or 802.11b/g) Network Status check box.
   c. Click Apply to commit your changes.
Step 2  Choose Wireless > 802.11a/n or 802.11b/g/n > RRM > DCA to open the 802.11a (or 802.11b/g) > RRM > Dynamic Channel Assignment (DCA) page.

Figure 13-1  802.11a > RRM > Dynamic Channel Assignment (DCA) Page

Step 3  Choose one of the following options from the Channel Assignment Method drop-down list to specify the controller’s DCA mode:

- **Automatic**—Causes the controller to periodically evaluate and, if necessary, update the channel assignment for all joined access points. This is the default value.

- **Freeze**—Causes the controller to evaluate and update the channel assignment for all joined access points, if necessary, but only when you click **Invoke Channel Update Once**.

  **Note**  The controller does not evaluate and update the channel assignment immediately after you click **Invoke Channel Update Once**. It waits for the next interval to elapse.

- **OFF**—Turns off DCA and sets all access point radios to the first channel of the band, which is the default value. If you choose this option, you must manually assign channels on all radios.

  **Note**  For optimal performance, we recommend that you use the Automatic setting. See the “Disabling Dynamic Channel and Power Assignment Globally for a Controller” section on page 13-39 for instructions if you need to disable the controller’s dynamic channel and power settings.

Step 4  From the Interval drop-down list, choose one of the following options to specify how often the DCA algorithm is allowed to run: **10 minutes, 1 hour, 2 hours, 3 hours, 4 hours, 6 hours, 8 hours, 12 hours, or 24 hours**. The default value is 10 minutes.

  **Note**  If your controller supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.
Step 5  From the AnchorTime drop-down list, choose a number to specify the time of day when the DCA algorithm is to start. The options are numbers between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.

Step 6  Select the **Avoid Foreign AP Interference** check box to cause the controller’s RRM algorithms to consider 802.11 traffic from foreign access points (those not included in your wireless network) when assigning channels to lightweight access points, or unselect it to disable this feature. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign access points. The default value is selected.

Step 7  Select the **Avoid Cisco AP Load** check box to cause the controller’s RRM algorithms to consider 802.11 traffic from Cisco lightweight access points in your wireless network when assigning channels, or unselect it to disable this feature. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load. The default value is unselected.

Step 8  Select the **Avoid Non-802.11a (802.11b) Noise** check box to cause the controller’s RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight access points, or unselect it to disable this feature. For example, RRM may have access points avoid channels with significant interference from nonaccess point sources, such as microwave ovens. The default value is selected.

Step 9  Select the **Avoid Persistent Non-WiFi Interference** check box to enable the controller to ignore persistent non-WiFi interference.

Step 10 From the **DCA Channel Sensitivity** drop-down list, choose one of the following options to specify how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channels:

- **Low**—The DCA algorithm is not particularly sensitive to environmental changes.
- **Medium**—The DCA algorithm is moderately sensitive to environmental changes.
- **High**—The DCA algorithm is highly sensitive to environmental changes.

The default value is Medium. The DCA sensitivity thresholds vary by radio band, as noted in Table 13-1.

<table>
<thead>
<tr>
<th>Option</th>
<th>2.4-GHz DCA Sensitivity Threshold</th>
<th>5-GHz DCA Sensitivity Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>5 dB</td>
<td>5 dB</td>
</tr>
<tr>
<td>Medium</td>
<td>10 dB</td>
<td>15 dB</td>
</tr>
<tr>
<td>Low</td>
<td>20 dB</td>
<td>20 dB</td>
</tr>
</tbody>
</table>

Step 11  For 802.11a/n networks only, choose one of the following channel width options to specify the channel bandwidth supported for all 802.11n radios in the 5-GHz band:

- **20 MHz**—The 20-MHz channel bandwidth (default)
- **40 MHz**—The 40-MHz channel bandwidth

**Note**  If you choose 40 MHz, be sure to choose at least two adjacent channels from the DCA Channel List in Step 13 (for example, a primary channel of 36 and an extension channel of 40). If you choose only one channel, that channel is not used for 40-MHz channel width.
If you choose 40 MHz, you can also configure the primary and extension channels used by individual access points. See the “Statically Assigning Channel and Transmit Power Settings to Access Point Radios” section on page 13-33 for configuration instructions.

To override the globally configured DCA channel width setting, you can statically configure an access point’s radio for 20- or 40-MHz mode on the 802.11a/n Cisco APs > Configure page. If you then change the static RF channel assignment method to WLC Controlled on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

If you choose 40 MHz on the A radio, you cannot pair channels 116, 140, and 165 with any other channels.

This page also shows the following nonconfigurable channel parameter settings:

- Channel Assignment Leader—The MAC address of the RF group leader, which is responsible for channel assignment.
- Last Auto Channel Assignment—The last time RRM evaluated the current channel assignments.

Select the Avoid check for non-DFS channel to enable the controller to avoid checks for non-DFS channels. DCA configuration requires at least one non-DFS channel in the list. In the EU countries, outdoor deployments do not support non-DFS channels. Customers based in EU or regions with similar regulations must enable this option or at least have one non-DFS channel in the DCA list even if the channel is not supported by the APs.

This parameter is applicable only for deployments having outdoor access points such as 1522 and 1524.

In the DCA Channel List area, the DCA Channels text box shows the channels that are currently selected. To choose a channel, select its check box in the Select column. To exclude a channel, unselect its check box.

The ranges are as follows:
- 802.11a/n—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165, 190, 196
- 802.11b/g/n—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

The defaults are as follows:
- 802.11a/n—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161
- 802.11b/g/n—1, 6, 11

These extended UNII-2 channels in the 802.11a/n band do not appear in the channel list: 100, 104, 108, 112, 116, 132, 136, and 140. If you have Cisco Aironet 1520 series mesh access points in the -E regulatory domain, you must include these channels in the DCA channel list before you start operation. If you are upgrading from a previous release, verify that these channels are included in the DCA channel list. To include these channels in the channel list, select the Extended UNII-2 Channels check box.
Step 14 If you are using Cisco Aironet 1520 series mesh access points in your network, you need to set the 4.9-GHz channels in the 802.11a/n band on which they are to operate. The 4.9-GHz band is for public safety client access traffic only. To choose a 4.9-GHz channel, select its check box in the Select column. To exclude a channel, unselect its check box.

The ranges are as follows:
802.11a/n—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26

The defaults are as follows:
802.11a/n—20, 26

Step 15 Click Apply to commit your changes.

Step 16 Reenable the 802.11a/n or 802.11b/g/n network as follows:

a. Choose Wireless > 802.11a/n or 802.11b/g/n > Network to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Select the 802.11a (or 802.11b/g) Network Status check box.

c. Click Apply to commit your changes.

Step 17 Click Save Configuration to save your changes.

Note To see why the DCA algorithm changed channels, choose Monitor and then choose View All under Most Recent Traps. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change.

Configuring Coverage Hole Detection (GUI)

Note In controller software release 5.2 or later releases, you can disable coverage hole detection on a per-WLAN basis. See the “Disabling Accounting Servers per WLAN (GUI)” section on page 8-69 for more information.

Step 1 Disable the 802.11a/n or 802.11b/g/n network as follows:

a. Choose Wireless > 802.11a/n or 802.11b/g/n > Network to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Unselect the 802.11a (or 802.11b/g) Network Status check box.

c. Click Apply to commit your changes.

Step 2 Choose Wireless > 802.11a/n or 802.11b/g/n > RRM > Coverage to open the 802.11a (or 802.11b/g) > RRM > Coverage page.
Figure 13-2  802.11a > RRM > Coverage Page

Step 3  Select the Enable Coverage Hole Detection check box to enable coverage hole detection, or unselect it to disable this feature. If you enable coverage hole detection, the controller automatically determines, based on data received from the access points, if any access points have clients that are potentially located in areas with poor coverage. The default value is selected.

Step 4  In the Data RSSI text box, enter the minimum receive signal strength indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –80 dBm. The access point takes data RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.

Step 5  In the Voice RSSI text box, enter the minimum receive signal strength indication (RSSI) value for voice packets received by the access point. The value that you enter is used to identify coverage holes within your network. If the access point receives a packet in the voice queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –75 dBm. The access point takes voice RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.

Step 6  In the Min Failed Client Count per AP text box, enter the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold. The valid range is 1 to 75, and the default value is 3.

Step 7  In the Coverage Exception Level per AP text box, enter the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. The valid range is 0 to 100%, and the default value is 25%.

Note  If both the number and percentage of failed packets exceed the values configured for Failed Packet Count and Failed Packet Percentage (configurable through the controller CLI) for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes. False positives are generally due to the poor roaming logic implemented on most clients. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the Min Failed Client Count per AP and Coverage Exception Level per AP text boxes over a 90-second period. The controller determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Step 8  Click Apply to commit your changes.
Step 9  Reenable the 802.11a/n or 802.11b/g/n network as follows:

a. Choose **Wireless > 802.11a/n or 802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Select the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

Step 10  Click **Save Configuration** to save your changes.

---

**Configuring RRM Profile Thresholds, Monitoring Channels, and Monitor Intervals (GUI)**

Step 1  Choose **Wireless > 802.11a/n or 802.11b/g/n > RRM > General** to open the 802.11a (or 802.11b/g) > RRM > General page.

**Figure 13-3  802.11a > RRM > General Page**

---

Step 2  Configure profile thresholds used for alarming as follows:

*Note* The profile thresholds have no bearing on the functionality of the RRM algorithms. Lightweight access points send an SNMP trap (or an alert) to the controller when the values set for these threshold parameters are exceeded.

a. In the Interference text box, enter the percentage of interference (802.11 traffic from sources outside of your wireless network) on a single access point. The valid range is 0 to 100%, and the default value is 10%.

b. In the Clients text box, enter the number of clients on a single access point. The valid range is 1 to 75, and the default value is 12.

c. In the Noise text box, enter the level of noise (non-802.11 traffic) on a single access point. The valid range is –127 to 0 dBm, and the default value is –70 dBm.
d. In the Utilization text box, enter the percentage of RF bandwidth being used by a single access point. The valid range is 0 to 100%, and the default value is 80%.

**Step 3**

From the Channel List drop-down list, choose one of the following options to specify the set of channels that the access point uses for RRM scanning:

- **All Channels**—RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation.
- **Country Channels**—RRM channel scanning occurs only on the data channels in the country of operation. This is the default value.
- **DCA Channels**—RRM channel scanning occurs only on the channel set used by the DCA algorithm, which by default includes all of the non-overlapping channels allowed in the country of operation. However, you can specify the channel set to be used by DCA if desired. To do so, follow the instructions in the “Dynamic Channel Assignment” section on page 13-3.

**Step 4**

Configure monitor intervals as follows:

a. In the Channel Scan Interval text box, enter (in seconds) the sum of the time between scans for each channel within a radio band. The entire scanning process takes 50 ms per channel, per radio and runs at the interval configured here. The time spent listening on each channel is determined by the non-configurable 50-ms scan time and the number of channels to be scanned. For example, in the U.S. all 11 802.11b/g/n channels are scanned for 50 ms each within the default 180-second interval. So every 16 seconds, 50 ms is spent listening on each scanned channel (180/11 = ~16 seconds). The Channel Scan Interval parameter determines the interval at which the scanning occurs. The valid range is 60 to 3600 seconds, and the default value is 60 seconds for 802.11a radios and 180 seconds for the 802.11b/g/n radios.

**Note**

If your controller supports only OfficeExtend access points, we recommend that you set the channel scan interval to 1800 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.

b. In the Neighbor Packet Frequency text box, enter (in seconds) how frequently neighbor packets (messages) are sent, which eventually builds the neighbor list. The valid range is 60 to 3600 seconds, and the default value is 60 seconds.

**Note**

If your controller supports only OfficeExtend access points, we recommend that you set the neighbor packet frequency to 600 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.

**Note**

In controller software release 4.1.185.0 or later releases, if the access point radio does not receive a neighbor packet from an existing neighbor within 60 minutes, the controller deletes that neighbor from the neighbor list. In controller software releases prior to 4.1.185.0, the controller waits only 20 minutes before deleting an unresponsive neighbor radio from the neighbor list.

**Step 5**

Click **Apply** to commit your changes.

**Step 6**

Click **Save Configuration** to save your changes.
Configuring RRM (CLI)

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

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

**Step 2** Choose the Transmit Power Control version by entering this command:

```
config advanced {802.11a | 802.11b} tpc-version {1 | 2}
```

where:

- TPCv1: Coverage-optimal—(Default) Offers strong signal coverage and stability.
- TPCv2: Interference-optimal—For scenarios where voice calls are extensively used. Tx power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there can be higher roaming delays and coverage hole incidents.

**Step 3** Perform one of the following to configure transmit power control:

- To have RRM automatically set the transmit power for all 802.11a/n or 802.11b/g/n radios at periodic intervals, enter this command:

```
config {802.11a | 802.11b} txPower global auto
```

- To have RRM automatically reset the transmit power for all 802.11a/n or 802.11b/g/n radios one time, enter this command:

```
config {802.11a | 802.11b} txPower global once
```

- To configure the transmit power range that overrides the Transmit Power Control algorithm, use this command to enter the maximum and minimum transmit power used by RRM:

```
config {802.11a | 802.11b} txPower global {max | min} txpower
```

where `txpower` is a value from –10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

If you configure a maximum transmit power, RRM does not allow any access point to exceed this transmit power (whether the maximum is set at RRM startup, or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm, unless the access point is configured manually.

- To manually change the default transmit power setting, enter this command:

```
config advanced {802.11a | 802.11b} {tpcv1-thresh | tpcv2-thresh} threshold
```

where `threshold` is a value from –80 to –50 dBm. Increasing this value causes the access points to operate at higher transmit power rates. Decreasing the value has the opposite effect.

In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm in order to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients may have difficulty processing a large number of BSSIDs or a high beacon rate and may exhibit problematic behavior with the default threshold.

- To configure the Transmit Power Control Version 2 on a per-channel basis, enter the following command:
Step 4  Perform one of the following to configure dynamic channel assignment (DCA):

- To have RRM automatically configure all 802.11a/n or 802.11b/g/n channels based on availability and interference, enter this command:

  ```
  config {802.11a | 802.11b} channel global auto
  ```

- To have RRM automatically reconfigure all 802.11a/n or 802.11b/g/n channels one time based on availability and interference, enter this command:

  ```
  config {802.11a | 802.11b} channel global once
  ```

- To disable RRM and set all channels to their default values, enter this command:

  ```
  config {802.11a | 802.11b} channel global off
  ```

- To specify the channel set used for DCA, enter this command:

  ```
  config advanced {802.11a | 802.11b} channel {add | delete} channel_number
  ```

  You can enter only one channel number per command. This command is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

Step 5  Configure additional DCA parameters by entering these commands:

- To specify the time of day when the DCA algorithm is to start, enter this command:

  ```
  config advanced {802.11a | 802.11b} channel dca anchor-time value
  ```

  value is a number between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.

- To specify how often the DCA algorithm is allowed to run, enter this command:

  ```
  config advanced {802.11a | 802.11b} channel dca interval value
  ```

  value is one of the following: 1, 2, 3, 4, 6, 8, 12, or 24 hours or 0, which is the default value of 10 minutes (or 600 seconds).

  **Note**  If your controller supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.

- To specify how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channel, enter this command:

  ```
  config advanced {802.11a | 802.11b} channel dca sensitivity {low | medium | high}
  ```

  low means that the DCA algorithm is not particularly sensitive to environmental changes.

  medium means that the DCA algorithm is moderately sensitive to environmental changes.

  high means that the DCA algorithm is highly sensitive to environmental changes.

The DCA sensitivity thresholds vary by radio band, as noted in Table 13-2.

**Table 13-2  DCA Sensitivity Thresholds**

<table>
<thead>
<tr>
<th>Option</th>
<th>2.4-GHz DCA Sensitivity Threshold</th>
<th>5-GHz DCA Sensitivity Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>5 dB</td>
<td>5 dB</td>
</tr>
<tr>
<td>Medium</td>
<td>10 dB</td>
<td>15 dB</td>
</tr>
<tr>
<td>Low</td>
<td>20 dB</td>
<td>20 dB</td>
</tr>
</tbody>
</table>
Chapter 13 Configuring Radio Resource Management

• config advanced 802.11a channel dca chan-width-11n {20 | 40}—Configures the DCA channel width for all 802.11n radios in the 5-GHz band.

where

- 20 sets the channel width for 802.11n radios to 20 MHz. This is the default value.
- 40 sets the channel width for 802.11n radios to 40 MHz.

Note If you choose 40, be sure to set at least two adjacent channels in the config advanced 802.11a channel {add | delete} channel_number command in Step 4 (for example, a primary channel of 36 and an extension channel of 40). If you set only one channel, that channel is not used for 40-MHz channel width.

Note If you choose 40, you can also configure the primary and extension channels used by individual access points. See the “Statically Assigning Channel and Transmit Power Settings (CLI)” section on page 13-37 for configuration instructions.

Note To override the globally configured DCA channel width setting, you can statically configure an access point’s radio for 20- or 40-MHz mode using the config 802.11a chan_width Cisco_AP {20 | 40} command. If you then change the static configuration to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

• config advanced {802.11a | 802.11b} channel outdoor-ap-dca {enable | disable}—Enables or disables to the controller to avoid checks for non-DFS channels.

Note This parameter is applicable only for deployments having outdoor access points such as 1522 and 1524.

• config advanced {802.11a | 802.11b} channel foreign {enable | disable}—Enables or disables foreign access point interference avoidance in the channel assignment.

• config advanced {802.11a | 802.11b} channel load {enable | disable}—Enables or disables load avoidance in the channel assignment.

• config advanced {802.11a | 802.11b} channel noise {enable | disable}—Enables or disables noise avoidance in the channel assignment.

• config advanced {802.11a | 802.11b} channel update—Initiates an update of the channel selection for every Cisco access point.

Step 6 Configure coverage hole detection by entering these commands:

Note In controller software release 5.2 or later releases, you can disable coverage hole detection on a per-WLAN basis. See the “Disabling Coverage Hole Detection per WLAN” section on page 8-69 for more information.
Chapter 13 Configuring Radio Resource Management

- `config advanced {802.11a | 802.11b} coverage {enable | disable}`—Enables or disables coverage hole detection. If you enable coverage hole detection, the controller automatically determines, based on data received from the access points, if any access points have clients that are potentially located in areas with poor coverage. The default value is enabled.

- `config advanced {802.11a | 802.11b} coverage {data | voice} rssi-threshold rssi`—Specifies the minimum receive signal strength indication (RSSI) value for packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data or voice queue with an RSSI value below the value you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –80 dBm for data packets and –75 dBm for voice packets. The access point takes RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.

- `config advanced {802.11a | 802.11b} coverage level global clients`— Specifies the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold. The valid range is 1 to 75, and the default value is 3.

- `config advanced {802.11a | 802.11b} coverage exception global percent`—Specifies the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. The valid range is 0 to 100%, and the default value is 25%.

- `config advanced {802.11a | 802.11b} coverage {data | voice} packet-count packets`—Specifies the minimum failure count threshold for uplink data or voice packets. The valid range is 1 to 255 packets, and the default value is 10 packets.

- `config advanced {802.11a | 802.11b} coverage {data | voice} fail-rate percent`— Specifies the failure rate threshold for uplink data or voice packets. The valid range is 1 to 100%, and the default value is 20%.

**Note** If both the number and percentage of failed packets exceed the values entered in the `packet-count` and `fail-rate` commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes. False positives are generally due to the poor roaming logic implemented on most clients. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the `coverage level global` and `coverage exception global` commands over a 90-second period. The controller determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

**Step 7** Enable the 802.11a/n or 802.11b/g/n network by entering this command:

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

**Note** To enable the 802.11g network, enter `config 802.11b 11gSupport enable` after the `config 802.11b enable network` command.

**Step 8** Save your settings by entering this command:

```
save config
```
Viewing RRM Settings (CLI)

To see 802.11a/n and 802.11b/g/n RRM settings, use these commands:

```
show advanced {80.11a | 80.11b} ?
```

where `?` is one of the following:

- **ccx {global | Cisco_AP}**—Shows the CCX RRM configuration.

  802.11a Client Beacon Measurements:
  disabled

- **channel**—Shows the channel assignment configuration and statistics.

  Automatic Channel Assignment
  Channel Assignment Mode........................ ONCE
  Channel Update Interval.......................... 600 seconds
  Anchor time (Hour of the day).................. 20
  Channel Update Count............................ 0
  Channel Update Contribution..................... S.IU
  Channel Assignment Leader..................... 00:0b:85:40:90:c0
  Last Run....................................... 532 seconds ago
  DCA Sensitivity Level.......................... MEDIUM (20 dB)
  DCA 802.11n Channel Width...................... 40 MHz
  Channel Energy Levels
  Minimum...................................... unknown
  Average...................................... unknown
  Maximum...................................... unknown
  Channel Dwell Times
  Minimum...................................... unknown
  Average...................................... unknown
  Maximum...................................... unknown
  Auto-RF Allowed Channel List................... 36,40
  Auto-RF Unused Channel List.................... 44,48,52,56,60,64,100,104,  
                                             108,112,116,132,136,140,149,  
                                             153,157,161,165,190,196
  DCA Outdoor AP option......................... Disabled

- **coverage**—Shows the coverage hole detection configuration and statistics.

  Coverage Hole Detection
  802.11a Coverage Hole Detection Mode.......... Enabled
  802.11a Coverage Voice Packet Count............ 10 packets
  802.11a Coverage Voice Packet Percentage...... 20%
  802.11a Coverage Voice RSSI Threshold......... -75 dBm
  802.11a Coverage Data Packet Count............. 10 packets
  802.11a Coverage Data Packet Percentage....... 20%
  802.11a Coverage Data RSSI Threshold.......... -80 dBm
  802.11a Global coverage exception level....... 25%
  802.11a Global client minimum exception lev. 3 clients

- **group**—Shows the configuration and statistics for Radio RF Grouping.

  Radio RF Grouping
  802.11a Group Mode............................. AUTO
  802.11a Group Update Interval.................. 600 seconds
  802.11a Group Leader........................... CTRL1 (209.165.200.226)
  802.11a Group Member........................... CTRL1 (209.165.200.226)
  802.11a Last Run............................... 229 seconds ago

- **logging**—Shows the RF event and performance logging.

  RF Event and Performance Logging
  Channel Update Logging........................ Off
Coverage Profile Logging ......................... Off
Foreign Profile Logging .......................... Off
Load Profile Logging ............................. Off
Noise Profile Logging ............................ Off
Performance Profile Logging ....................... Off
TxPower Update Logging ............................ Off

- **monitor**—Shows the Cisco radio monitoring.

  Default 802.11a AP monitoring
  802.11a Monitor Mode ......................... enable
  802.11a Monitor Channels ..................... Country channels
  802.11a AP Coverage Interval .................. 180 seconds
  802.11a AP Load Interval ....................... 60 seconds
  802.11a AP Noise Interval ...................... 180 seconds
  802.11a AP Signal Strength Interval .......... 60 seconds

- **profile (global | Cisco_AP)**—Shows the access point performance profiles.

  Default 802.11a AP performance profiles
  802.11a Global Interference threshold .......... 10%  
  802.11a Global noise threshold ................ -70 dBm
  802.11a Global RF utilization threshold ....... 80%
  802.11a Global throughput threshold .......... 1000000 bps
  802.11a Global clients threshold ............. 12 clients

- **receiver**—Shows the 802.11a/n or 802.11b/g/n receiver configuration and statistics.

  802.11a Advanced Receiver Settings
  RxsStart : Signal Threshold .......................... 15
  RxsStart : Signal Jump Threshold ..................... 5
  RxsStart : Preamble Power Threshold .................. 2
  RxsRestart: Signal Jump Status .................... Enabled
  RxsRestart: Signal Jump Threshold ................... 10
  TxStomp  : Low RSSI Status ......................... Enabled
  TxStomp  : Low RSSI Threshold ....................... 30
  TxStomp  : Wrong BSSID Status ...................... Enabled
  TxStomp  : Wrong BSSID Data Only Status .......... Enabled
  RxAbsrt  : Raw Power Drop Status .................... Disabled
  RxAbsrt  : Raw Power Drop Threshold .............. 10
  RxAbsrt  : Low RSSI Status ......................... Disabled
  RxAbsrt  : Low RSSI Threshold ...................... 0
  RxAbsrt  : Wrong BSSID Status ..................... Disabled
  RxAbsrt  : Wrong BSSID Data Only Status .......... Disabled
  RXAbort  : Raw Power Drop Status ................... Disabled
  RXAbort  : Raw Power Drop Threshold .............. 10
  RXAbort  : Low RSSI Status ......................... Disabled
  RXAbort  : Low RSSI Threshold ...................... 0
  RXAbort  : Wrong BSSID Status ..................... Disabled
  RXAbort  : Wrong BSSID Data Only Status .......... Disabled

  pico-cell-V2 parameters in dbm units:

  RxSensitivity: Min,Max,Current RxSense Thres........ 0,0,0
  CCA Threshold: Min,Max,Current Clear Channel...... 0,0,0
  Tx Pwr: Min,Max,Current Transmit Power for A.... 0,0,0

- **summary**—Shows the configuration and statistics of the 802.11a/n or 802.11b/g/n access points.

  Leader RRM Information

  AP_1 : [53:1d:c0] Ch 36  TxPower 14dBm (Level 1)  CHDM 0dBm AP Util 100% dBm
  [14/13/12/10/8/6/4/2]
  RxsNbrs:: total 6 [ 7:60] [ 2:69] [ 5:80] [ 4:80] [ 3:81] [ 6:90]
  TxNbrs:: total 6 [ 7:57] [ 3:62] [ 4:71] [ 6:78] [ 2:79] [ 5:1]
  AP_2 : [85:c6:20] Ch157  TxPower 17dBm (Level 1)  CHDM 0dBm AP Util 100% dBm
  [17/14/11/8/5/2/-1/1]
  RxsNbrs:: total 6 [ 4:29] [ 7:42] [ 5:42] [ 3:55] [ 6:78] [ 1:79]
  TxNbrs:: total 6 [ 4:24] [ 7:35] [ 3:39] [ 5:40] [ 1:69] [ 6:-]
### Member RRM Information

<table>
<thead>
<tr>
<th>AP Name</th>
<th>MAC Address</th>
<th>Admin</th>
<th>Oper</th>
<th>Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap5</td>
<td>68:bd:ab:85:c6:20</td>
<td>ENABLED</td>
<td>UP</td>
<td>157</td>
</tr>
<tr>
<td>1/7</td>
<td>(17 dBm)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ap7</td>
<td>64:d9:89:42:15:10</td>
<td>DISABLED</td>
<td>DOWN</td>
<td>36</td>
</tr>
<tr>
<td>1/7</td>
<td>(14 dBm)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ap1</td>
<td>c4:7d:4f:53:1d:c0</td>
<td>ENABLED</td>
<td>UP</td>
<td>36</td>
</tr>
<tr>
<td>1/8</td>
<td>(14 dBm)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ap6</td>
<td>10:8c:cf:b0:dc:d0</td>
<td>ENABLED</td>
<td>UP</td>
<td>36</td>
</tr>
<tr>
<td>*7/7</td>
<td>(-1 dBm)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ap8</td>
<td>64:d9:89:42:15:60</td>
<td>ENABLED</td>
<td>UP</td>
<td>36</td>
</tr>
<tr>
<td>2/7</td>
<td>(11 dBm)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ap4</td>
<td>00:1a:a2:fd:76:20</td>
<td>ENABLED</td>
<td>UP</td>
<td>52*</td>
</tr>
<tr>
<td>*8/8</td>
<td>(-1 dBm)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ap3</td>
<td>00:1d:71:21:23:30</td>
<td>ENABLED</td>
<td>UP</td>
<td>60</td>
</tr>
<tr>
<td>1/8</td>
<td>(17 dBm)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ap2</td>
<td>00:1e:4a:55:55:10</td>
<td>ENABLED</td>
<td>UP</td>
<td>157</td>
</tr>
<tr>
<td>1/8</td>
<td>(17 dBm)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **txpower**—Shows the transmit power assignment configuration and statistics.

---

### Leader Automatic Transmit Power Assignment

- **Transmit Power Assignment Mode**................. AUTO
- **Transmit Power Update Interval**............... 600 seconds
- **Transmit Power Threshold**...................... -70 dBm
- **Transmit Power Neighbor Count**................ 3 APs
- **Min Transmit Power**............................. -10 dBm
- **Max Transmit Power**............................. 30 dBm
- **Transmit Power Update Contribution**............ SNI
- **Transmit Power Assignment Leader**.............. rangans (9.6.137.10)
- **Last Run**..................................... 507 seconds ago
- **TPC Mode**...................................... Version 1
- **TPCv2 Target RSSI**............................. -67.0 dBm
- **TPCv2 VoWLAN Guide RSSI**....................... -67.0 dBm
- **TPCv2 SOP**.................................... -85.0 dBm
- **TPCv2 Default Client Ant Gain**................ 0.0 dBi
- **TPCv2 Path Loss Decay Factor**.................. 3.6
- **TPCv2 Search Intensity**........................ 10 Iterations
Debug RRM Issues (CLI)

Use these commands to troubleshoot and verify RRM behavior:

```
debug airewave-director ?
```

where ? is one of the following:

- `all`—Enables debugging for all RRM logs.
- `channel`—Enables debugging for the RRM channel assignment protocol.
- `detail`—Enables debugging for RRM detail logs.
- `error`—Enables debugging for RRM error logs.
- `group`—Enables debugging for the RRM grouping protocol.
- `manager`—Enables debugging for the RRM manager.
- `message`—Enables debugging for RRM messages.
- `packet`—Enables debugging for RRM packets.
- `power`—Enables debugging for the RRM power assignment protocol as well as coverage hole detection.
- `profile`—Enables debugging for RRM profile events.
- `radar`—Enables debugging for the RRM radar detection/avoidance protocol.
- `rf-change`—Enables debugging for RRM RF changes.

## Configuring RRM Neighbor Discovery Packets

The Cisco Neighbor Discovery Packet (NDP) is the fundamental tool for RRM and other wireless applications that provides information about the neighbor radio information. Starting in the 7.0.116.0 releases and later, you can configure the controller to encrypt neighbor discovery packets.

This feature enables you to be compliant with the PCI specifications.

### Important About RRM NDP and RF Grouping

An RF group can only be formed between controllers that have the same encryption mechanism. That is, an access point associated to a controller that is encrypted can not be neighbors with an access point associated to a controller that is not encrypted. The two controllers and their access points will not recognize each other as neighbors and cannot form an RF group. It is possible to assign two controllers in a static RF group configuration that has mismatched encryption settings. In this case, the two controllers do not function as a single RF group because the access points belonging to the mismatched controllers do not recognize one another as neighbors in the group.

For more information on RF groups, see the “Configuring RF Groups” section on page 13-29.

---

**Caution**

Inter-operation between 7.0.116.0 release and earlier releases: Because the NDP feature has been introduced from the 7.0.116.0 release, only transparent settings can ensure a RF-group formation between these cases. Previous controller releases do not have the NDP encryption mechanism.
Configuring RRM NDP (CLI)

To configure RRM NDP using the controller CLI, follow these steps:

```
config advanced 802.11{a|b} monitor ndp-mode {protected | transparent}
```

This command configures NDP mode. By default, the mode is set to “transparent”. The following options are available:

- Protected—Packets are encrypted.
- Transparent—Packets are sent as is.

Use the following command to see the discovery type:

```
show advanced 802.11{a|b} monitor
```

Configuring RF Groups

This section contains the following topics:

- Information About RF Groups, page 13-26
- Guidelines and Limitations, page 13-28
- Configuring RF Groups, page 13-29

Information About RF Groups

An RF group is a logical collection of controllers 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 controllers into a single RF group enable the RRM algorithms to scale beyond the capabilities of a single controller.

Lightweight access points periodically send out neighbor messages over the air. Access points using the the same RF group name validate messages from each other.

When access points on different controllers hear validated neighbor messages at a signal strength of –80 dBm or stronger, the controllers dynamically form an RF neighborhood in auto mode. In static mode, the leader is manually selected and the members are added to the RF Group. To know more about RF Group modes, see the “RF Group Leader” section on page 13-27.

RF groups and mobility groups are similar in that they both define clusters of controllers, 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 controller redundancy. See Chapter 15, “Configuring Mobility Groups,” for more information on mobility groups.
RF Group Leader

Starting in the 7.0.116.0 release, the RF Group Leader can be configured in two ways as follows:

- **Auto Mode**—In this mode, the members of an RF group elect an RF group leader to maintain a “master” power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or if RF group members experience major changes).

- **Static Mode**—In this mode, the user selects a controller as an RF group leader manually. In this mode, the leader and the members are manually configured and are therefore fixed. If the members are unable to join the RF group, the reason is indicated. The leader tries to establish a connection with a member every 1 minute if the member has not joined in the previous attempt.

The RF group leader analyzes real-time radio data collected by the system, calculates the power and channel assignments, and sends them to each of the controllers in the RF group. The RRM algorithms ensure system-wide stability and restrain channel and power scheme changes to the appropriate local RF neighborhoods.

In controller software releases prior to 6.0, the dynamic channel assignment (DCA) search algorithm attempts to find a good channel plan for the radios associated to controllers in the RF group, but it does not adopt a new channel plan unless it is considerably better than the current plan. The channel metric of the worst radio in both plans determines which plan is adopted. Using the worst-performing radio as the single criterion for adopting a new channel plan can result in pinning or cascading problems.

Pinning occurs when the algorithm could find a better channel plan for some of the radios in an RF group but is prevented from pursuing such a channel plan change because the worst radio in the network does not have any better channel options. The worst radio in the RF group could potentially prevent other radios in the group from seeking better channel plans. The larger the network, the more likely pinning becomes.

Cascading occurs when one radio’s channel change results in successive channel changes to optimize the remaining radios in the RF neighborhood. Optimizing these radios could lead to their neighbors and their neighbors’ neighbors having a suboptimal channel plan and triggering their channel optimization. This effect could propagate across multiple floors or even multiple buildings, if all the access point radios belong to the same RF group. This change results in considerable client confusion and network instability.

The main cause of both pinning and cascading is the way in which the search for a new channel plan is performed and that any potential channel plan changes are controlled by the RF circumstances of a single radio. In controller software release 6.0, the DCA algorithm has been redesigned to prevent both pinning and cascading. The following changes have been implemented:

- **Multiple local searches**—The DCA search algorithm performs multiple local searches initiated by different radios within the same DCA run rather than performing a single global search driven by a single radio. This change addresses both pinning and cascading while maintaining the desired flexibility and adaptability of DCA and without jeopardizing stability.

- **Multiple channel plan change initiators (CPCIs)**—Previously, the single worst radio was the sole initiator of a channel plan change. Now each radio within the RF group is evaluated and prioritized as a potential initiator. Intelligent randomization of the resulting list ensures that every radio is eventually evaluated, which eliminates the potential for pinning.

- **Limiting the propagation of channel plan changes (Localization)**—For each CPCI radio, the DCA algorithm performs a local search for a better channel plan, but only the CPCI radio itself and its one-hop neighboring access points are actually allowed to change their current transmit channels.
The impact of an access point triggering a channel plan change is felt only to within two RF hops from that access point, and the actual channel plan changes are confined to within a one-hop RF neighborhood. Because this limitation applies across all CPCI radios, cascading cannot occur.

- Non-RSSI-based cumulative cost metric—A cumulative cost metric measures how well an entire region, neighborhood, or network performs with respect to a given channel plan. The individual cost metrics of all access points in that area are considered in order to provide an overall understanding of the channel plan’s quality. These metrics ensure that the improvement or deterioration of each single radio is factored into any channel plan change. The objective is to prevent channel plan changes in which a single radio improves but at the expense of multiple other radios experiencing a considerable performance decline.

The RRM algorithms run at a specified updated interval, which is 600 seconds by default. Between update intervals, the RF group leader sends keepalive messages to each of the RF group members and collects real-time RF data.

### Note

Several monitoring intervals are also available. See the “Configuring RRM” section on page 13-5 for details.

### RF Group Name

A controller is configured with an RF group name, which is sent to all access points joined to the controller and used by the access points as the shared secret for generating the hashed MIC in the neighbor messages. To create an RF group, you configure all of the controllers to be included in the group with the same RF group name.

If there is any possibility that an access point joined to a controller may hear RF transmissions from an access point on a different controller, you should configure the controllers with the same RF group name. If RF transmissions between access points can be heard, then system-wide RRM is recommended to avoid 802.11 interference and contention as much as possible.

### Guidelines and Limitations

- Controller software release 4.2.99.0 or later releases support up to 20 controllers and 1000 access points in an RF group. For example, a Cisco WiSM controller supports up to 150 access points, so you can have up to 6 WiSM controllers in an RF group (150 access points x 6 controllers = 900 access points, which is less than 1000). Similarly, a 4404 controller supports up to 100 access points, so you can have up to ten (10) 4404 controllers in an RF group (100 x 10 = 1000).

- In controller software release 4.2.61.0 or earlier releases, RRM supports no more than five Cisco 4400 Series Controllers in an RF group.

- Starting in the 7.0.116.0 release, the RF group members are added based on the following criteria:
  - Maximum number of APs Supported: The maximum limit for the number of access points in an RF group is 1000. The number of access points supported is determined by the number of APs licensed to operate on the controller.
  - Twenty controllers: Only 20 controllers (including the leader) can be part of an RF group if the sum of the access points of all controllers combined is less than or equal to the upper access point limit.
Configuring RF Groups

This section describes how to configure RF groups through either the GUI or the CLI.

**Note**
The RF group name is generally set at deployment time through the Startup Wizard. However, you can change it as necessary.

**Note**
When the multiple-country feature is being used, all controllers intended to join the same RF group must be configured with the same set of countries, configured in the same order.

**Note**
You can also configure RF groups using the Cisco Wireless Control System (WCS). See the *Cisco Wireless Control System Configuration Guide* for instructions.

Configuring an RF Group Name (GUI)

**Step 1**
Choose **Controller > General** to open the General page.

**Figure 13-4** General Page

- **Step 2**
Enter a name for the RF group in the RF-Network Name text box. The name can contain up to 19 ASCII characters.

- **Step 3**
Click **Apply** to commit your changes.

- **Step 4**
Click **Save Configuration** to save your changes.
Step 5  Repeat this procedure for each controller that you want to include in the RF group.

Configuring an RF Group Name (CLI)

Step 1  Create an RF group by entering the `config network rf-network-name name` command:

**Note** Enter up to 19 ASCII characters for the group name.

Step 2  See the RF group by entering the `show network` command.

Step 3  Save your settings by entering the `save config` command.

Step 4  Repeat this procedure for each controller that you want to include in the RF group.

Viewing the RF Group Status

This section describes how to view the status of the RF group through either the GUI or the CLI.

**Note** You can also view the status of RF groups using the Cisco Wireless Control System (WCS). See Cisco Wireless Control System Configuration Guide for instructions.

Viewing RF Group Status (GUI)

Step 1  Choose Wireless > 802.11a/n or 802.11b/g/n > RRM > RF Grouping to open the 802.11a (or 802.11b/g) RRM > RF Grouping page.
Figure 13-5  802.11a > RRM > RF Grouping Page

This page shows the details of the RF group, displaying the configurable parameter **RF Group mode**, the **RF Group role** of this controller, the **Update Interval** and the controller name and IP address of the **Group Leader** to this controller.

**Note**  RF grouping mode can be set using the **Group Mode** drop-down. See the “Configuring the RF Group Mode (GUI)” section on page 13-6 for more information on this parameter.

**Tip**  Once a controller has joined as a static member and you want to change the grouping mode, we recommend that you remove the member from the configured static-leader and also make sure that a member controller has not been configured to be a member on multiple static leaders. This is to avoid repeated join attempts from one or more RF static leaders.

**Step 2**  (Optional) Repeat this procedure for the network type that you did not select (802.11a or 802.11b/g).

**Viewing RF Group Status (CLI)**

**Step 1**  See which controller is the RF group leader for the 802.11a/n RF network by entering this command:

```
show advanced 802.11a group
```

Information similar to the following appears:

```
Radio RF Grouping
802.11a Group Mode.............................. STATIC
```
802.11a Group Update Interval................. 600 seconds
802.11a Group Leader.......................... test (209.165.200.225)
  802.11a Group Member........................ test (209.165.200.225)
  802.11a Last Run.............................. 397 seconds ago

This output shows the details of the RF group, specifically the grouping mode for the controller, how often the group information is updated (600 seconds by default), the IP address of the RF group leader, the IP address of this controller, and the last time the group information was updated.

**Note**
If the IP addresses of the group leader and the group member are identical, this controller is currently the group leader.

**Note**
A * indicates that the controller has not joined as a static member.

**Step 2**
See which controller is the RF group leader for the 802.11b/g/n RF network by entering this command:

```
show advanced 802.11b group
```

## Overriding RRM

This section contains the following topics:

- **Information About Overriding RRM**, page 13-32
- **Guidelines and Limitations**, page 13-33
- **Statically Assigning Channel and Transmit Power Settings to Access Point Radios**, page 13-33

### Information About Overriding RRM

In some deployments, it is desirable to statically assign channel and transmit power settings to the access points instead of relying on the RRM algorithms provided by Cisco. Typically, this is true in challenging RF environments and non standard deployments but not the more typical carpeted offices.

**Note**
If you choose to statically assign channels and power levels to your access points and/or to disable dynamic channel and power assignment, you should still use automatic RF grouping to avoid spurious rogue device events.

You can disable dynamic channel and power assignment globally for a controller, or you can leave dynamic channel and power assignment enabled and statically configure specific access point radios with a channel and power setting. While you can specify a global default transmit power parameter for each network type that applies to all the access point radios on a controller, you must set the channel for each access point radio when you disable dynamic channel assignment. You may also want to set the transmit power for each access point instead of leaving the global transmit power in effect.
Guidelines and Limitations

We recommend that you assign different nonoverlapping channels to access points that are within close proximity to each other. The nonoverlapping channels in the U.S. are 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, and 161 in an 802.11a network and 1, 6, and 11 in an 802.11b/g/n network.

Do not assign all access points that are within close proximity to each other to the maximum power level.

Statically Assigning Channel and Transmit Power Settings to Access Point Radios

This section contains the following topics:

- Statically Assigning Channel and Transmit Power Settings (GUI), page 13-33
- Statically Assigning Channel and Transmit Power Settings (CLI), page 13-37

Statically Assigning Channel and Transmit Power Settings (GUI)

**Step 1** Choose Wireless > Access Points > Radios > 802.11a/n or 802.11b/g/n to open the 802.11a/n (or 802.11b/g/n) Radios page.

*Figure 13-6 802.11a/n Radios Page*

This page shows all the 802.11a/n or 802.11b/g/n access point radios that are joined to the controller and their current settings. The Channel text box shows both the primary and extension channels and uses an asterisk to indicate if they are globally assigned.

**Step 2** Hover your cursor over the blue drop-down arrow for the access point for which you want to modify the radio configuration and choose Configure. The 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page appears.
Overriding RRM

Chapter 13  Configuring Radio Resource Management

Figure 13-7  802.11a/n Cisco APs > Configure Page

Step 3  Choose one of the following options from the Channel Width drop-down list:

- **20 MHz**—Allows the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels. This is the default value.

- **40 MHz**—Allows 40-MHz 802.11n radios to communicate using two adjacent 20-MHz channels bonded together. The radio uses the primary channel that you choose in Step 6 as well as its extension channel for faster throughput. Each channel has only one extension channel (36 and 40 are a pair, 44 and 48 are a pair, and so on). For example, if you choose a primary channel of 44, the controller would use channel 48 as the extension channel. If you choose a primary channel of 48, the controller would use channel 44 as the extension channel.

**Note**  You cannot configure access points supporting 40 MHz channel width on 2.4 GHz.

**Note**  The Channel Width parameter can be configured for 802.11a/n radios only if you use the Custom RF channel assignment method.

**Note**  Statically configuring an access point’s radio for 20- or 40-MHz mode overrides the globally configured DCA channel width setting on the 802.11a > RRM > Dynamic Channel Assignment (DCA) page. If you change the static RF channel assignment method back to Global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.
Figure 13-8 shows channel bonding in the 5-GHz band. Low channels are preferred.

**Note** Channels 116, 120, 124, and 128 are not available in the U.S. and Canada for 40-MHz channel bonding.

**Figure 13-8  Channel Bonding in the 5-GHz Band**

**Step 4** Specify the RF Channel Assignment from the following options:
- **Global**—Choose this to specify a global value.
- **Custom**—Choose this and then select a value from the adjacent drop-down list to specify a custom value.

**Note** The Current Channel text box shows the current primary channel. If you chose 40 MHz for the channel width in **Step 3**, the extension channel appears in parentheses after the primary channel.

**Note** Changing the operating channel causes the access point radio to reset.

**Step 5** Configure the antenna parameters for this radio as follows:
- a. From the Antenna Type drop-down list, choose **Internal** or **External** to specify the type of antennas used with the access point radio.
b. Select and unselect the check boxes in the Antenna text box to enable and disable the use of specific antennas for this access point, where A, B, and C are specific antenna ports. A is the right antenna port, B is the left antenna port, and C is the center antenna port. For example, to enable transmissions from antenna ports A and B and receptions from antenna port C, you would select the following check boxes: Tx: A and B and Rx: C.

c. In the Antenna Gain text box, enter a number to specify an external antenna’s ability to direct or focus radio energy over a region of space. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain is measured in 0.5 dBi units, and the default value is 7 times 0.5 dBi, or 3.5 dBi.

If you have a high-gain antenna, enter a value that is twice the actual dBi value (see Cisco Aironet Antenna Reference Guide for antenna dBi values). Otherwise, enter 0. For example, if your antenna has a 4.4-dBi gain, multiply the 4.4 dB by 2 to get 8.8 and then round down to enter only the whole number (8). The controller reduces the actual equivalent isotropic radiated power (EIRP) to make sure that the antenna does not violate your country’s regulations.

d. Choose one of the following options from the Diversity drop-down list:
   - **Enabled**—Enables the antenna connectors on both sides of the access point. This is the default value.
   - **Side A or Right**—Enables the antenna connector on the right side of the access point.
   - **Side B or Left**—Enables the antenna connector on the left side of the access point.

**Step 6** Specify the Transmit Power Level from the following options:

- **Global**—Choose this to specify a global value.
- **Custom**—Choose this and then select a value from the adjacent drop-down list to specify a custom value.

The transmit power level is assigned an integer value instead of a value in mW or dBm. The integer corresponds to a power level that varies depending on the regulatory domain in which the access points are deployed. The number of available power levels varies based on the access point model. However, power level 1 is always the maximum power level allowed per country code setting, with each successive power level representing 50% of the previous power level. For example, 1 = maximum power level in a particular regulatory domain, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and so on.

**Note** See the hardware installation guide for your access point for the maximum transmit power levels supported per regulatory domain. Also, see the data sheet for your access point for the number of power levels supported.

**Note** If the access point is not operating at full power, the “Due to low PoE, radio is transmitting at degraded power” message appears under the Tx Power Level Assignment section. See the “Configuring Power over Ethernet” section on page 9-110 for more information on PoE power levels.

**Step 7** Choose **Enable** from the Admin Status drop-down list to enable this configuration for the access point.

**Step 8** Click **Apply** to commit your changes.

**Step 9** Configure the controller send the access point radio admin state immediately to WCS as follows:

a. Choose **Wireless > 802.11a/n** or **802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.
Step 10 Click **Save Configuration** to save your changes.

Step 11 Repeat this procedure for each access point radio for which you want to assign a static channel and power level.

### Statically Assigning Channel and Transmit Power Settings (CLI)

**Step 1** Disable the radio of a particular access point on the 802.11a or 802.11b/g/n network by entering this command:

```
config {802.11a | 802.11b} disable Cisco_AP
```

**Step 2** Configure the channel width for a particular access point by entering this command:

```
config {802.11a | 802.11b} chan_width Cisco_AP {20 | 40}
```

where

- **20** allows the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels. This is the default value.
- **40** allows 40-MHz 802.11n radios to communicate using two adjacent 20-MHz channels bonded together. The radio uses the primary channel that you choose in Step 5 as well as its extension channel for faster throughput. Each channel has only one extension channel (36 and 40 are a pair, 44 and 48 are a pair, and so on). For example, if you choose a primary channel of 44, the controller would use channel 48 as the extension channel. If you choose a primary channel of 48, the controller would use channel 44 as the extension channel.

**Note** This parameter can be configured only if the primary channel is statically assigned.

**Note** Statically configuring an access point’s radio for 20- or 40-MHz mode overrides the globally configured DCA channel width setting (configured using the `config advanced 802.11a channel dca chan-width-11n {20 | 40}` command). If you ever change the static configuration back to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

Figure 13-8 on page 13-35 shows channel bonding in the 5-GHz band. Low channels are preferred.

**Note** Channels 116, 120, 124, and 128 are not available in the U.S. and Canada for 40-MHz channel bonding.

**Step 3** Enable or disable the use of specific antennas for a particular access point by entering this command:

```
config {802.11a | 802.11b} 11nsupport antenna {tx | rx} Cisco_AP {A | B | C} {enable | disable}
```
where A, B, and C are antenna ports. A is the right antenna port, B is the left antenna port, and C is the center antenna port. For example, to enable transmissions from the antenna in access point AP1’s antenna port C on the 802.11a network, you would enter this command:

```
config 802.11a 11nsupport antenna tx AP1 C enable
```

**Step 4**
Specify the external antenna gain, which is a measure of an external antenna’s ability to direct or focus radio energy over a region of space entering this command:

```
config {802.11a | 802.11b} antenna extAntGain antenna_gain Cisco_AP
```

High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain is measured in 0.5 dBi units, and the default value is 7 times 0.5 dBi, or 3.5 dBi.

If you have a high-gain antenna, enter a value that is twice the actual dBi value (see Cisco Aironet Antenna Reference Guide for antenna dBi values). Otherwise, enter 0. For example, if your antenna has a 4.4-dBi gain, multiply the 4.4 dBi by 2 to get 8.8 and then round down to enter only the whole number (8). The controller reduces the actual equivalent isotropic radiated power (EIRP) to make sure that the antenna does not violate your country’s regulations.

**Step 5**
Specify the channel that a particular access point is to use by entering this command:

```
config {802.11a | 802.11b} channel ap Cisco_AP channel
```

For example, to configure 802.11a channel 36 as the default channel on AP1, enter the `config 802.11a channel ap AP1 36` command.

The channel you choose is the primary channel (for example, channel 36), which is used for communication by legacy 802.11a radios and 802.11n 20-MHz radios. 802.11n 40-MHz radios use this channel as the primary channel but also use an additional bonded extension channel for faster throughput, if you chose 40 for the channel width in Step 2.

**Note** Changing the operating channel causes the access point radio to reset.

**Step 6**
Specify the transmit power level that a particular access point is to use by entering this command:

```
config {802.11a | 802.11b} txPower ap Cisco_AP power_level
```

For example, to set the transmit power for 802.11a AP1 to power level 2, enter the `config 802.11a txPower ap AP1 2` command.

The transmit power level is assigned an integer value instead of a value in mW or dBm. The integer corresponds to a power level that varies depending on the regulatory domain in which the access points are deployed. The number of available power levels varies based on the access point model. However, power level 1 is always the maximum power level allowed per country code setting, with each successive power level representing 50% of the previous power level. For example, 1 = maximum power level in a particular regulatory domain, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and so on.

**Note** See the hardware installation guide for your access point for the maximum transmit power levels supported per regulatory domain. Also, see data sheet for your access point for the number of power levels supported.

**Step 7**
Save your settings by entering this command:

```
save config
```

**Step 8**
Repeat Step 2 through Step 7 for each access point radio for which you want to assign a static channel and power level.

**Step 9**
Reenable the access point radio by entering this command:
**Overriding RRM**

**Step 10** Configure the controller send the access point radio admin state immediately to WCS by entering this command:

```
config {802.11a | 802.11b} enable Cisco_AP
```

**Step 11** Save your changes by entering this command:

```
save config
```

**Step 12** See the configuration of a particular access point by entering this command:

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

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Cisco AP Identifier</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco AP Name</td>
<td>AP1</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>Tx Power</td>
<td></td>
</tr>
<tr>
<td>Num Of Supported Power Levels</td>
<td>8</td>
</tr>
<tr>
<td>Tx Power Level 1</td>
<td>20 dBm</td>
</tr>
<tr>
<td>Tx Power Level 2</td>
<td>17 dBm</td>
</tr>
<tr>
<td>Tx Power Level 3</td>
<td>14 dBm</td>
</tr>
<tr>
<td>Tx Power Level 4</td>
<td>11 dBm</td>
</tr>
<tr>
<td>Tx Power Level 5</td>
<td>8 dBm</td>
</tr>
<tr>
<td>Tx Power Level 6</td>
<td>5 dBm</td>
</tr>
<tr>
<td>Tx Power Level 7</td>
<td>2 dBm</td>
</tr>
<tr>
<td>Tx Power Level 8</td>
<td>-1 dBm</td>
</tr>
<tr>
<td>Tx Power Configuration</td>
<td>CUSTOMIZED</td>
</tr>
<tr>
<td>Current Tx Power Level</td>
<td>1</td>
</tr>
<tr>
<td>Phy OFDM parameters</td>
<td></td>
</tr>
<tr>
<td>Configuration</td>
<td>CUSTOMIZED</td>
</tr>
<tr>
<td>Current Channel</td>
<td>36</td>
</tr>
<tr>
<td>Extension Channel</td>
<td>40</td>
</tr>
<tr>
<td>Channel Width</td>
<td>40 Mhz</td>
</tr>
<tr>
<td>Allowed Channel List</td>
<td>36,44,52,60,100,108,116,123,149,157</td>
</tr>
<tr>
<td>TI Threshold</td>
<td>-50</td>
</tr>
<tr>
<td>Antenna Type</td>
<td>EXTERNAL_ANTENNA</td>
</tr>
<tr>
<td>External Antenna Gain (in .5 dBi units)</td>
<td>7</td>
</tr>
<tr>
<td>Diversity</td>
<td>DIVERSITY_ENABLED</td>
</tr>
<tr>
<td>802.11Antennas</td>
<td></td>
</tr>
<tr>
<td>Tx</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>ENABLED</td>
</tr>
<tr>
<td>B</td>
<td>ENABLED</td>
</tr>
<tr>
<td>Rx</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>DISABLED</td>
</tr>
<tr>
<td>B</td>
<td>DISABLED</td>
</tr>
<tr>
<td>C</td>
<td>ENABLED</td>
</tr>
</tbody>
</table>

---

**Disabling Dynamic Channel and Power Assignment Globally for a Controller**

This section contains the following topics:

- Disabling Dynamic Channel and Power Assignment (GUI), page 13-40
- Disabling Dynamic Channel and Power Assignment (CLI), page 13-40
Disabling Dynamic Channel and Power Assignment (GUI)

Step 1  Choose Wireless > 802.11a/n or 802.11b/g/n > RRM > Auto RF to open the 802.11a (or 802.11b/g) Global Parameters > Auto RF page.

Step 2  Disable dynamic channel assignment by choosing OFF under RF Channel Assignment.

Step 3  Disable dynamic power assignment by choosing Fixed under Tx Power Level Assignment and choosing a default transmit power level from the drop-down list.

Note  See Step 6 on page 13-36 for information on transmit power levels.

Step 4  Click Apply to commit your changes.

Step 5  Click Save Configuration to save your changes.

Step 6  If you are overriding the default channel and power settings on a per radio basis, assign static channel and power settings to each of the access point radios that are joined to the controller.

Step 7  (Optional) Repeat this procedure for the network type that you did not select (802.11a or 802.11b/g).

Disabling Dynamic Channel and Power Assignment (CLI)

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

```plaintext
config {802.11a | 802.11b} disable network
```

Step 2  Disable RRM for all 802.11a/n or 802.11b/g/n radios and set all channels to the default value by entering this command:

```plaintext
config {802.11a | 802.11b} channel global off
```

Step 3  Enable the 802.11a/n or 802.11b/g/n network by entering this command:

```plaintext
config {802.11a | 802.11b} enable network
```

Note  To enable the 802.11g network, enter the config 802.11b 11gSupport enable command after the config 802.11b enable network command.

Step 4  Save your changes by entering this command:

```plaintext
save config
```

Configuring Rogue Access Point Detection in RF Groups

This section contains the following topics:

- Information About Rogue Access Point Detection in RF Groups, page 13-41
- Configuring Rogue Access Point Detection in RF Groups, page 13-41
Information About Rogue Access Point Detection in RF Groups

After you have created an RF group of controllers, you need to configure the access points connected to the controllers to detect rogue access points. The access points will then select the beacon/probe-response frames in neighboring access point messages to see if they contain an authentication information element (IE) that matches that of the RF group. If the select is successful, the frames are authenticated. Otherwise, the authorized access point reports the neighboring access point as a rogue, records its BSSID in a rogue table, and sends the table to the controller.

Configuring Rogue Access Point Detection in RF Groups

This section contains the following topics:

- Enabling Rogue Access Point Detection in RF Groups (GUI), page 13-41
- Configuring Rogue Access Point Detection in RF Groups (CLI), page 13-43

Enabling Rogue Access Point Detection in RF Groups (GUI)

**Step 1** Make sure that each controller in the RF group has been configured with the same RF group name.

**Note** The name is used to verify the authentication IE in all beacon frames. If the controllers have different names, false alarms will occur.

**Step 2** Choose Wireless to open the All APs page.

**Figure 13-9 All APs Page**

**Step 3** Click the name of an access point to open the All APs > Details page.
Choose either local or monitor from the AP Mode drop-down list and click **Apply** to commit your changes.

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

Repeat Step 2 through Step 5 for every access point connected to the controller.

Choose **Security > Wireless Protection Policies > AP Authentication/MFP** to open the AP Authentication Policy page.

The name of the RF group to which this controller belongs appears at the top of the page.

Choose **AP Authentication** from the Protection Type drop-down list to enable rogue access point detection.

Enter a number in the Alarm Trigger Threshold edit box to specify when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.
Chapter 13 Configuring Radio Resource Management

Configuring Rogue Access Point Detection in RF Groups

Configuring Rogue Access Point Detection in RF Groups (CLI)

Step 1 Make sure that each controller in the RF group has been configured with the same RF group name.

Note The name is used to verify the authentication IE in all beacon frames. If the controllers have different names, false alarms will occur.

Step 2 Configure a particular access point for local (normal) mode or monitor (listen-only) mode by entering this command:

   config ap mode local Cisco_AP or config ap mode monitor Cisco_AP

Step 3 Save your changes by entering this command:

   save config

Step 4 Repeat Step 2 and Step 3 for every access point connected to the controller.

Step 5 Enable rogue access point detection by entering this command:

   config wps ap-authentication

Step 6 Specify when a rogue access point alarm is generated by entering this command. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.

   config wps ap-authentication threshold

Note The valid threshold range is from 1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.

Step 7 Save your changes by entering this command:

   save config

Step 8 Repeat Step 5 through Step 7 on every controller in the RF group.
Configuring CCX Radio Management Features

This section contains the following topics:

- Information About CCX Radio Management Features, page 13-44
- Guidelines and Limitations, page 13-45
- Configuring CCX Radio Management, page 13-45

Information About CCX Radio Management Features

You can configure two parameters that affect client location calculations:

- Radio measurement requests
- Location calibration

These parameters are supported in Cisco Client Extensions (CCX) v2 and later releases are designed to enhance location accuracy and timeliness for participating CCX clients. See the “Configuring Cisco Client Extensions” section on page 8-57 for more information on CCX.

For the location features to operate properly, the access points must be configured for normal, monitor, or FlexConnect mode. However, for FlexConnect mode, the access point must be connected to the controller.

Radio Measurement Requests

When you enable the radio measurements requests feature, lightweight access points issue broadcast radio measurement request messages to clients running CCXv2 or later releases. The access points transmit these messages for every SSID over each enabled radio interface at a configured interval. In the process of performing 802.11 radio measurements, CCX clients send 802.11 broadcast probe requests on all the channels specified in the measurement request. The Cisco Location Appliance uses the uplink measurements based on these requests received at the access points to quickly and accurately calculate the client location. You do not need to specify on which channels the clients are to measure. The controller, access point, and client automatically determine which channels to use.

In controller software release 4.1 or later releases, the radio measurement feature has been expanded to enable the controller to also obtain information on the radio environment from the client’s perspective (rather than from just that of the access point). In this case, the access points issue unicast radio measurement requests to a particular CCXv4 or v5 client. The client then sends various measurement reports back to the access point and onto the controller. These reports include information about the radio environment and data used to interpret the location of the clients. To prevent the access points and controller from being overwhelmed by radio measurement requests and reports, only two clients per access point and up to 20 clients per controller are supported. You can view the status of radio measurement requests for a particular access point or client as well as radio measurement reports for a particular client from the controller CLI.

Note

If rogue access point detection is not enabled on every controller in the RF group, the access points on the controllers with this feature disabled are reported as rogues.
Controller software release 4.1 or later releases improve the ability of the Location Appliance to accurately interpret the location of a device through a CCXv4 feature called location-based services. The controller issues a path-loss request to a particular CCXv4 or v5 client. If the client chooses to respond, it sends a path-loss measurement report to the controller. These reports contain the channel and transmit power of the client.

Note
Non-CCX and CCXv1 clients ignore the CCX measurement requests and do not participate in the radio measurement activity.

Location Calibration
For CCX clients that need to be tracked more closely (for example, when a client calibration is performed), the controller can be configured to command the access point to send unicast measurement requests to these clients at a configured interval and whenever a CCX client roams to a new access point. These unicast requests can be sent out more often to these specific CCX clients than the broadcast measurement requests, which are sent to all clients. When location calibration is configured for non-CCX and CCXv1 clients, the clients are forced to disassociate at a specified interval to generate location measurements.

Guidelines and Limitations
CCX is not supported on the AP1030.

Configuring CCX Radio Management
This section contains the following topics:
- Configuring CCX Radio Management (GUI), page 13-45
- Configuring CCX Radio Management (CLI), page 13-46
- Viewing CCX Radio Management Information (CLI), page 13-47
- Debugging CCX Radio Management Issues (CLI), page 13-48

Configuring CCX Radio Management (GUI)

Step 1
Choose Wireless > 802.11a/n or 802.11b/g/n > Network to open the 802.11a (or 802.11b/g) Global Parameters page.
Step 2  Under CCX Location Measurement, select the **Mode** check box to globally enable CCX radio management. This parameter causes the access points connected to this controller to issue broadcast radio measurement requests to clients running CCX v2 or later releases. The default value is disabled (or unselected).

Step 3  If you selected the Mode check box in the previous step, enter a value in the **Interval** text box to specify how often the access points are to issue the broadcast radio measurement requests.

The range is 60 to 32400 seconds.

The default is 60 seconds.

Step 4  Click **Apply** to commit your changes.

Step 5  Click **Save Configuration** to save your settings.

Step 6  Follow the instructions in **Step 2** of the “Configuring CCX Radio Management (CLI)” section below to enable access point customization.

---

**Note**  To enable CCX radio management for a particular access point, you must enable access point customization, which can be done only through the controller CLI.

Step 7  If desired, repeat this procedure for the other radio band (802.11a/n or 802.11b/g/n).

---

**Configuring CCX Radio Management (CLI)**

Step 1  Globally enable CCX radio management by entering this command:

```
config advanced {802.11a | 802.11b} ccx location-meas global enable interval_seconds
```
The range for the `interval_seconds` parameter is 60 to 32400 seconds, and the default value is 60 seconds. This command causes all access points connected to this controller in the 802.11a/n or 802.11b/g/n network to issue broadcast radio measurement requests to clients running CCXv2 or later releases.

**Step 2** Enable access point customization by entering these commands:

```
config advanced {802.11a \ 802.11b} ccx customize Cisco_AP {on | off}
```

This command enables or disables CCX radio management features for a particular access point in the 802.11a/n or 802.11b/g/n network.

```
config advanced {802.11a \ 802.11b} ccx location-meas ap Cisco_AP enable interval_seconds
```

The range for the `interval_seconds` parameter is 60 to 32400 seconds, and the default value is 60 seconds. This command causes a particular access point in the 802.11a/n or 802.11b/g/n network to issue broadcast radio measurement requests to clients running CCXv2 or higher.

**Step 3** Enable or disable location calibration for a particular client by entering this command:

```
config client location-calibration {enable | disable} client_mac interval_seconds
```

**Note** You can configure up to five clients per controller for location calibration.

**Step 4** Save your settings by entering this command:

```
save config
```

### Viewing CCX Radio Management Information (CLI)

- To see the CCX broadcast location measurement request configuration for all access points connected to this controller in the 802.11a/n or 802.11b/g/n network, enter this command:

```
show advanced {802.11a \ 802.11b} ccx global
```

- To see the CCX broadcast location measurement request configuration for a particular access point in the 802.11a/n or 802.11b/g/n network, enter this command:

```
show advanced {802.11a \ 802.11b} ccx ap Cisco_AP
```

- To see the status of radio measurement requests for a particular access point, enter this command:

```
show ap ccx rm Cisco_AP status
```

Information similar to the following appears:

**A Radio**

- Beacon Request................................. Enabled
- Channel Load Request.......................... Enabled
- Frame Request.................................. Disabled
- Noise Histogram Request....................... Disabled
- Path Loss Request.............................. Disabled
- Interval....................................... 60
- Iteration...................................... 5

**B Radio**

- Beacon Request.................................... Disabled
- Channel Load Request.......................... Enabled
- Frame Request.................................. Disabled
- Noise Histogram Request....................... Enabled
Configuring CCX Radio Management Features

Chapter 13  Configuring Radio Resource Management

Path Loss Request.............................. Disabled
Interval....................................... 60
Iteration................................... 5

To see the status of radio measurement requests for a particular client, enter this command:

```plaintext
show client ccx rm client_mac status
```

Information similar to the following appears:

```plaintext
Client Mac Address............................... 00:40:96:ae:53:b4
Beacon Request................................... Enabled
Channel Load Request............................. Disabled
Frame Request................................... Disabled
Noise Histogram Request.......................... Disabled
Path Loss Request................................. Disabled
Interval......................................... 5
Iteration........................................ 3
```

To see radio measurement reports for a particular client, enter these commands:

- `show client ccx rm client_mac report beacon`—Shows the beacon report for the specified client.
- `show client ccx rm client_mac report chan-load`—Shows the channel-load report for the specified client.
- `show client ccx rm client_mac report noise-hist`—Shows the noise-histogram report for the specified client.
- `show client ccx rm client_mac report frame`—Shows the frame report for the specified client.

To see the clients configured for location calibration, enter this command:

```plaintext
show client location-calibration summary
```

To see the RSSI reported for both antennas on each access point that heard the client, enter this command:

```plaintext
show client detail client_mac
```

Debugging CCX Radio Management Issues (CLI)

To debug CCX broadcast measurement request activity, enter this command:

```plaintext
debug airewave-director message {enable | disable}
```

To debug client location calibration activity, enter this command:

```plaintext
debug ccxrm [all | error | warning | message | packet | detail {enable | disable}]
```

The CCX radio measurement report packets are encapsulated in Internet Access Point Protocol (IAPP) packets. Therefore, if the previous `debug ccxrm` command does not provide any debugs, enter this command to provide debugs at the IAPP level:

```plaintext
debug iapp error {enable | disable}
```

To debug the output for forwarded probes and their included RSSI for both antennas, enter this command:

```plaintext
debug dot11 load-balancing
```
This chapter contains the following sections:

- Information About CleanAir, page 14-1
- Guidelines and Limitations, page 14-4
- Configuring Cisco CleanAir, page 14-5
- Monitoring the Interference Devices, page 14-14
- Monitoring the Air Quality of Radio Bands, page 14-19
- Configuring a Spectrum Expert Connection, page 14-24
- Additional References, page 14-26
- Feature History for Configuring CleanAir, page 14-27

## Information About CleanAir

Cisco CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all of the users of the shared spectrum (both native devices and foreign interferers). It also enables you or your network to act upon this information. For example, you could manually remove the interfering device, or the system could automatically change the channel away from the interference.

A Cisco CleanAir system consists of CleanAir-enabled access points, controllers, and WCS. These access points collect information about all devices that operate in the industrial, scientific, and medical (ISM) bands, identify and evaluate the information as a potential interference source, and forward it to the controller. The controller controls the access points, collects spectrum data, and forwards information to WCS or a Cisco mobility services engine (MSE) upon request. The controller provides a local user interface to configure basic CleanAir features and display basic spectrum information. WCS provides an advanced user interface for configuring Cisco CleanAir features, displaying information, and keeping records. The MSE is optional for the basic feature set but required for advanced features such as tracking the location of non-Wi-Fi interference devices.

For every device operating in the unlicensed band, Cisco CleanAir tells you what it is, where it is, how it is impacting your wireless network, and what actions you or your network should take. It simplifies RF so that you do not have to be an RF expert.

Wireless LAN systems operate in unlicensed 2.4- and 5-GHz ISM bands. Many devices, such as microwave ovens, cordless phones, and Bluetooth devices also operate in these bands and can negatively affect Wi-Fi operations.
Some of the most advanced WLAN services, such as voice over wireless and IEEE 802.11n radio communications, could be significantly impaired by the interference caused by other legal users of the ISM bands. The integration of Cisco CleanAir functionality into the Cisco Unified Wireless Network addresses this problem of radio frequency (RF) interference.

Role of the Controller in a Cisco CleanAir System

The controller performs the following tasks in a Cisco CleanAir system:

- Configures Cisco CleanAir capabilities on the access point.
- Provides interfaces (GUI, CLI, and SNMP) for configuring Cisco CleanAir features and retrieving data.
- Displays spectrum data.
- Collects and processes air quality reports from the access point and stores them in the air quality database. Air Quality Report (AQR) contains information about the total interference from all identified sources represented by Air Quality Index (AQI) and summary for the most severe interference categories. The CleanAir system can also include unclassified interference information under per interference type reports which enable you to take action in cases where the interference due to unclassified interfering devices is frequent.
- Collects and processes interference device reports (IDRs) from the access point and stores them in the interference device database.
- Forwards spectrum data to WCS and the MSE.

Interference Types that Cisco CleanAir can Detect

Cisco CleanAir can detect interference, report on the location and severity of the interference, and recommend different mitigation strategies. Two such mitigation strategies are persistent device avoidance and spectrum event-driven RRM.

Wi-Fi chip-based RF management systems share these characteristics:

- Any RF energy that cannot be identified as a Wi-Fi signal is reported as noise.
- Noise measurements that are used to assign a channel plan tend to be averaged over a period of time to avoid instability or rapid changes that can be disruptive to certain client devices.
- Averaging measurements reduces the resolution of the measurement. As such, a signal that disrupts clients might not look like it needs to be mitigated after averaging.
- All RF management systems available today are reactive in nature.

Cisco CleanAir is different and can positively identify not only the source of the noise but also its location and potential impact to a WLAN. Having this information allows you to consider the noise within the context of the network and make intelligent and, where possible, proactive decisions. For CleanAir, two types of interference events are common:

- Persistent interference
- Spontaneous interference

Persistent interference events are created by devices that are stationary in nature and have intermittent but largely repeatable patterns of interference. For example, consider the case of a microwave oven located in a break room. Such a device might be active for only 1 or 2 minutes at a time. When operating, however, it can be disruptive to the performance of the wireless network and associated clients. Using
Cisco CleanAir, you can positively identify the device as a microwave oven rather than indiscriminate noise. You can also determine exactly which part of the band is affected by the device, and because you can locate it, you can understand which access points are most severely affected. You can then use this information to direct RRM in selecting a channel plan that avoids this source of interference for the access points within its range. Because this interference is not active for a large portion of the day, existing RF management applications might attempt to again change the channels of the affected access points. Persistent device avoidance is unique, however, in that it remains in effect as long as the source of interference is periodically detected to refresh the persistent status. The Cisco CleanAir system knows that the microwave oven exists and includes it in all future planning. If you move either the microwave oven or the surrounding access points, the algorithm updates RRM automatically.

**Note**

Spectrum event-driven RRM can be triggered only by Cisco CleanAir-enabled access points in local mode.

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a threshold for air quality (AQ) that, if exceeded, triggers an immediate channel change for the affected access point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active. Cisco CleanAir also identifies and locates the source of interference so that more permanent mitigation of the device can be performed at a later time.

In the case of Bluetooth devices, Cisco CleanAir-enabled access points can detect and report interference only if the devices are actively transmitting. Bluetooth devices have extensive power save modes. For example, interference can be detected when data or voice is being streamed between the connected devices.

**Persistent Devices**

Some interference devices such as outdoor bridges and Microwave Ovens only transmit when needed. These devices can cause significant interference to the local WLAN due to short duration and periodic operation remain largely undetected by normal RF management metrics. With CleanAir the RRM DCA algorithm can detect, measure, register and remember the impact and adjust the DCA algorithm. This minimizes the use of channels affected by the persistent devices in the channel plan local to the interference source. Cisco CleanAir detects and stores the persistent device information in the controller and this information is used to mitigate interfering channels.

**Persistent Devices Detection**

CleanAir-capable Monitor Mode access point collects information about persistent devices on all configured channels and store the information in controller. Local/Bridge mode AP detects interference devices on the serving channels only.
Guidelines and Limitations

Only Cisco CleanAir-enabled access points using the following access point modes can perform Cisco CleanAir spectrum monitoring:

- Local—In this mode, each Cisco CleanAir-enabled access point radio provides air quality and interference detection reports for the current operating channel only.

- FlexConnect—When a FlexConnect access point is connected to the controller, its Cisco CleanAir functionality is identical to local mode.

- Monitor—When Cisco CleanAir is enabled in monitor mode, the access point provides air quality and interference detection reports for all monitored channels.

The following options are available:

- All—All channels
- DCA—Channel selection governed by the DCA list
- Country—All channel legal within a regulatory domain

Note: Suppose you have two APs, one in the FlexConnect mode and the other in the monitor mode. Also suppose that you have created a profile enabling EAP attack against 802.1x auth. The Airmagnet (AM) tool, which can generate different types of attacks, fails to generate any attack even if you have provided valid AP MAC and STA MAC addresses. But if the AP MAC and STA MAC addresses in the AM tool are swapped, that is, the AP MAC address is specified in the STA MAC field and the STA MAC address is specified in the AP MAC field, then the tool is able to generate attacks, which the AP in the Monitor mode is also able to detect.

Note: The access point does not participate in AQ HeatMap in WCS.

- SE-Connect—This mode enables a user to connect a Spectrum Expert application running on an external Microsoft Windows XP or Vista PC to a Cisco CleanAir-enabled access point in order to display and analyze detailed spectrum data. The Spectrum Expert application connects directly to the access point, bypassing the controller. An access point in SE-Connect mode does not provide any Wi-Fi, RF, or spectrum data to the controller. In addition to performing spectrum intelligence, an access point can provide other. See the “Configuring a Spectrum Expert Connection” section on page 14-24 for instructions on establishing a Spectrum Expert console connection.

- Access points in monitor mode do not transmit Wi-Fi traffic or 802.11 packets. They are excluded from radio resource management (RRM) planning and are not included in the neighbor access point list. IDR clustering depends on the controller’s ability to detect neighboring in-network access points. Correlating interference device detections from multiple access points is limited between monitor-mode access points.

Persistent Devices Propagation

Persistent device information that is detected by local or monitor mode access points is propagated to the neighboring access points connected to the same controller. This provides better chance of handling and avoiding persistent devices. Persistent device detected by the CleanAir-enabled access point is propagated to neighboring non-CleanAir access points, which enhances channel selection quality.
• Spectrum Expert (SE) Connect functionality is supported for local, flexconnect, bridge, and monitor modes. The access point provides spectrum information to Spectrum Expert only for the current channel(s). For local, FlexConnect, and bridge modes, the spectrum data is available for the current active channel(s) and for the monitor mode, the common monitored channel list is available. The access point continues to send AQ (Air Quality) and IDR (Interference Device Reports) reports to the controller and perform normal activities according to the current mode. Sniffer and rogue detections access point modes are incompatible with all types of CleanAir spectrum monitoring.

• Controllers have limitations on the number of monitor mode AP’s that they can support. This is because, a monitor mode AP saves data for all the channels.

• Do not connect access points in SE connect mode directly to any physical port on the 2500 Series Controller.

• Spectrum Expert (Windows XP laptop client) and AP should be pingable, otherwise; it will not work.

Configuring Cisco CleanAir

This section contains the following topics:

• Configuring Cisco CleanAir on the Controller, page 14-5
• Configuring Cisco CleanAir on an Access Point, page 14-11

Configuring Cisco CleanAir on the Controller

This section contains the following topics:

• Configuring Cisco CleanAir on the Controller (GUI), page 14-5
• Configuring Cisco CleanAir on the Controller (CLI), page 14-8

Configuring Cisco CleanAir on the Controller (GUI)

Step 1

Choose Wireless > 802.11a/n or 802.11b/g/n > CleanAir to open the 802.11a (or 802.11b) > CleanAir page.
Step 2  Select the **CleanAir** check box to enable Cisco CleanAir functionality on the 802.11a/n or 802.11b/g/n network, or unselect it to prevent the controller from detecting spectrum interference. By default, the value is not selected.

Step 3  Select the **Report Interferers** check box to enable the Cisco CleanAir system to report any detected sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.

**Note**  Device Security alarms, Event Driven RRM, and Persistence Device Avoidance algorithm do not work if Report Interferers are disabled.

Step 4  Select the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables you to propagate information about persistent devices to the neighboring access points connected to the same controller. Persistent interferers are present at a location and interfere with the WLAN operations even if they are not detectable at all times.

Step 5  Ensure that any sources of interference that need to be detected and reported by the Cisco CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferences to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are detected. The possible sources of interference that you can choose are as follows:

- **Bluetooth Paging Inquiry**—A Bluetooth discovery (802.11b/g/n only)
- **Bluetooth Sco Acl**—A Bluetooth link (802.11b/g/n only)
- **Generic DECT**—A digital enhanced cordless communication (DECT)-compatible phone
- **Generic TDD**—A time division duplex (TDD) transmitter
- **Generic Waveform**—A continuous transmitter
- **Jammer**—A jamming device
- **Microwave**—A microwave oven (802.11b/g/n only)
- **Canopy**—A canopy bridge device
- **Spectrum 802.11 FH**—An 802.11 frequency-hopping device (802.11b/g/n only)
Chapter 14      Configuring Cisco CleanAir

- **Spectrum 802.11 inverted**—A device using spectrally inverted Wi-Fi signals
- **Spectrum 802.11 non std channel**—A device using nonstandard Wi-Fi channels
- **Spectrum 802.11 SuperG**—An 802.11 SuperAG device
- **Spectrum 802.15.4**—An 802.15.4 device (802.11b/g/n only)
- **Video Camera**—An analog video camera
- **WiMAX Fixed**—A WiMAX fixed device (802.11a/n only)
- **WiMAX Mobile**—A WiMAX mobile device (802.11a/n only)
- **XBox**—A Microsoft Xbox (802.11b/g/n only)

**Note**
Access points that are associated to the controller send interference reports only for the interferers that appear in the Interferences to Detect box. This functionality allows you to filter out interferers that you do not want as well as any that may be flooding the network and causing performance problems for the controller or WCS. Filtering allows the system to resume normal performance levels.

**Step 6**
Configure Cisco CleanAir alarms as follows:

a. Select the **Enable AQI (Air Quality Index) Trap** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature. The default value is selected.

b. If you selected the Enable AQI Trap check box in Step a, enter a value between 1 and 100 (inclusive) in the AQI Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

Enter the **AQI Alarm Threshold (1 to 100)** that you want to set. An alarm is generated when the air quality falls below the configured threshold value. The default is 35. The valid range is from 1 and 100.

- Select the **Enable trap for Unclassified Interferences** check box to enable the AQI alarm to be generated upon detection of unclassified interference beyond the severity threshold specified in the AQI Alarm Threshold. Unclassified interferences are interferences that are detected but do not correspond to any of the identifiable interference types.

- Enter the **Threshold for Unclassified category trap (1 to 99)**. The valid range is from 1 and 99. The default is 20. This is the severity index threshold for an unclassified interference category.

c. Select the **Enable Interference Type Trap** check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is selected.

d. Make sure that any sources of interference that need to trigger interferer alarms appear in the Trap on These Types box and any that do not need to trigger interferer alarms appear in the Do Not Trap on These Types box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.

For example, if you want the controller to send an alarm when it detects a jamming device, select the **Enable Interference Type Trap check box** and move the jamming device to the Trap on These Types box.

**Step 7**
Click **Apply** to commit your changes.
Step 8  Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference as follows:

a. Look at the EDRRM field to see the current status of spectrum event-driven RRM and, if enabled, the Sensitivity Threshold field to see the threshold level at which event-driven RRM is invoked.

b. If you want to change the current status of event-driven RRM or the sensitivity level, click Change Settings. The 802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA) page appears.

c. Select the EDRRM check box to trigger RRM to run when an access point detects a certain level of interference, or unselect it to disable this feature. The default value is selected.

d. If you selected the EDRRM check box in Step c, choose Low, Medium, High, or Custom from the Sensitivity Threshold drop-down list to specify the threshold at which you want RRM to be triggered. When the interference for the access point rises and the corresponding AQ index falls below the threshold level, RRM initiates a local channel assignment and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

If you selected the EDRRM sensitivity threshold as custom, you must set a threshold value in the Custom Sensitivity Threshold field. The default sensitivity is 35.

The EDRRM AQ threshold value for low sensitivity is 35, medium sensitivity is 50, and high sensitivity is 60.

The default value is Medium.

e. Click Apply to commit your changes.

Step 9  Click Save Configuration to save your changes.

---

### Configuring Cisco CleanAir on the Controller (CLI)

Step 1  Configure Cisco CleanAir functionality on the 802.11a/n or 802.11b/g/n network by entering this command:

```
config {802.11a | 802.11b} cleanair {enable | disable} all
```

If you disable this feature, the controller does not receive any spectrum data. The default value is enable.

Step 2  Configure interference detection and specify sources of interference that need to be detected by the Cisco CleanAir system by entering this command:

```
config {802.11a | 802.11b} cleanair device {enable | disable} type
```

where you choose the type is one of the following:

- **802.11-fh**—An 802.11 frequency-hopping device (802.11b/g/n only)
- **802.11-inv**—A device using spectrally inverted Wi-Fi signals
- **802.11-nonstd**—A device using nonstandard Wi-Fi channels
- **802.15.4**—An 802.15.4 device (802.11b/g/n only)
- **all**—All interference device types (this is the default value)
- **bt-discovery**—A bluetooth discovery (802.11b/g/n only)
- **bt-link**—A bluetooth link (802.11b/g/n only)
- **canopy**—A canopy device
Chapter 14 Configuring Cisco CleanAir

Configuring Cisco CleanAir

• cont-tx—A continuous transmitter
• dect-like—A digital enhanced cordless communication (DECT)-compatible phone
• jammer—A jamming device
• mw-oven—A microwave oven (802.11b/g/n only)
• superag—An 802.11 SuperAG device
• tdd-tx—A time division duplex (TDD) transmitter
• video camera—An analog video camera
• wimax-fixed—A WiMAX fixed device
• wimax-mobile—A WiMAX mobile device
• xbox—A Microsoft Xbox (802.11b/g/n only)

Note Access points that are associated to the controller send interference reports only for the interference types specified in this command. This functionality allows you to filter out interferers that may be flooding the network and causing performance problems for the controller or WCS. Filtering allows the system to resume normal performance levels.

Step 3 Configure the triggering of air quality alarms by entering this command:
```plaintext
config {802.11a | 802.11b} cleanair alarm air-quality {enable | disable}
```
The default value is enabled.

Step 4 Specify the threshold at which you want the air quality alarm to be triggered by entering this command:
```plaintext
config {802.11a | 802.11b} cleanair alarm air-quality threshold threshold
```
where `threshold` is a value between 1 and 100 (inclusive). When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

Step 5 Enable the triggering of interferer alarms by entering this command:
```plaintext
config {802.11a | 802.11b} cleanair alarm device {enable | disable}
```
The default value is enable.

Step 6 Specify sources of interference that trigger alarms by entering this command:
```plaintext
config {802.11a | 802.11b} cleanair alarm device type {enable | disable}
```
where you choose `type` as one of the following:

• 802.11-fh—An 802.11 frequency-hopping device (802.11b/g/n only)
• 802.11-inv—A device using spectrally inverted Wi-Fi signals
• 802.11-nonsdt—A device using nonstandard Wi-Fi channels
• 802.15.4—An 802.15.4 device (802.11b/g/n only)
• all—All interference device types (this is the default value)
• bt-discovery—A Bluetooth discovery (802.11b/g/n only)
• bt-link—A Bluetooth link (802.11b/g/n only)
• canopy—A canopy device
• cont-tx—A continuous transmitter
Step 7 Configure the triggering of air quality alarms for unclassified devices by entering this command:

```
config {802.11a | 802.11b} cleanair alarm unclassified {enable | disable}
```

Step 8 Specify the threshold at which you want the air quality alarm to be triggered for unclassified devices by entering this command:

```
config {802.11a | 802.11b} cleanair alarm unclassified threshold threshold
```

where `threshold` is a value from 1 and 99 (inclusive). When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

Step 9 Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference by entering these commands:

```
config advanced {802.11a | 802.11b} channel cleanair-event {enable | disable} — Enables or disables spectrum event-driven RRM. The default value is disabled.
config advanced {802.11a | 802.11b} channel cleanair-event sensitivity {low | medium | high | custom} — Specifies the threshold at which you want RRM to be triggered. When the interference level for the access point rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while high represents an increased sensitivity. You can also set the sensitivity to a custom level of your choice. The default value is medium.
config advanced {802.11a | 802.11b} channel cleanair-event sensitivity threshold thresholdvalue — If you set the threshold sensitivity as custom, you must set a custom threshold value. The default is 35.
```

Step 10 Enable persistent devices propagation by entering this command:

```
config advanced {802.11a | 802.11b} channel pda-prop {enable | disable}
```

Step 11 Save your changes by entering this command:

```
save config
```

Step 12 See the Cisco CleanAir configuration for the 802.11a/n or 802.11b/g/n network by entering this command:

```
show {802.11a | 802.11b} cleanair config
```

Information similar to the following appears:

```
(Cisco Controller) > show 802.11a cleanair config

Clean Air Solution......................... Disabled
Air Quality Settings:
```

- **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
- **jammer**—A jamming device
- **mw-oven**—A microwave oven (802.11b/g/n only)
- **superag**—An 802.11 SuperAG device
- **tdd-tx**—A time division duplex (TDD) transmitter
- **video camera**—An analog video camera
- **wimax-fixed**—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device
- **xbox**—A Microsoft Xbox (802.11b/g/n only)
Air Quality Reporting........................ Enabled
Air Quality Reporting Period (min)........ 15
Air Quality Alarms.......................... Enabled
Air Quality Alarm Threshold............. 35
Unclassified Interference.................. Disabled
Unclassified Severity Threshold............ 20

Interference Device Settings:
Interference Device Reporting............. Enabled
Interference Device Types:
  TDD Transmitter.......................... Enabled
  Jammer.................................. Enabled
  Continuous Transmitter.................. Enabled
  DECT-like Phone........................ Enabled
  Video Camera............................ Enabled
  WiFi Inverted........................... Enabled
  WiFi Invalid Channel................... Enabled
  SuperAG.................................. Enabled
  Canopy.................................. Enabled
  WiMax Mobile........................... Enabled
  WiMax Fixed................................ Enabled

Interference Device Alarms.................. Enabled
Interference Device Types Triggering Alarms:
  TDD Transmitter.......................... Disabled
  Jammer.................................. Enabled
  Continuous Transmitter.................. Disabled
  DECT-like Phone........................ Disabled
  Video Camera............................ Disabled
  WiFi Inverted........................... Enabled
  WiFi Invalid Channel................... Enabled
  SuperAG.................................. Disabled
  Canopy.................................. Disabled
  WiMax Mobile........................... Disabled
  WiMax Fixed................................ Disabled

Additional Clean Air Settings:
CleanAir ED-RRM State......................... Disabled
CleanAir ED-RRM Sensitivity.................. Medium
CleanAir ED-RRM Custom Threshold............ 50
CleanAir Persistent Devices state........ Disabled
CleanAir Persistent Device Propagation..... Enabled

---

**Step 13** See the spectrum event-driven RRM configuration for the 802.11a/n or 802.11b/g/n network by entering this command:

```bash
show advanced {802.11a | 802.11b} channel
```

Information similar to the following appears:

Automatic Channel Assignment
  Channel Assignment Mode.................. AUTO
  Channel Update Interval.................. 600 seconds [startup]
  Anchor time (Hour of the day)............. 0
  Channel Update Contribution................ SNI
  CleanAir Event-driven RRM option........... Enabled
  CleanAir Event-driven RRM sensitivity..... Medium

---

**Configuring Cisco CleanAir on an Access Point**

This section contains the following topics:

- Configuring Cisco CleanAir on an Access Point (GUI), page 14-12
Configuring Cisco CleanAir on an Access Point (GUI)

To configure Cisco CleanAir functionality for a specific access point using the controller GUI, follow these steps:

**Step 1** Choose Wireless > Access Points > Radios > 802.11a/n or 802.11b/g/n to open the 802.11a/n (or 802.11b/g/n) Radios page.

**Figure 14-2 802.11a/n Cisco APs > Configure Page**

**Step 2** Hover your cursor over the blue drop-down arrow for the desired access point and click Configure. The 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page appears.

The CleanAir Capable field shows whether this access point can support CleanAir functionality. If it can, go to the next step to enable or disable CleanAir for this access point. If the access point cannot support CleanAir functionality, you cannot enable CleanAir for this access point.

**Note** By default, the Cisco CleanAir functionality is enabled on the radios.

**Step 3** Enable Cisco CleanAir functionality for this access point by choosing Enable from the CleanAir Status drop-down list. To disable CleanAir functionality for this access point, choose Disable. The default value is Enable. This setting overrides the global CleanAir configuration for this access point.

The Number of Spectrum Expert Connections text box shows the number of Spectrum Expert applications that are currently connected to the access point radio. Up to three active connections are possible.

**Step 4** Click Apply to commit your changes.
**Step 5** Click Save Configuration to save your changes.
**Step 6** Click Back to return to the 802.11a/n (or 802.11b/g/n) Radios page.
Step 7 View the Cisco CleanAir status for each access point radio by looking at the CleanAir Status text box on the 802.11a/n (or 802.11b/g/n) Radios page.

The Cisco CleanAir status is one of the following:

- **UP**—The spectrum sensor for the access point radio is currently operational (error code 0).
- **DOWN**—The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio.
- **ERROR**—The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable Cisco CleanAir functionality on the radio.
- **N/A**—This access point radio is not capable of supporting Cisco CleanAir functionality.

**Note** You can create a filter to make the 802.11a/n Radios page or the 802.11b/g/n Radios page show only access point radios that have a specific Cisco CleanAir status (such as UP, DOWN, ERROR, or N/A). This feature is especially useful if your list of access point radios spans multiple pages, preventing you from viewing them all at once. To create a filter, click Change Filter to open the Search AP dialog box, select one or more of the CleanAir Status check boxes, and click Find. Only the access point radios that match your search criteria appear on the 802.11a/n Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, CleanAir Status: UP).

### Configuring Cisco CleanAir on an Access Point (CLI)

**Step 1** Configure Cisco CleanAir functionality for a specific access point by entering this command:

```
config {802.11a | 802.11b} cleanair {enable | disable} Cisco_AP
```

**Step 2** Save your changes by entering this command:

```
save config
```

**Step 3** See the Cisco CleanAir configuration for a specific access point on the 802.11a/n or 802.11b/g/n network by entering this command:

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

Information similar to the following appears:

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... CISCO_AP3500

... Spectrum Management Information
  Spectrum Management Capable.............. Yes
  Spectrum Management Admin State........ Enabled
  Spectrum Management Operation State..... Up
  Rapid Update Mode......................... Disabled
  Spectrum Expert connection.............. Disabled
  Spectrum Sensor State.................... Configured (Error code = 0)
```

**Note** See Step 7 in the “Configuring Cisco CleanAir on an Access Point (GUI)” section for descriptions of the spectrum management operation states and the possible error codes for the spectrum sensor state.
Monitoring the Interference Devices

This section contains the following topics:

- Prerequisites for Monitoring the Interference Devices, page 14-14
- Monitoring the Interference Device (GUI), page 14-14
- Monitoring the Interference Device (CLI), page 14-16
- Monitoring Persistent Devices (GUI), page 14-18
- Monitoring Persistent Devices (CLI), page 14-18

Prerequisites for Monitoring the Interference Devices

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Monitoring the Interference Device (GUI)

**Step 1**  Choose Monitor > Cisco CleanAir > 802.11a/n or 802.11b/g > Interference Devices to open the CleanAir > Interference Devices page.

![CleanAir > Interference Device Page](image)

This page shows the following information:

- AP Name—The name of the access point where the interference device is detected.
- Radio Slot #—Slot where the radio is installed.
- Interferer Type—Type of the interferer.
- Affected Channel—Channel that the device affects.
- Detected Time—Time at which the interference was detected.
- Severity—Severity index of the interfering device.
- Duty Cycle (%)—Proportion of time during which the interfering device was active.
- RSSI—Receive signal strength indicator (RSSI) of the access point.
- DevID—Device identification number that uniquely identified the interfering device.
• ClusterID—Cluster identification number that uniquely identifies the type of the devices.

  When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed which results in the spectrum sensor to temporarily stop detecting the device. This device is then correctly marked as down. A down device is correctly removed from the spectrum database. In cases when all the interferer detections for a specific devices are reported, the cluster ID is kept alive for an extended period of time to prevent possible device detection bouncing. If the same device is detected again, it is merged with the original cluster ID and the device detection history is preserved.

  For example, some bluetooth headsets operate on battery power. These devices employ methods to reduce power consumption, such as turning off the transmitter when not actually needed. Such devices can appear to come and go from the classification. To manage these devices, CleanAir keeps the cluster IDs longer and they are remerged into a single record upon detection. This process smoothens the user records and accurately represents the device history.

  Step 2 Click Change Filter to display the information about interference devices based on a particular criteria.

  Step 3 Click Clear Filter to remove the filter and display the entire access point list.

  You can create a filter to display the list of interference devices that are based on the following filtering parameters:

  • Cluster ID—To filter based on the Cluster ID, select the check box and enter the Cluster ID in the text box next to this field.

  • AP Name—To filter based on the access point name, select the check box and enter the access point name in the text box next to this field.

  • Interferer Type—To filter based on the type of the interference device, select the check box and select the interferer device from the options.

  Choose one of the interferer devices:

  - BT Link
  - MW Oven
  - 802.11 FH
  - BT Discovery
  - TDD Transmit
  - Jammer
  - Continuous TX
  - DECT Phone
  - Video Camera
  - 802.15.4
  - WiFi Inverted
  - WiFi Inv. Ch
  - SuperAG
  - Canopy
  - XBox
  - WiMax Mobile
  - WiMax Fixed
Monitoring the Interference Devices

- WiFi ACI
- Unclassified
  - Activity Channels
  - Severity
  - Duty Cycle (%)
  - RSSI

Step 4 Click Find to commit your changes.
The current filter parameters are displayed in the Current Filter field.

---

Monitoring the Interference Device (CLI)

This section describes the commands that you can use to monitor the interference devices for the 802.11a/n or 802.11b/g/n radio band.

Detecting Interferers by an Access Point

See information for all of the interferers detected by a specific access point on the 802.11a/n or 802.11b/g/n radio band by entering this command:

```
show {802.11a | 802.11b} cleanair device ap Cisco_AP
```

Information similar to the following appears:

DC = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI = Received Signal Strength Index (dBm)
DevID = Device ID

<table>
<thead>
<tr>
<th>No</th>
<th>ClusterID</th>
<th>DevID</th>
<th>Type</th>
<th>AP Name</th>
<th>ISI</th>
<th>RSSI</th>
<th>DC</th>
<th>Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>c2:f7:40:00:00:03</td>
<td>0x8001</td>
<td>DECT phone</td>
<td>CISCO_AP3500</td>
<td>1</td>
<td>-43</td>
<td>3</td>
<td>149,153,157,161</td>
</tr>
<tr>
<td>3</td>
<td>c2:f7:40:00:00:03</td>
<td>0x8005</td>
<td>Canopy</td>
<td>CISCO_AP3500</td>
<td>2</td>
<td>-62</td>
<td>2</td>
<td>153,157,161,165</td>
</tr>
</tbody>
</table>

When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed which results in the spectrum sensor to temporarily stop detecting the device. This device is then correctly marked as down. A down device is correctly removed from the spectrum database. In cases when all the interferer detections for a specific devices are reported, the cluster ID is kept alive for an extended period of time to prevent possible device detection bouncing. If the same device is detected again, it is merged with the original cluster ID and the device detection history is preserved.

For example, some bluetooth headsets operate on battery power. These devices employ methods to reduce power consumption, such as turning off the transmitter when not actually needed. Such devices can appear to come and go from the classification. To manage these devices, CleanAir keeps the cluster IDs longer and they are remerged into a single record upon detection. This process smoothen the user records and accurately represents the device history.
Detecting Interferers by Device Type

See information for all of the interferers of a specific device type on the 802.11a/n or 802.11b/g/n radio band by entering this command:

```
show {802.11a | 802.11b} cleanair device type type
```

Information similar to the following appears:

DC = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI = Received Signal Strength Index (dBm)
DevID = Device ID
* indicates cluster center device

```
No  ClusterID  DevID   Type       AP Name    ISI  RSSI DC Channel
---  ---------  ------  ---------- ------------ ---- ----- --- --------------
1    b4:f7:40:00:00:03 0x4185 DECT-like (26) CISCO_AP35001 -58   3 153,157,161,165
```

Detecting Persistent Sources of Interference

View a list of persistent sources of interference for a specific access point on the 802.11a/n or 802.11b/g/n radio band by entering this command:

```
show ap auto-rf {802.11a | 802.11b} Cisco_AP
```

Information similar to the following appears:

```
Number Of Slots................................. 2
AP Name.......................................... AP1-L
MAC Address...................................... c4:7d:4f:3a:07:1e
Slot ID........................................ 1
Radio Type..................................... RADIO_TYPE_80211a
Sub-band Type.................................. All
Noise Information
   Noise Profile............................... PASSED
      Channel 34.................................. -97 dBm
      Channel 36.................................. -90 dBm
      Channel 38.................................. -97 dBm
Interference Information
   Interference Profile......................... PASSED
      Channel 34.................................. -128 dBm @ 0 % busy
      Channel 36.................................. -128 dBm @ 0 % busy
      Channel 38.................................. -128 dBm @ 0 % busy
      Channel 40.................................. -128 dBm @ 0 % busy
Load Information
   Load Profile................................. PASSED
   Receive Utilization........................ 0 %
   Transmit Utilization....................... 0 %
   Channel Utilization........................ 0 %
   Attached Clients................................ 0 clients
Coverage Information
   Coverage Profile............................ PASSED
   Failed Clients................................ 0 clients
Client Signal Strengths
   RSSI -100 dbm................................ 0 clients
   RSSI -92 dbm................................ 0 clients
   RSSI -84 dbm................................ 0 clients
Client Signal To Noise Ratios
   SNR 0 dB..................................... 0 clients
   SNR 10 dB................................... 0 clients
   SNR 15 dB................................... 0 clients
Nearby APs
Monitoring the Interference Devices

AP c4:7d:4f:52:cf:a0 slot 1................. -36 dBm on 149 (10.10.10.27)
AP c4:7d:4f:53:1b:50 slot 1................. -10 dBm on 149 (10.10.10.27)

Radar Information
Channel Assignment Information
Current Channel Average Energy.............. unknown
Previous Channel Average Energy.............. unknown
Channel Change Count.......................... 0

Last Channel Change Time.................... Mon May 17 11:56:32 2010
Recommended Best Channel................... 149

RF Parameter Recommendations
Power Level................................... 7
RTS/CTS Threshold........................... 2347
Fragmentation Threshold..................... 2346
Antenna Pattern................................ 0

Persistent Interference Devices

<table>
<thead>
<tr>
<th>Class Type</th>
<th>Channel</th>
<th>DC (%)</th>
<th>RSSI (dBm)</th>
<th>Last Update Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canopy</td>
<td>149</td>
<td>4</td>
<td>-63</td>
<td>Tue May 18 03:21:16 2010</td>
</tr>
</tbody>
</table>

All third party trademarks are the property of their respective owners.

Monitoring Persistent Devices (GUI)

To monitor persistent devices on a specific access point using the controller GUI:
Choose Wireless > Access Points > Radios > 802.11a/n or 802.11b/g/n to open the 802.11a/n (or 802.11b/g/n) Radios page. Hover your cursor over the blue drop-down arrow for the desired access point and click Detail. The 802.11a/n (or 802.11b/g/n) AP Interfaces > Detail page appears.

This page displays the details of the access points along with the list of persistent devices detected by this access point. Details of the persistent devices is displayed under the Persistent Devices section.

The following information for each persistent device is available:

Class Type—The class type of the persistent device.
Channel—Channel this device is affecting.
DC(%)—Duty cycle (in percentage) of the persistent device.
RSSI(dBm)—RSSI indicator of the persistent device.
Last Seen Time—Timestamp when the device was last active.

Monitoring Persistent Devices (CLI)

To view the list of persistent devices using the CLI, use the following command:

```
show ap auto-rf {802.11a | 802.11b} ap_name
```

Number Of Slots............................. 2
AP Name......................................... AP_1142_MAP
MAC Address................................... c4:7d:4f:3a:35:38
Slot ID......................................... 1
Radio Type..................................... RADIO_TYPE_80211a
Sub-band Type................................. All
Noise Information
Power Level................................... 1
RTS/CTS Threshold........................... 2347
Fragmentation Threshold.................... 2346
**Antenna Pattern**

**Persistent Interference Devices**

<table>
<thead>
<tr>
<th>Class Type</th>
<th>Channel</th>
<th>DC (%)</th>
<th>RSSI (dBm)</th>
<th>Last Update Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Camera</td>
<td>149</td>
<td>100</td>
<td>-34</td>
<td>Tue Nov 8 10:06:25 2011</td>
</tr>
</tbody>
</table>

The following information for each persistent device is available:

- **Class Type**—The class type of the persistent device.
- **Channel**—Channel on which this device is affecting.
- **DC(%)**—Duty cycle (in percentage) of the persistent device.
- **RSSI(dBm)**—RSSI indicator of the persistent device.
- **Last Updated Time**—Timestamp when the device was last active.

---

**Monitoring the Air Quality of Radio Bands**

This section contains the following topics:

- Monitoring the Air Quality of Radio Bands (GUI), page 14-19
- Monitoring the Air Quality of Radio Bands (CLI), page 14-20
- Monitoring the Worst Air Quality of Radio Bands (GUI), page 14-21
- Monitoring the Air Quality of Radio Bands (CLI), page 14-20

---

**Monitoring the Air Quality of Radio Bands (GUI)**

To monitor the air quality of radio bands using the controller GUI, follow this step:

Choose **Monitor > Cisco CleanAir > 802.11a/n or 802.11b/g > Air Quality Report** to open the **CleanAir > Air Quality Report** page.

**Figure 14-4** CleanAir > Air Quality Report Page

This page shows the air quality of both the 802.11a/n and 802.11b/g/n radio bands. Specifically, it shows the following information:
Monitoring the Air Quality of Radio Bands

This section describes the commands that you can use to monitor the air quality of the 802.11a/n or 802.11b/g/n radio band.

Viewing a Summary of the Air Quality

See a summary of the air quality for the 802.11a/n or 802.11b/g/n radio band by entering this command:

```
show {802.11a | 802.11b} cleanair air-quality summary
```

Information similar to the following appears:

```
AQ = Air Quality
DFS = Dynamic Frequency Selection

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Channel</th>
<th>Avg AQ</th>
<th>Min AQ</th>
<th>Interferers</th>
<th>DFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO_AP3500</td>
<td>36</td>
<td>95</td>
<td>70</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CISCO_AP3500</td>
<td>40</td>
<td>93</td>
<td>75</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CISCO_AP3500</td>
<td>44</td>
<td>95</td>
<td>80</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CISCO_AP3500</td>
<td>48</td>
<td>97</td>
<td>75</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CISCO_AP3500</td>
<td>52</td>
<td>98</td>
<td>80</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Viewing Air Quality for all Access Points on a Radio Band

See information for the 802.11a/n or 802.11b/g/n access point with the air quality by entering this command:

```
show {802.11a | 802.11b} cleanair air-quality
```

Information similar to the following appears:

```
AQ = Air Quality
DFS = Dynamic Frequency Selection

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Channel</th>
<th>Avg AQ</th>
<th>Min AQ</th>
<th>Interferers</th>
<th>DFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO_AP3500</td>
<td>1</td>
<td>83</td>
<td>57</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>
```

- AP Name—The name of the access point that reported the worst air quality for the 802.11a/n or 802.11b/g/n radio band.
- Radio Slot—The slot number where the radio is installed.
- Channel—The radio channel where the air quality is monitored.
- Minimum AQ—The minimum air quality for this radio channel.
- Average AQ—The average air quality for this radio channel.
- Interferer—The number of interferers detected by the radios on the 802.11a/n or 802.11b/g/n radio band.
- DFS—Dynamic Frequency Selection. This indicates if DFS is enabled or not.
Viewing Air Quality for an Access Point on a Radio Band

See air quality information for a specific access point on the 802.11a/n or 802.11b/g/n radio band by entering this command:

```
show {802.11a | 802.11b} cleanair air-quality Cisco_AP
```

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Slot</th>
<th>Channel</th>
<th>Avg AQ</th>
<th>Min AQ</th>
<th>Total Power (dBm)</th>
<th>Total Duty Cycle (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>140</td>
<td>100</td>
<td>100</td>
<td>-89</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interferer Power (dBm)</th>
<th>Interferer Duty Cycle (%)</th>
<th>Interferers DFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>-128</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Monitoring the Worst Air Quality of Radio Bands (GUI)

**Step 1** Choose Monitor > Cisco CleanAir > 802.11b/g > Worst Air-Quality to open the CleanAir > Worst Air Quality Report page.

This page shows the air quality of both the 802.11a/n and 802.11b/g/n radio bands. Specifically, it shows the following information:

- **AP Name**—The name of the access point that reported the worst air quality for the 802.11a/n or 802.11b/g/n radio band.
- **Channel Number**—The radio channel with the worst reported air quality.
- **Minimum Air Quality Index (1 to 100)**—The minimum air quality for this radio channel. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Average Air Quality Index (1 to 100)**—The average air quality for this radio channel. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Interference Device Count**—The number of interferers detected by the radios on the 802.11a/n or 802.11b/g/n radio band.
Chapter 14      Configuring Cisco CleanAir

Monitoring the Air Quality of Radio Bands

Step 2  View a list of persistent sources of interference for a specific access point radio as follows:

a.  Choose Wireless > Access Points > Radios > 802.11a/n or 802.11b/g/n to open the 802.11a/n (or 802.11b/g/n) Radios page.

b.  Hover your cursor over the blue drop-down arrow for the desired access point radio and click CleanAir-RRM. The 802.11a/n (or 802.11b/g/n) Cisco APs > Access Point Name > Persistent Devices page appears. This page lists the device types of persistent sources of interference detected by this access point radio. It also shows the channel on which the interference was detected, the percentage of time that the interferer was active (duty cycle), the received signal strength (RSSI) of the interferer, and the day and time when the interferer was last detected.

Monitoring the Worst Air Quality of Radio Bands (CLI)

This section describes the commands that you can use to monitor the air quality of the 802.11a/n or 802.11b/g/n radio band.

Viewing a Summary of the Air Quality (CLI)

See a summary of the air quality for the 802.11a/n or 802.11b/g/n radio band by entering this command:

```
show {802.11a | 802.11b} cleanair air-quality summary
```

Information similar to the following appears:

```
AQ = Air Quality  
DFS = Dynamic Frequency Selection
AP Name    Channel  Avg AQ  Min AQ  Interferers DFS
-------------- -------- ------- ------- ------------ -----
CISCO_AP3500  36   95  70  0
CISCO_AP3500  40        93 75   0
CISCO_AP3500  44        95 80   0
CISCO_AP3500  48        97 75   0
CISCO_AP3500  52        98 80   0
```

Viewing Worst Air Quality Information for all Access Points on a Radio Band (CLI)

See information for the 802.11a/n or 802.11b/g/n access point with the worst air quality by entering this command:

```
show {802.11a | 802.11b} cleanair air-quality worst
```

Information similar to the following appears:

```
AQ = Air Quality  
DFS = Dynamic Frequency Selection
AP Name    Channel  Avg AQ  Min AQ  Interferers  DFS
-------------- --------- -------- --------- ------------ -----
CISCO_AP3500 1  83   57    3   5
```
Viewing Air Quality for an Access Point on a Radio Band (CLI)

See air quality information for a specific access point on the 802.11a/n or 802.11b/g/n radio band by entering this command:

```
show {802.11a | 802.11b} cleanair air-quality Cisco_AP
```

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Slot</th>
<th>Channel</th>
<th>Avg AQ</th>
<th>Min AQ</th>
<th>Total Power (dBm)</th>
<th>Total Duty Cycle (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>140</td>
<td>100</td>
<td>100</td>
<td>-89</td>
<td>0</td>
</tr>
</tbody>
</table>

Interferer Power (dBm) Interferer Duty Cycle (%) Interferers DFS

| -128 | 0 | 0 |

Viewing Air Quality for an Access Point by Device Type (CLI)

- See information for all of the interferers detected by a specific access point on the 802.11a/n or 802.11b/g/n radio band by entering this command:

```
show {802.11a | 802.11b} cleanair device ap Cisco_AP
```

Information similar to the following appears:

- DC = Duty Cycle (%)
- ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
- RSSI = Received Signal Strength Index (dBm)
- DevID = Device ID

<table>
<thead>
<tr>
<th>No</th>
<th>ClusterID</th>
<th>DevID</th>
<th>Type</th>
<th>AP Name</th>
<th>ISI</th>
<th>RSSI</th>
<th>DC</th>
<th>Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>c2:f7:40:00:00:03</td>
<td>0x8001 DECT phone</td>
<td>CISCO_AP3500 1</td>
<td>-43</td>
<td>3</td>
<td>149,153,157,161</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>c2:f7:40:00:00:03</td>
<td>0x8005 Canopy</td>
<td>CISCO_AP3500 2</td>
<td>-62</td>
<td>2</td>
<td>153,157,161,165</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- See information for all of the interferers of a specific device type on the 802.11a/n or 802.11b/g/n radio band by entering this command:

```
show {802.11a | 802.11b} cleanair device type type
```

where you choose the type as one of the following:

- **802.11-fh**—An 802.11 frequency-hopping device (802.11b/g/n only)
- **802.11-inv**—A device using spectrally inverted Wi-Fi signals
- **802.11-nonstd**—A device using nonstandard Wi-Fi channels
- **802.15.4**—An 802.15.4 device (802.11b/g/n only)
- **all**—All interference device types (this is the default value)
- **bt-discovery**—A bluetooth discovery (802.11b/g/n only)
- **bt-link**—A bluetooth link (802.11b/g/n only)
- **canopy**—A canopy bridge device
- **cont-tx**—A continuous transmitter
- **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
- **jammer**—A jamming device
- **mw-oven**—A microwave oven (802.11b/g/n only)
Detecting Persistent Sources of Interference (CLI)

See a list of persistent sources of interference for a specific access point on the 802.11a/n or 802.11b/g/n radio band by entering this command:

```plaintext
show ap auto-rf {802.11a | 802.11b} Cisco_AP
```

Information similar to the following appears:

Number Of Slots.................................. 2
AP Name.......................................... CISCO_AP3500

Persistent Interferers

<table>
<thead>
<tr>
<th>Classtype</th>
<th>Channel</th>
<th>DC (%)</th>
<th>RSSI (dBm)</th>
<th>Last Update Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11FH</td>
<td>149</td>
<td>3</td>
<td>-58</td>
<td>Thu Jan 1 00:20:34 2009</td>
</tr>
<tr>
<td>Radar</td>
<td>153</td>
<td>2</td>
<td>-81</td>
<td>Thu Jan 1 00:20:35 2009</td>
</tr>
<tr>
<td>Continuous Transmitter</td>
<td>157</td>
<td>2</td>
<td>-62</td>
<td>Thu Jan 1 00:20:36 2009</td>
</tr>
</tbody>
</table>

All third party trademarks are the property of their respective owners.

Configuring a Spectrum Expert Connection

To obtain detailed spectrum data that can be used to generate RF analysis plots similar to those provided by a spectrum analyzer, you can configure a Cisco CleanAir-enabled access point to connect directly to a Microsoft Windows XP or Vista PC running the Spectrum Expert application (referred to as a Spectrum Expert console). You can initiate the Spectrum Expert connection semi-automatically from WCS or by manually launching it from the controller. This section provides instructions for the latter.

To configure a Spectrum Expert, follow these steps:
Step 1  Prior to establishing a connection between the Spectrum Expert console and the access point, make sure that IP address routing is properly configured and the network spectrum interface (NSI) ports are open in any intervening firewalls.

Step 2  Make sure that Cisco CleanAir functionality is enabled for the access point that will be connected to the Spectrum Expert console.

Step 3  Configure the access point for SE-Connect mode using the controller GUI or CLI.

Note  The SE-Connect mode is set for the entire access point, not just a single radio. However, the Spectrum Expert console connects to a single radio at a time.

• If you are using the controller GUI, follow these steps:
  a. Choose Wireless > Access Points > All APs to open the All APs page.
  b. Click the name of the desired access point to open the All APs > Details page.
  c. Choose SE-Connect from the AP Mode drop-down list. This mode is available only for access points that are capable of supporting Cisco CleanAir functionality. For the SE-Connect mode to appear as an available option, the access point must have at least one spectrum-capable radio in the Enable state.
  d. Click Apply to commit your changes.
  e. Click OK when prompted to reboot the access point.

• If you are using the controller CLI, follow these steps:
  a. To configure the access point for SE-Connect mode, enter this command:
     `config ap mode se-connect Cisco_AP`
  b. When prompted to reboot the access point, enter Y.
  c. To verify the SE-Connect configuration status for the access point, enter this command:
     `show ap config {802.11a | 802.11b} Cisco_AP`
     Information similar to the following appears:
     ```
     Cisco AP Identifier.............................. 0
     Cisco AP Name.................................... CISCO_AP3500
     ...
     Spectrum Management Information
     Spectrum Management Capable............... Yes
     Spectrum Management Admin State......... Enabled
     Spectrum Management Operation State..... Up
     Rapid Update Mode............................. Disabled
     Spectrum Expert connection............... Enabled
     Spectrum Sensor State......................... Configured (Error code = 0)
     ```

Step 4  On the Windows PC, access the Cisco Software Center from this URL:
`http://www.cisco.com/cisco/software/navigator.html`

Step 5  Click Product > Wireless > Cisco Spectrum Intelligence > Cisco Spectrum Expert > Cisco Spectrum Expert Wi-Fi, and then download the Spectrum Expert 4.0 executable (*.exe) file.

Step 6  Run the Spectrum Expert application on the PC.
Step 7  When the Connect to Sensor dialog box appears, enter the IP address of the access point, choose the access point radio, and enter the 16-byte network spectrum interface (NSI) key to authenticate. The Spectrum Expert application opens a TCP/IP connection directly to the access point using the NSI protocol.

Note  The access point must be a TCP server listening on ports 37540 for 2.4 GHz and 37550 for 5 GHz frequencies. These ports must be opened for the spectrum expert application to connect to the access point using the NSI protocol.

Note  To view the NSI key from the controller CLI, enter the `show ap config {802.11a | 802.11b} Cisco_AP` command. To view the NSI key from the controller GUI, choose Wireless > Access Points > All APs to open the All APs page. Click the name of the desired access point to open the All APs > Details page. The NSI key appears in the General tab.

When an access point in SE-Connect mode joins a controller, it sends a Spectrum Capabilities notification message, and the controller responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the controller for use in NSI authentication. The controller generates one key per access point, which the access point stores until it is rebooted.

Note  You can establish up to three Spectrum Expert console connections per access point radio. The Number of Spectrum Expert Connections text box on the 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page of the controller GUI shows the number of Spectrum Expert applications that are currently connected to the access point radio.

Step 8  Verify that the Spectrum Expert console is connected to the access point by selecting the Slave Remote Sensor text box in the bottom right corner of the Spectrum Expert application. If the two devices are connected, the IP address of the access point appears in this text box.

Step 9  Use the Spectrum Expert application to view and analyze spectrum data from the access point.

Additional References

For additional information related to configuring CleanAir, see the following sections:
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco WCS Reports on CleanAir</td>
<td>Cisco Wireless Control System Configuration Guide</td>
</tr>
<tr>
<td>To initiate a Spectrum Expert connection using WCS</td>
<td>Cisco Wireless Control System Configuration Guide</td>
</tr>
</tbody>
</table>

Feature History for Configuring CleanAir

Table 14-1 lists the release history for this feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster ID</td>
<td>7.0.116.0</td>
<td>Cluster identification number that uniquely identifies the type of the devices.</td>
</tr>
<tr>
<td>CleanAir</td>
<td>7.0.98.0</td>
<td>CleanAir enables you to identify and track non-Wi-Fi sources of interference, adjust your network configuration for optimal performance, identify threats from malicious devices, and allow your WLAN to coexist with other wireless devices.</td>
</tr>
</tbody>
</table>
Configuring Mobility Groups

This chapter contains these sections:

- Information About Mobility, page 15-1
- Information About Mobility Groups, page 15-4
- Configuring Mobility Groups, page 15-9
- Viewing Mobility Group Statistics, page 15-16
- Configuring Auto-Anchor Mobility, page 15-19
- Validating WLAN Mobility Security Values, page 15-23
- Using Symmetric Mobility Tunneling, page 15-24
- Verifying Symmetric Mobility Tunneling, page 15-26
- Running Mobility Ping Tests, page 15-27
- Configuring Dynamic Anchoring for Clients with Static IP Addresses, page 15-28
- Configuring Foreign Mappings, page 15-30

Information About Mobility

Mobility, or roaming, is a wireless LAN client’s ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible. This section explains how mobility works when controllers are included in a wireless network.

When a wireless client associates and authenticates to an access point, the access point’s controller places an entry for that client in its client database. This entry includes the client’s MAC and IP addresses, security context and associations, quality of service (QoS) contexts, the WLAN, and the associated access point. The controller uses this information to forward frames and manage traffic to and from the wireless client. Figure 15-1 shows a wireless client that roams from one access point to another when both access points are joined to the same controller.
When the wireless client moves its association from one access point to another, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well.

The process becomes more complicated, however, when a client roams from an access point joined to one controller to an access point joined to a different controller. It also varies based on whether the controllers are operating on the same subnet. Figure 15-2 shows inter-controller roaming, which occurs when the controllers’ wireless LAN interfaces are on the same IP subnet.
Figure 15-2  Inter-Controller Roaming

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

Note

All clients configured with 802.1X/Wi-Fi Protected Access (WPA) security complete a full authentication in order to comply with the IEEE standard.

Figure 15-3 shows inter-subnet roaming, which occurs when the controllers’ wireless LAN interfaces are on different IP subnets.
Inter-subnet roaming is similar to inter-controller roaming in that the controllers exchange mobility messages on the client roam. However, instead of moving the client database entry to the new controller, 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 controller. The roam remains transparent to the wireless client, and the client maintains its original IP address.

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

**Note**
Seamless mobility is not supported for native IPv6 clients if the interface is untagged.

## Information About 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 controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers 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. Figure 15-4 shows an example of a mobility group.

**Note**

Controllers do not have to be of the same model to be a member of a mobility group. Mobility groups can be comprised of any combination of controller platforms.

**Figure 15-4 Single Mobility Group**

As shown above, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message (or multicast message if mobility multicast is configured) to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client.

**Note**

Controller software release 5.1 or later releases support up to 24 controllers in a single mobility group. The number of access points supported in a mobility group is bound by the number of controllers and controller types in the group.

Examples:

1. A 4404-100 controller supports up to 100 access points. Therefore, a mobility group that consists of 24 4404-100 controllers supports up to 2400 access points (24 * 100 = 2400 access points).
2. A 4402-25 controller supports up to 25 access points, and a 4402-50 controller supports up to 50 access points. Therefore, a mobility group that consists of 12 4402-25 controllers and 12 4402-50 controllers supports up to 900 access points (12 * 25 + 12 * 50 = 300 + 600 = 900 access points).
Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different controllers within the same wireless network. Figure 15-5 shows the results of creating distinct mobility group names for two groups of controllers.

![Figure 15-5 Two Mobility Groups](image)

The controllers in the ABC mobility group share access point and client information with each other. The controllers in the ABC mobility group do not share the access point or client information with the XYZ controllers, which are in a different mobility group. Likewise, the controllers in the XYZ mobility group do not share access point or client information with the controllers in the ABC mobility group. This feature ensures mobility group isolation across the network.

Every controller maintains information about its peer controllers in a mobility list. Controllers can communicate across mobility groups and clients may roam between access points in different mobility groups if the controllers are included in each other’s mobility lists. In the following example, controller 1 can communicate with either controller 2 or 3, but controller 2 and controller 3 can communicate only with controller 1 and not with each other. Similarly, clients can roam between controller 1 and controller 2 or between controller 1 and controller 3 but not between controller 2 and controller 3.

**Example:**

<table>
<thead>
<tr>
<th>Controller 1</th>
<th>Controller 2</th>
<th>Controller 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility group: A</td>
<td>Mobility group: A</td>
<td>Mobility group: C</td>
</tr>
<tr>
<td>Mobility list:</td>
<td>Mobility list:</td>
<td>Mobility list:</td>
</tr>
<tr>
<td>Controller 1 (group A)</td>
<td>Controller 1 (group A)</td>
<td>Controller 1 (group A)</td>
</tr>
<tr>
<td>Controller 2 (group A)</td>
<td>Controller 2 (group A)</td>
<td>Controller 3 (group C)</td>
</tr>
<tr>
<td>Controller 3 (group C)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Controller software release 5.1 or later releases support up to 72 controllers in a controller's mobility list. The support for 24 controllers in a mobility group has been the same across all releases.

The controller supports seamless roaming across multiple mobility groups. During seamless roaming, the client maintains its IP address across all mobility groups; however, Cisco Centralized Key Management (CCKM) and public key cryptography (PKC) are supported only for inter-mobility-group roaming. When a client crosses a mobility group boundary during a roam, the client is fully authenticated, but the IP address is maintained, and mobility tunneling is initiated for Layer 3 roaming.

Controller software release 5.0 release supports up to 48 controllers in a mobility list.

**Determining When to Include Controllers in a Mobility Group**

If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, but both controllers should be in the same mobility group.

**Messaging Among Mobility Groups**

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers. In controller software release 5.0 or later releases, two improvements have been made to mobility messaging, each of which is especially useful when sending messages to the full list of mobility members:

- Sending Mobile Announce messages within the same group first and then to other groups in the list
- The controller sends a Mobile Announce message to members in the mobility list each time that a new client associates to it. In controller software releases prior to 5.0, the controller sends this message to all members in the list irrespective of the group to which they belong. However, in controller software release 5.0 or later releases, the controller sends the message only to those members that are in the same group as the controller (the local group) and then includes all of the other members while sending retries.
- Sending Mobile Announce messages using multicast instead of unicast

In controller software releases prior to 5.0, the controller sends all mobility messages using unicast mode, which requires sending a copy of the messages to every mobility member. This behavior is not efficient because many messages (such as Mobile Announce, PMK Update, AP List Update, and IDS Shun) are meant for all members in the group. In controller software release 5.0 or later releases, the controller may be configured to use multicast to send the Mobile Announce messages. This behavior allows the controller to send only one copy of the message to the network, which destines it to the multicast group that contains all the mobility members. To derive the maximum benefit from multicast messaging, we recommend that it be enabled on all group members.

**Using Mobility Groups with NAT Devices**

In controller software releases prior to 4.2, mobility between controllers in the same mobility group does not work if one of the controllers is behind a network address translation (NAT) device. This behavior creates a problem for the guest anchor feature where one controller is expected to be outside the firewall.
Mobility message payloads carry IP address information about the source controller. This IP address is validated with the source IP address of the IP header. This behavior is a problem when a NAT device is introduced in the network because it changes the source IP address in the IP header. In the guest WLAN feature, any mobility packet, that is being routed through a NAT device is dropped because of the IP address mismatch.

In controller software release 4.2 or later releases, the mobility group lookup is changed to use the MAC address of the source controller. Because the source IP address is changed due to the mapping in the NAT device, the mobility group database is searched before a reply is sent to get the IP address of the requesting controller. This process is done using the MAC address of the requesting controller.

When configuring the mobility group in a network where NAT is enabled, enter the IP address that is sent to the controller from the NAT device rather than the controller’s management interface IP address. Also, make sure that the following ports are open on the firewall if you are using a firewall such as PIX:

- UDP 16666 for tunnel control traffic
- IP protocol 97 for user data traffic
- UDP 161 and 162 for SNMP

Client mobility among controllers works only if auto-anchor mobility (also called guest tunneling) or symmetric mobility tunneling is enabled. Asymmetric tunneling is not supported when mobility controllers are behind the NAT device. See the “Configuring Auto-Anchor Mobility” and “Using Symmetric Mobility Tunneling” sections for details on these mobility options.

Figure 15-6 shows an example mobility group configuration with a NAT device. In this example, all packets pass through the NAT device (that is, packets from the source to the destination and vice versa). Figure 15-7 shows an example mobility group configuration with two NAT devices. In this example, one NAT device is used between the source and the gateway, and the second NAT device is used between the destination and the gateway.
Configuring Mobility Groups

This section describes how to configure controller mobility groups through either the GUI or the CLI.

**Note**
You can also configure mobility groups using the Cisco Wireless Control System (WCS). See the *Cisco Wireless Control System Configuration Guide* for instructions.

**Prerequisites for Configuring Mobility Groups**

Before you add controllers to a mobility group, you must verify that the following requirements have been met for all controllers that are to be included in the group:

- IP connectivity must exist between the management interfaces of all controllers.
  
  **Note**
  You can verify IP connectivity by pinging the controllers.

- Mobility control packets can use any interface address as the source, based on routing table. It is recommended that all controllers in the mobility group should have the management interface in the same subnet. A topology where one controller’s management interface and other controller’s dynamic interface are on same subnet not recommended for seamless mobility.

- All controllers must be configured with the same mobility group name.
Chapter 15  Configuring Mobility Groups

Note  The mobility group name is generally set at deployment time through the Startup Wizard. However, you can change it if necessary through the Default Mobility Domain Name text box on the Controller > General page. The mobility group name is case sensitive.

Note  For the Cisco WiSM, both controllers should be configured with the same mobility group name for seamless routing among 300 access points.

Note  If one controller in the mobility group is configured for preferred call configuration, other controllers in the mobility group must also be configured with the same preferred call configuration.

- When controllers in the mobility list use different software versions, Layer 2 or Layer 3 clients have limited roaming support. Layer 2 or Layer 3 client roaming is supported only between controllers that use the same version or with controllers that run versions 4.2.X, 6.0.X, and 7.0.X. See Table 15-2 for more information on mobility support across controllers.

Note  If you inadvertently configure a controller that runs software release 5.2 or later releases with a failover controller that runs a different software release (such as 4.2, 5.0, or 5.1), the access point might take a long time to join the failover controller because the access point starts the discovery process in CAPWAP and then changes to LWAPP discovery.

- All controllers must be configured with the same virtual interface IP address.

Note  If necessary, you can change the virtual interface IP address by editing the virtual interface name on the Controller > Interfaces page. See Chapter 4, “Configuring Ports and Interfaces,” for more information on the controller’s virtual interface.

Note  If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming may appear to work, but the handoff does not complete, and the client loses connectivity for a period of time.

- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you will be configuring all controllers with the MAC address and IP address of all the other mobility group members.

Note  You can find the MAC and IP addresses of the other controllers to be included in the mobility group on the Controller > Mobility Groups page of each controller’s GUI.

- When you configure mobility groups using a third-party firewall, for example, Cisco PIX, or Cisco ASA, you must open port 16666, and IP protocol 97.
- For inter-controller CAPWAP data and control traffic for releases 5.0, 6.0, and 7.0, you must open the ports 5247 and 5246.
For inter-controller LWAPP data and control traffic for prior releases to 5.0, do not open ports 12222 and 12223.

Table 15-1 lists the protocols and port numbers that must be used for management and operational purposes:

<table>
<thead>
<tr>
<th>Protocol/Service</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH/Telnet</td>
<td>TCP Port 22 or 29</td>
</tr>
<tr>
<td>TFTP</td>
<td>UDP Port 69</td>
</tr>
<tr>
<td>NTP</td>
<td>UDP Port 123</td>
</tr>
<tr>
<td>SNMP</td>
<td>UDP Port 161 for gets and sets and UDP port 162 for traps.</td>
</tr>
<tr>
<td>HTTPS/HTTP</td>
<td>TCP port 443 for HTTPS and port 80 for HTTP</td>
</tr>
<tr>
<td>Syslog</td>
<td>TCP port 514</td>
</tr>
<tr>
<td>Radius Auth/Account</td>
<td>UDP port 1812 and 1813</td>
</tr>
</tbody>
</table>

Note: You cannot perform port address translation (PAT) on the firewall. You must configure one-to-one network address translation (NAT).

Table 15-2 describes support for mobility across controllers with different software versions.

<table>
<thead>
<tr>
<th>CUWN Service</th>
<th>4.2.X.X</th>
<th>5.0.X.X</th>
<th>5.1.X.X</th>
<th>6.0.X.X</th>
<th>7.0.X.X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 and Layer 3 Roaming</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Guest access/termination</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Rogue detection</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Fast roaming (CCKM) in a mobility group</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Location services</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Radio Resource Management (RRM)</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Management Frame Protection (MFP)</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>AP failover</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Configuring Mobility Groups (GUI)

Step 1: Choose Controller > Mobility Management > Mobility Groups to open the Static Mobility Group Members page.
Figure 15-8  Static Mobility Group Members Page

This page shows the mobility group name in the Default Mobility Group text box and lists the MAC address and IP address of each controller that is currently a member of the mobility group. The first entry is the local controller, which cannot be deleted.

**Note**  If you want to delete any of the remote controllers from the mobility group, hover your cursor over the blue drop-down arrow for the desired controller and choose Remove.

**Step 2**  Perform one of the following to add controllers to a mobility group:

- If you are adding only one controller or want to individually add multiple controllers, click New and go.
  
  OR

- If you are adding multiple controllers and want to add them in bulk, click EditAll and go to .

  **Note**  The EditAll option enables you to enter the MAC and IP addresses of all the current mobility group members and then copy and paste all the entries from one controller to the other controllers in the mobility group.

**Step 3**  Click New to open the Mobility Group Member > New page.

**Step 4**  Add a controller to the mobility group as follows:

a. In the Member IP Address text box, enter the management interface IP address of the controller to be added.

  **Note**  If you are configuring the mobility group in a network where network address translation (NAT) is enabled, enter the IP address that is sent to the controller from the NAT device rather than the controller’s management interface IP address. Otherwise, mobility will fail among controllers in the mobility group.

b. In the Member MAC Address text box, enter the MAC address of the controller to be added.

c. In the Group Name text box, enter the name of the mobility group.

  **Note**  The mobility group name is case sensitive.
d. Click **Apply** to commit your changes. The new controller is added to the list of mobility group members on the Static Mobility Group Members page.

e. Click **Save Configuration** to save your changes.

f. Repeat Step a through Step e to add all of the controllers in the mobility group.

g. Repeat this procedure on every controller to be included in the mobility group. All controllers in the mobility group must be configured with the MAC address and IP address of all other mobility group members.

The Mobility Group Members > Edit All page (see Figure 15-9) lists the MAC address, IP address, and mobility group name (optional) of all the controllers currently in the mobility group. The controllers are listed one per line with the local controller at the top of the list.

**Note** If desired, you can edit or delete any of the controllers in the list.

---

**Figure 15-9** Mobility Group Members > Edit All Page

---

**Step 5** Add more controllers to the mobility group as follows:

a. Click inside the edit box to start a new line.

b. Enter the MAC address, the management interface IP address, and the name of the mobility group for the controller to be added.

**Note** You should enter these values on one line and separate each value with one or two spaces.

**Note** The mobility group name is case sensitive.

c. Repeat Step a and Step b for each additional controller that you want to add to the mobility group.

d. Highlight and copy the complete list of entries in the edit box.

e. Click **Apply** to commit your changes. The new controllers are added to the list of mobility group members on the Static Mobility Group Members page.

f. Click **Save Configuration** to save your changes.

g. Paste the list into the text box on the Mobility Group Members > Edit All page of all the other controllers in the mobility group and click **Apply** and **Save Configuration**.
Step 6  Choose Multicast Messaging to open the Mobility Multicast Messaging page.

![Mobility Multicast Messaging Page](image)

The names of all the currently configured mobility groups appear in the middle of the page.

Step 7  On the Mobility Multicast Messaging page, select the Enable Multicast Messaging check box to enable the controller to use multicast mode to send Mobile Announce messages to the mobility members. If you leave it unselected, the controller uses unicast mode to send the Mobile Announce messages. The default value is unselected.

Step 8  If you enabled multicast messaging in the previous step, enter the multicast group IP address for the local mobility group in the Local Group Multicast IP Address text box. This address is used for multicast mobility messaging.

**Note** In order to use multicast messaging, you must configure the IP address for the local mobility group.

Step 9  Click Apply to commit your changes.

Step 10  If desired, you can also configure the multicast group IP address for nonlocal groups within the mobility list. To do so, click the name of a nonlocal mobility group to open the Mobility Multicast Messaging > Edit page (see Figure 15-11), and enter the multicast group IP address for the nonlocal mobility group in the Multicast IP Address text box.

**Note** If you do not configure the multicast IP address for nonlocal groups, the controller uses unicast mode to send mobility messages to those members.

![Mobility Multicast Messaging > Edit Page](image)

Step 11  Click Apply to commit your changes.

Step 12  Click Save Configuration to save your changes.
Configuring Mobility Groups (CLI)

**Step 1** Check the current mobility settings by entering this command:

```
show mobility summary
```

Information similar to the following appears:

- Symmetric Mobility Tunneling (current) ........... Enabled
- Symmetric Mobility Tunneling (after reboot) ..... Enabled
- Mobility Protocol Port ................................ 16666
- Mobility Security Mode ................................ Disabled
- Default Mobility Domain............................. snmp_gui
- Multicast Mode .......................................... Disabled
- Mobility Domain ID for 802.11r...................... 0x66bd
- Mobility Keepalive Interval......................... 10
- Mobility Keepalive Count............................. 3
- Mobility Group Members Configured............... 3
- Mobility Control Message DSCP Value.............. 0

Controllers configured in the Mobility Group

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>Group Name</th>
<th>Multicast IP</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:85:32:42:c0</td>
<td>1.100.163.24</td>
<td>snmp_gui</td>
<td>0.0.0.0</td>
<td>Up</td>
</tr>
<tr>
<td>00:cc:11:ee:1b:10</td>
<td>10.100.100.1</td>
<td>VoWLAN</td>
<td>0.0.0.0</td>
<td>Control and Data Path Down</td>
</tr>
<tr>
<td>11:22:11:33:11:44</td>
<td>1.2.3.4</td>
<td>test</td>
<td>0.0.0.0</td>
<td>Control and Data Path Down</td>
</tr>
</tbody>
</table>

**Step 2** Create a mobility group by entering this command:

```
config mobility group domain domain_name
```

**Note** Enter up to 31 case-sensitive ASCII characters for the group name. Spaces are not allowed in mobility group names.

**Step 3** Add a group member by entering this command:

```
config mobility group member add mac_address ip_address
```

**Note** If you are configuring the mobility group in a network where network address translation (NAT) is enabled, enter the IP address that is sent to the controller from the NAT device rather than the controller’s management interface IP address. Otherwise, mobility will fail among controllers in the mobility group.

**Note** Enter the `config mobility group member delete mac_address` command if you want to delete a group member.

**Step 4** Enable or disable multicast mobility mode by entering this command:

```
config mobility multicast-mode {enable | disable} local_group_multicast_address
```

Where `local_group_multicast_address` is the multicast group IP address for the local mobility group. This address is used for multicast mobility messaging.

If you enable multicast mobility mode, the controller uses multicast mode to send Mobile Announce messages to the local group. If you disable multicast mobility mode, the controller uses unicast mode to send the Mobile Announce messages to the local group. The default value is disabled.
Step 5  (Optional) You can also configure the multicast group IP address for nonlocal groups within the mobility list. To do so, enter this command:

    config mobility group multicast-address group_name IP_address

If you do not configure the multicast IP address for nonlocal groups, the controller uses unicast mode to send mobility messages to those members.

Step 6  Verify the mobility configuration by entering this command:

    show mobility summary

Step 7  Save your changes by entering this command:

    save config

Step 8  Repeat this procedure on every controller to be included in the mobility group. All controllers in the mobility group must be configured with the MAC address and IP address of all other mobility group members.

Step 9  Enable or disable debugging of multicast usage for mobility messages by entering this command:

    debug mobility multicast {enable | disable}

---

Viewing Mobility Group Statistics

You can view three types of mobility group statistics from the controller GUI:

- Global statistics—Affect all mobility transactions
- Mobility initiator statistics—Generated by the controller initiating a mobility event
- Mobility responder statistics—Generated by the controller responding to a mobility event

You can view mobility group statistics using the controller GUI or CLI.

Viewing Mobility Group Statistics (GUI)

Step 1  Choose Monitor > Statistics > Mobility Statistics to open the Mobility Statistics page.
This page contains the following fields:

- **Group Mobility Statistics**
  - **Rx Errors**—Generic protocol packet receive errors, such as packet too short or format incorrect.
  - **Tx Errors**—Generic protocol packet transmit errors, such as packet transmission fail.
  - **Responses Retransmitted**—Mobility protocol that uses UDP and resends requests several times if it does not receive a response. Because of network or processing delays, the responder may receive one or more retry requests after it initially responds to a request. This text box shows a count of the response resends.
  - **Handoff Requests Received**—Total number of handoff requests received, ignored, or responded to.
  - **Handoff End Requests Received**—Total number of handoff end requests received. These requests are sent by the anchor or foreign controller to notify the other about the close of a client session.

![Mobility Statistics Page](image-url)
- State Transitions Disallowed—Policy enforcement module (PEM) that has denied a client state transition, usually resulting in the handoff being aborted.
- Resource Unavailable—Necessary resource, such as a buffer, was unavailable, resulting in the handoff being aborted.

Mobility Initiator Statistics
- Handoff Requests Sent—Number of clients that have associated to the controller and have been announced to the mobility group.
- Handoff Replies Received—Number of handoff replies that have been received in response to the requests sent.
- Handoff as Local Received—Number of handoffs in which the entire client session has been transferred.
- Handoff as Foreign Received—Number of handoffs in which the client session was anchored elsewhere.
- Handoff Denys Received—Number of handoffs that were denied.
- Anchor Request Sent—Number of anchor requests that were sent for a three-party (foreign-to-foreign) handoff. The handoff was received from another foreign controller, and the new controller is requesting the anchor to move the client.
- Anchor Deny Received—Number of anchor requests that were denied by the current anchor.
- Anchor Grant Received—Number of anchor requests that were approved by the current anchor.
- Anchor Transfer Received—Number of anchor requests that closed the session on the current anchor and transferred the anchor back to the requestor.

Mobility Responder Statistics
- Handoff Requests Ignored—Number of handoff requests or client announcements that were ignored because the controller had no knowledge of that client.
- Ping Pong Handoff Requests Dropped—Number of handoff requests that were denied because the handoff period was too short (3 seconds).
- Handoff Requests Dropped—Number of handoff requests that were dropped due to either an incomplete knowledge of the client or a problem with the packet.
- Handoff Requests Denied—Number of handoff requests that were denied.
- Client Handoff as Local—Number of handoff responses sent while the client is in the local role.
- Client Handoff as Foreign—Number of handoff responses sent while the client is in the foreign role.
- Anchor Requests Received—Number of anchor requests received.
- Anchor Requests Denied—Number of anchor requests denied.
- Anchor Requests Granted—Number of anchor requests granted.
- Anchor Transferred—Number of anchors transferred because the client has moved from a foreign controller to a controller on the same subnet as the current anchor.

Step 2: If you want to clear the current mobility statistics, click Clear Stats.
Viewing Mobility Group Statistics (CLI)

- See mobility group statistics by entering the `show mobility statistics` command.
- To clear the current mobility statistics, enter the `clear stats mobility` command.

Configuring Auto-Anchor Mobility

This section contains the following topics:

- Information About Auto-Anchor Mobility, page 15-19
- Guidelines and Limitations, page 15-20
- Configuring Auto-Anchor Mobility (GUI), page 15-20
- Configuring Auto-Anchor Mobility (CLI), page 15-21

Information About Auto-Anchor Mobility

You can use auto-anchor mobility (also called guest tunneling) to improve load balancing and security for roaming clients on your wireless LANs. Under normal roaming conditions, client devices join a wireless LAN and are anchored to the first controller that they contact. If a client roams to a different subnet, the controller to which the client roamed sets up a foreign session for the client with the anchor controller. However, when you use the auto-anchor mobility feature, you can specify a controller or set of controllers as the anchor points for clients on a wireless LAN.

In auto-anchor mobility mode, a subset of a mobility group is specified as the anchor controllers for a WLAN. You can use this feature to restrict a WLAN to a single subnet, regardless of a client’s entry point into the network. Clients can then access a guest WLAN throughout an enterprise but still be restricted to a specific subnet. Auto-anchor mobility can also provide geographic load balancing because the WLANs can represent a particular section of a building (such as a lobby, a restaurant, and so on), effectively creating a set of home controllers for a WLAN. Instead of being anchored to the first controller that they happen to contact, mobile clients can be anchored to controllers that control access points in a particular vicinity.

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated through a mobility tunnel using EtherIP and sent to the anchor controller, where they are decapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller decapsulates the packets and forwards them to the client.

If multiple controllers are added as mobility anchors for a particular WLAN on a foreign controller, the foreign controller internally sorts the controller by their IP address. The controller with the lowest IP address is the first anchor. For example, a typical ordered list would be 172.16.7.25, 172.16.7.28, 192.168.5.15. If the first client associates to the foreign controller’s anchored WLAN, the client database...
entry is sent to the first anchor controller in the list, the second client is sent to the second controller in
the list, and so on, until the end of the anchor list is reached. The process is repeated starting with the
first anchor controller. If any of the anchor controller is detected to be down, all the clients anchored to
the controller are deauthenticated, and the clients then go through the authentication/anchoring process
again in a round-robin manner with the remaining controller in the anchor list. This functionality is also
extended to regular mobility clients through mobility failover. This feature enables mobility group
members to detect failed members and reroute clients.

Guidelines and Limitations

- In controller software releases prior to 4.1, there is no automatic way of determining if a particular
  controller in a mobility group is unreachable. As a result, the foreign controller may continually
  send all new client requests to a failed anchor controller, and the clients remain connected to this
  failed controller until a session timeout occurs. In controller software release 4.1 or later releases,
  mobility list members can send ping requests to one another to check the data and control paths
  among them to find failed members and reroute clients. You can configure the number and interval
  of ping requests that are sent to each anchor controller. This functionality provides guest N+1
  redundancy for guest tunneling and mobility failover for regular mobility.
- The IPsec and L2TP Layer 3 security policies are unavailable for WLANs that are configured with
  a mobility anchor.
- You must add controllers to the mobility group member list before you can designate them as
  mobility anchors for a WLAN.
- You can configure multiple controllers as mobility anchors for a WLAN.
- You must disable the WLAN before configuring mobility anchors for it.
- Auto-anchor mobility supports web authorization but does not support other Layer 3 security types.
- You must configure the WLANs on both the foreign controller and the anchor controller with
  mobility anchors. On the anchor controller, configure the anchor controller itself as a mobility
  anchor. On the foreign controller, configure the anchor as a mobility anchor.
- Auto-anchor mobility is not supported for use with DHCP option 82.
- When using the guest N+1 redundancy and mobility failover features with a firewall, make sure that
  the following ports are open:
  - UDP 16666 for tunnel control traffic
  - IP Protocol 97 for user data traffic
  - UDP 161 and 162 for SNMP

Configuring Auto-Anchor Mobility (GUI)

| Step 1 | Configure the controller to detect failed anchor controllers within a mobility group as follows:
  a. Choose Controller > Mobility Management > Mobility Anchor Config to open the Mobility
     Anchor Config page.
  b. In the Keep Alive Count text box, enter the number of times a ping request is sent to an anchor
     controller before the anchor is considered to be unreachable. The valid range is 3 to 20, and the
     default value is 3. |
c. In the Keep Alive Interval text box, enter the amount of time (in seconds) between each ping request that is sent to an anchor controller. The valid range is 1 to 30 seconds, and the default value is 10 seconds.

d. In the DSCP Value text box, enter the DSCP value. The default is 0.
e. Click **Apply** to commit your changes.

**Step 2**  
Choose WLANs to open the WLANs page.

**Step 3**  
Click the blue drop-down arrow for the desired WLAN or wired guest LAN and choose **Mobility Anchors**. The Mobility Anchors page appears.

This page lists the controllers that have already been configured as mobility anchors and shows the current state of their data and control paths. Controllers within a mobility group communicate among themselves over a well-known UDP port and exchange data traffic through an Ethernet-over-IP (EoIP) tunnel. They send mpings, which test mobility control packet reachability over the management interface over mobility UDP port 16666 and they send epings, which test the mobility data traffic over the management interface over EoIP port 97. The Control Path text box shows whether mpings have passed (up) or failed (down), and the Data Path text box shows whether epings have passed (up) or failed (down). If the Data or Control Path text box shows “down,” the mobility anchor cannot be reached and is considered failed.

**Step 4**  
Select the IP address of the controller to be designated a mobility anchor in the Switch IP Address (Anchor) drop-down list.

**Step 5**  
Click **Mobility Anchor Create**. The selected controller becomes an anchor for this WLAN or wired guest LAN.

**Note**  
To delete a mobility anchor for a WLAN or wired guest LAN, hover your cursor over the blue drop-down arrow for the anchor and choose **Remove**.

**Step 6**  
Click **Save Configuration** to save your changes.

**Step 7**  
Repeat Step 4 and Step 6 to set any other controllers as mobility anchors for this WLAN or wired guest LAN.

**Step 8**  
Configure the same set of mobility anchors on every controller in the mobility group.

---

**Configuring Auto-Anchor Mobility (CLI)**

- The controller is programmed to always detect failed mobility list members. To change the parameters for the ping exchange between mobility members, enter these commands:

  - `config mobility group keepalive count count`—Specifies the number of times a ping request is sent to a mobility list member before the member is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.
  
  - `config mobility group keepalive interval seconds`—Specifies the amount of time (in seconds) between each ping request sent to a mobility list member. The valid range is 1 to 30 seconds, and the default value is 10 seconds.

- Disable the WLAN or wired guest LAN for which you are configuring mobility anchors by entering this command:

  `config {wlan | guest-lan} disable {wlan_id | guest_lan_id}`
• Create a new mobility anchor for the WLAN or wired guest LAN by entering one of these commands:

  - `config mobility group anchor add {wlan | guest-lan} {wlan_id | guest_lan_id} anchor_controller_ip_address`
  - `config {wlan | guest-lan} mobility anchor add {wlan_id | guest_lan_id} anchor_controller_ip_address`

  **Note** The `wlan_id` or `guest_lan_id` must exist and be disabled, and the `anchor_controller_ip_address` must be a member of the default mobility group.

• Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor.

• Delete a mobility anchor for the WLAN or wired guest LAN by entering one of these commands:

  - `config mobility group anchor delete {wlan | guest-lan} {wlan_id | guest_lan_id} anchor_controller_ip_address`
  - `config {wlan | guest-lan} mobility anchor delete {wlan_id | guest_lan_id} anchor_controller_ip_address`

  **Note** The `wlan_id` or `guest_lan_id` must exist and be disabled.

  **Note** Deleting the last anchor disables the auto-anchor mobility feature and resumes normal mobility for new associations.

• Save your settings by entering this command:

  `save config`

• See a list and status of controllers configured as mobility anchors for a specific WLAN or wired guest LAN by entering this command:

  `show mobility anchor {wlan | guest-lan} {wlan_id | guest_lan_id}`

  **Note** The `wlan_id` and `guest_lan_id` parameters are optional and constrain the list to the anchors in a particular WLAN or guest LAN. To see all of the mobility anchors on your system, enter the `show mobility anchor` command.

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Mobility Anchor Export List</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WLAN ID</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

| **GLAN ID** | **IP Address** | **Status** |
| 1 | 10.20.100.2 | UP |
Validating WLAN Mobility Security Values

Information About WLAN Mobility Security Values

For any anchoring or mobility event, the WLAN security policy values on each controller must match. These values can be validated in the controller debugs. Table 15-3 lists the WLAN mobility security values and their corresponding security policy.

<table>
<thead>
<tr>
<th>Security Hexadecimal Value</th>
<th>Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00000000</td>
<td>Security_None</td>
</tr>
<tr>
<td>0x00000001</td>
<td>Security_WEP</td>
</tr>
<tr>
<td>0x00000002</td>
<td>Security_802_1X</td>
</tr>
<tr>
<td>0x00000004</td>
<td>Security_IPSec*</td>
</tr>
</tbody>
</table>
Table 15-3  WLAN Mobility Security Values (continued)

<table>
<thead>
<tr>
<th>Security Hexadecimal Value</th>
<th>Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00000008</td>
<td>Security_IPSec_Passthrough*</td>
</tr>
<tr>
<td>0x00000010</td>
<td>Security_Web</td>
</tr>
<tr>
<td>0x00000020</td>
<td>Security_PPTP*</td>
</tr>
<tr>
<td>0x00000040</td>
<td>Security_DHCP_Required</td>
</tr>
<tr>
<td>0x00000080</td>
<td>Security_WPA_NotUsed</td>
</tr>
<tr>
<td>0x00000100</td>
<td>Security_Cranite_Passthrough*</td>
</tr>
<tr>
<td>0x00000200</td>
<td>Security_Fortress_Passthrough*</td>
</tr>
<tr>
<td>0x00000400</td>
<td>Security_L2TP_IPSec*</td>
</tr>
<tr>
<td>0x00000800</td>
<td>Security_802_11i_NotUsed</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Controllers running software release 6.0 or later do not support this security policy.</td>
</tr>
<tr>
<td>0x00001000</td>
<td>Security_Web_Passthrough</td>
</tr>
</tbody>
</table>

Using Symmetric Mobility Tunneling

This section contains the following topics:

- Information About Symmetric Mobility Tunneling, page 15-24
- Guidelines and Limitations, page 15-26

Information About Symmetric Mobility Tunneling

In asymmetric tunneling, client traffic to the wired network is routed directly through the foreign controller, as shown in Figure 15-13.
Asymmetric tunneling breaks when an upstream router has reverse path filtering (RPF) enabled. In this case, the client traffic is dropped at the router because the RPF check ensures that the path back to the source address matches the path from which the packet is coming. When symmetric mobility tunneling is enabled, all client traffic is sent to the anchor controller and can then successfully pass the RPF check, as shown in Figure 15-14.

Symmetric mobility tunneling is also useful in the following situations:

- If a firewall installation in the client packet path drops packets because the source IP address does not match the subnet on which the packets are received.
- If the access-point group VLAN on the anchor controller is different than the WLAN interface VLAN on the foreign controller. In this case, client traffic could be sent on an incorrect VLAN during mobility events.
Guidelines and Limitations

- Controller software releases 4.1 through 5.1 support both asymmetric and symmetric mobility tunneling. Controller software release 5.2 or later releases support only symmetric mobility tunneling, which is now always enabled by default.

Verifying Symmetric Mobility Tunneling

This section contains the following topics:

- Verifying Symmetric Mobility Tunneling (GUI), page 15-26
- Verifying if Symmetric Mobility Tunneling is Enabled (CLI), page 15-26

Verifying Symmetric Mobility Tunneling (GUI)

Step 1  Choose Controller > Mobility Management > Mobility Anchor Config to open the Mobility Anchor Config page. The Symmetric Mobility Tunneling Mode text box shows Enabled.

Figure 15-15 Mobility Anchor Config Page

Verifying if Symmetric Mobility Tunneling is Enabled (CLI)

To use the controller CLI to verify that symmetric mobility tunneling is enabled, enter this command:

```
show mobility summary
```

Information similar to the following appears:

```
Symmetric Mobility Tunneling (current) .......... Enabled
Symmetric Mobility Tunneling (after reboot) ..... Enabled
Mobility Protocol Port......................... 16666
Mobility Security Mode......................... Disabled
Default Mobility Domain........................ User1
Mobility Keepalive interval.................... 10
Mobility Keepalive count....................... 3
Mobility Group members configured............. 7
```
Running Mobility Ping Tests

This section contains the following topics:

- Information About Mobility Ping Tests, page 15-27
- Guidelines and Limitations, page 15-27
- Running Mobility Ping Tests (CLI), page 15-28

Information About Mobility Ping Tests

Controllers in a mobility list communicate with each other by controlling information over a well-known UDP port and exchanging data traffic through an Ethernet-over-IP (EoIP) tunnel. Because UDP and EoIP are not reliable transport mechanisms, there is no guarantee that a mobility control packet or data packet will be delivered to a mobility peer. Mobility packets may be lost in transit due to a firewall filtering the UDP port or EoIP packets or due to routing issues.

Guidelines and Limitations

Controller software release 4.0 or later releases enable you to test the mobility communication environment by performing mobility ping tests. These tests may be used to validate connectivity between members of a mobility group (including guest controllers). Two ping tests are available:

- Mobility ping over UDP—This test runs over mobility UDP port 16666. It tests whether the mobility control packet can be reached over the management interface.
- Mobility ping over EoIP—This test runs over EoIP. It tests the mobility data traffic over the management interface.

Only one mobility ping test per controller can be run at a given time.

Note These ping tests are not Internet Control Message Protocol (ICMP) based. The term “ping” is used to indicate an echo request and an echo reply message.

Note Any ICMP packet greater than 1280 bytes will always be responded with a packet that is truncated to 1280 bytes. For example, a ping with a packet that is greater than 1280 bytes from a host to the management interface is always responded with a packet that is truncated to 1280 bytes.
Running Mobility Ping Tests (CLI)

- To test the mobility UDP control packet communication between two controllers, enter this command:
  
  \texttt{mping mobility_peer_IP_address}  
  
  The \texttt{mobility_peer_IP_address} parameter must be the IP address of a controller that belongs to the mobility list.

- To test the mobility EoIP data packet communication between two controllers, enter this command:

  \texttt{eping mobility_peer_IP_address}  
  
  The \texttt{mobility_peer_IP_address} parameter must be the IP address of a controller that belongs to the mobility list.

- To troubleshoot your controller for mobility ping, enter these commands:

  \texttt{config logging buffered debugging}  

  \texttt{show logging}  
  
  To troubleshoot your controller for mobility ping over UDP, enter this command to display the mobility control packet:

  \texttt{debug mobility handoff enable}

\textbf{Note} We recommend using an ethereal trace capture when troubleshooting.

Configuring Dynamic Anchoring for Clients with Static IP Addresses

This section contains the following topics:

- Information About Dynamic Anchoring for Clients with Static IP, page 15-28
- Guidelines and Limitations, page 15-29
- Configuring Dynamic Anchoring of Static IP Clients (GUI), page 15-29
- Configuring Dynamic Anchoring of Static IP Clients (CLI), page 15-30

Information About Dynamic Anchoring for Clients with Static IP

At times you may want to configure static IP addresses for wireless clients. When these wireless clients move about in a network, they could try associating with other controllers. If the clients try to associate with a controller that does not support the same subnet as the static IP, the clients fail to connect to the network. You can now enable dynamic tunneling of clients with static IP addresses.

Dynamic anchoring of static IP clients with static IP addresses can be associated with other controllers where the client’s subnet is supported by tunneling the traffic to another controller in the same mobility group. This feature enables you to configure your WLAN so that the network is serviced even though the clients use static IP addresses.
How Dynamic Anchoring of Static IP Clients Works

The following sequence of steps occur when a client with a static IP address tries to associate with a controller:

1. When a client associates with a controller, for example, WLC-1, it performs a mobility announcement. If a controller in the mobility group responds (for example WLC-2), the client traffic is tunneled to the controller WLC-2. As a result, the controller WLC 1 becomes the foreign controller and WLC-2 becomes the anchor controller.

2. If none of the controllers respond, the client is treated as a local client and authentication is performed. The IP address for the client is updated either through an orphan packet handling or an ARP request processing. If the client's IP subnet is not supported in the controller (WLC-1), WLC-1 sends another static IP mobile announce and if a controller (for example WLC-3) that supports the client's subnet responds to that announcement, the client traffic is tunneled to that controller WLC-3. As a result, the controller WLC 1 becomes the export foreign controller and WLC-3 becomes the export anchor controller.

3. Once the acknowledgement is received, the client traffic is tunneled between the anchor and the controller (WLC-1).

**Note**
If you configure WLAN with an interface group and any of the interfaces in the interface group supports the static IP client subnet, the client is assigned to that interface. This situation occurs in local or remote (static IP Anchor) controller.

**Note**
A security level 2 authentication is performed only in the local (static IP foreign) controller, which is also known as the exported foreign controller.

Guidelines and Limitations

- Do not configure overridden interfaces when you perform AAA for static IP tunneling, this is because traffic can get blocked for the client if the overridden interface does not support the client’s subnet. This can be possible in extreme cases where the overriding interface group supports the client’s subnet.
- The local controller must be configured with the correct AAA server where this client entry is present.

The following restrictions apply when configuring static IP tunneling with other features on the same WLAN:

- Auto anchoring mobility (guest tunneling) cannot be configured for the same WLAN.
- FlexConnect local authentication cannot be configured for the same WLAN.
- The DHCP required option cannot be configured for the same WLAN.
- You cannot configure dynamic anchoring of static IP clients with FlexConnect local switching.

Configuring Dynamic Anchoring of Static IP Clients (GUI)

**Step 1** Choose **WLANs** to open the WLANs page.
Step 2  Click the ID number of the WLAN on which you want to enable dynamic anchoring of IP clients. The WLANs > Edit page is displayed.

Step 3  Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 4  Enable dynamic anchoring of static IP clients by selecting the **Static IP Tunneling** check box.

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

---

### Configuring Dynamic Anchoring of Static IP Clients (CLI)

```
config wlan static-ip tunneling {enable | disable} wlan_id
```

*`wlan_id`*— Enables or disables the dynamic anchoring of static IP clients on a given WLAN.

To monitor and troubleshoot your controller for clients with static IP, use the following commands:

- `show wlan wlan_id`—Enables you to see the status of the static IP clients feature.

```
..................
Static IP client tunneling............... Enabled
 ..................
```

- `debug client client-mac`
- `debug dot11 mobile enable`
- `debug mobility handoff enable`

---

### Configuring Foreign Mappings

This section contains the following topics:

- Information About Foreign Mappings, page 15-30
- Configuring Foreign Controller MAC Mapping (GUI), page 15-30
- Configuring Foreign Controller MAC Mapping (CLI), page 15-31

### Information About Foreign Mappings

Auto-Anchor mobility, also known as Foreign Mapping, allows you to configure users that are on different foreign controllers to obtain IP addresses from a subnet or group of subnets.

### Configuring Foreign Controller MAC Mapping (GUI)

**Step 1**  Choose the WLANs tab to open the WLAN page.

The WLANs page appears listing the available WLANs.

**Step 2**  Click the Blue drop down arrow for the desired WLAN and choose **Foreign-Maps**.

The foreign mappings page appears. This page also lists the MAC addresses of the foreign controllers that are in the mobility group and interfaces/interface groups.
Step 3  Choose the desired foreign controller MAC and the interface or interface group to which it must be mapped and click on Add Mapping.

Configuring Foreign Controller MAC Mapping (CLI)

```
config wlan mobility foreign-map add wlan-id foreign_ctlr_mac interface/interface_grp name
```

To configure a foreign mappings, use this command:

```
config wlan mobility foreign-map add wlan_id interface
```
 CHAPTER 16

Configuring FlexConnect

This chapter describes contains the following sections:

- Information About FlexConnect, page 16-1
- Configuring FlexConnect, page 16-7
- Configuring FlexConnect Groups, page 16-20
- Configuring AAA Overrides for FlexConnect, page 16-28
- Configuring Efficient AP Image Upgrades for FlexConnect Access Points, page 16-30

Information About 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 customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller. In the connected mode, the FlexConnect access point can also perform local authentication.

Figure 16-1 shows a typical FlexConnect deployment.
Information About FlexConnect

This section contains the following topics:

- **FlexConnect Authentication Process, page 16-2**
- **Guidelines and Limitations, page 16-5**

### FlexConnect Authentication Process

When an access point boots up, it looks for a controller. If it finds one, it joins the controller, downloads the latest software image and configuration from the controller, and initializes the radio. It saves the downloaded configuration in nonvolatile memory for use in standalone mode.

---

**Note**

Once the access point is rebooted after downloading the latest controller software, it must be converted to the FlexConnect mode. This can be done using the GUI or CLI.

A FlexConnect access point can learn the controller IP address in one of these ways:

- If the access point has been assigned an IP address from a DHCP server, it can discover a controller through the regular CAPWAP or LWAPP discovery process.

  **Note**

  OTAP is no longer supported on the controllers with 6.0.196 code and above.

- If the access point has been assigned a static IP address, it can discover a controller through any of the discovery process methods except DHCP option 43. If the access point cannot discover a controller through Layer 3 broadcast, we recommend DNS resolution. With DNS, any access point with a static IP address that knows of a DNS server can find at least one controller.

- If you want the access point to discover a controller from a remote network where CAPWAP or LWAPP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the access point CLI) the controller to which the access point is to connect.
For more information about how access points find controllers, see Chapter 9, “Controlling Lightweight Access Points,” or the controller deployment guide at: http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html

When a FlexConnect access point can reach the controller (referred to as the connected mode), the controller assists in client authentication. When a FlexConnect access point cannot access the controller, the access point enters the standalone mode and authenticates clients by itself.

The LEDs on the access point change as the device enters different FlexConnect modes. See the hardware installation guide for your access point for information on LED patterns.

When a client associates to a FlexConnect access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration. With respect to client authentication (open, shared, EAP, web authentication, and NAC) and data packets, the WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

- central authentication, central switching—In this state, the controller handles client authentication, and all client data is tunneled back to the controller. This state is valid only in connected mode.
- central authentication, local switching—In this state, the controller handles client authentication, and the FlexConnect access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the FlexConnect access point to start switching data packets locally. This message is sent per client. This state is applicable only in connected mode.
- local authentication, local switching—In this state, the FlexConnect access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

In connected mode, the access point provides minimal information about the locally authenticated client to the controller. The following information is not available to the controller:

- Policy type
- Access VLAN
- VLAN name
- Supported rates
- Encryption cipher

Local authentication is useful where you cannot maintain a remote office setup of a minimum bandwidth of 128 kbps with the round-trip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local authentication, the authentication capabilities are present in the access point itself. Local authentication reduces the latency requirements of the branch office.

Local authentication can only be enabled on the WLAN of a FlexConnect access point that is in local switching mode.

Notes about local authentication are as follows:

- Guest authentication cannot be done on a FlexConnect local authentication-enabled WLAN.
Information About FlexConnect

- Local RADIUS on the controller is not supported.
- Once the client has been authenticated, roaming is only supported after the controller and the other FlexConnect access points in the group are updated with the client information.
- Local authentication in connected mode requires a WLAN configuration.

Note: When locally switched clients that are connected to a FlexConnect access point renew the IP addresses, on joining back, the client continues to stay in the run state. These clients are not reauthenticated by the controller.

- authentication down, switch down—In this state, the WLAN disassociates existing clients and stops sending beacon and probe requests. This state is valid in both standalone mode and connected mode.
- authentication down, local switching—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

When a FlexConnect access point enters standalone mode, WLANs that are configured for open, shared, WPA-PSK, or WPA2-PSK authentication enter the “local authentication, local switching” state and continue new client authentications. In controller software release 4.2 or later releases, this configuration is also correct for WLANs that are configured for 802.1X, WPA-802.1X, WPA2-802.1X, or CCKM, but these authentication types require that an external RADIUS server be configured. You can also configure a local RADIUS server on a FlexConnect access point to support 802.1X in a standalone mode or with local authentication.

Other WLANs enter either the “authentication down, switching down” state (if the WLAN was configured for central switching) or the “authentication down, local switching” state (if the WLAN was configured for local switching).

When FlexConnect access points are connected to the controller (rather than in standalone mode), the controller uses its primary RADIUS servers and accesses them in the order specified on the RADIUS Authentication Servers page or in the `config radius auth add` CLI command (unless the server order is overridden for a particular WLAN). However, to support 802.1X EAP authentication, FlexConnect access points in standalone mode need to have their own backup RADIUS server to authenticate clients.

Note: A controller does not use a backup RADIUS server. The controller uses the backup RADIUS server in local authentication mode.

You can configure a backup RADIUS server for individual FlexConnect access points in standalone mode by using the controller CLI or for groups of FlexConnect access points in standalone mode by using either the GUI or CLI. A backup server configured for an individual access point overrides the backup RADIUS server configuration for a FlexConnect.

When a FlexConnect access point enters standalone mode, it disassociates all clients that are on centrally switched WLANs. For web-authentication WLANs, existing clients are not disassociated, but the FlexConnect access point stops sending beacons when the number of associated clients reaches zero (0). It also sends disassociation messages to new clients associating to web-authentication WLANs. Controller-dependent activities, such as network access control (NAC) and web authentication (guest access), are disabled, and the access point does not send any intrusion detection system (IDS) reports to the controller. Most radio resource management (RRM) features (such as neighbor discovery; noise, interference, load, and coverage measurements; use of the neighbor list; and rogue containment and detection) are disabled. However, a FlexConnect access point supports dynamic frequency selection in standalone mode.
Chapter 16  Configuring FlexConnect

Information About FlexConnect

Note

- For Wi-Fi Protected Access version 2 (WPA2) in FlexConnect standalone mode or local-auth in connected mode or cckm fast-roaming in connected mode, only Advanced Encryption Standard (AES) is supported.
- For Wi-Fi Protected Access (WPA) in FlexConnect standalone mode or local-auth in connected mode or cckm fast-roaming in connected mode, only Temporal Key Integrity Protocol (TKIP) is supported.
- WPA2 with TKIP and WPA with AES is not supported in standalone mode, local-auth in connected mode, and CCKM fast-roaming in connected mode.

Note

If your controller is configured for NAC, clients can associate only when the access point is in connected mode. When NAC is enabled, you need to create an unhealthy (or quarantined) VLAN so that the data traffic of any client that is assigned to this VLAN passes through the controller, even if the WLAN is configured for local switching. After a client is assigned to a quarantined VLAN, all of its data packets are centrally switched. See the “Configuring Dynamic Interfaces” section on page 4-15 for information on creating quarantined VLANs and the “Configuring NAC Out-of-Band Integration” section on page 8-70 for information on configuring NAC out-of-band support.

Note

Even after configuring WLAN Override to stop transmitting locally switched WLAN on both radios, the WLAN still appears in the H-REAP VLAN mapping configuration on the AP.

When a FlexConnect access point enters into a standalone mode, the following occurs:
- The access point checks whether it is able to reach the default gateway via ARP. If so, it will continue to try and reach the controller.

If the access point fails to establish the ARP, the following occurs:
- The access point attempts to discover for five times and if it still cannot find the controller, it tries to renew the DHCP on the ethernet interface to get a new DHCP IP.
- The access point will retry for five times, and if that fails, the access point will renew the IP address of the interface again, this will happen for three attempts.
- If the three attempts fail, the access point will fall back to the static IP and will reboot (only if the access point is configured with a static IP).
- Reboot is done to remove the possibility of any unknown error the access point configuration.

Once the access point reestablishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and realows client connectivity.

Guidelines and Limitations

- You can deploy a FlexConnect access point with either a static IP address or a DHCP address. In the case of DHCP, a DHCP server must be available locally and must be able to provide the IP address for the access point at bootup.
- FlexConnect supports up to four fragmented packets or a minimum 500-byte maximum transmission unit (MTU) WAN link.
- FlexConnect is supported only on the following access points: Cisco Aironet 1130AG, 1140, 1240, 1250, 1260, AP801, AP802 and Cisco Aironet 600 Series OfficeExtend Access Points.
Information About FlexConnect

- Round-trip latency must not exceed 300 milliseconds (ms) between the access point and the controller, and CAPWAP control packets must be prioritized over all other traffic. In cases where you cannot achieve the 300 milliseconds round-trip latency, you can configure the access point to perform local authentication.

- Starting with the 7.0.116.0 release, the controller software has a more robust fault tolerance methodology to FlexConnect access points. In previous releases, whenever a FlexConnect access point disassociates from a controller, it moves to the standalone mode. The clients that are centrally switched are disassociated. However, the FlexConnect access point continues to serve locally switched clients. When the FlexConnect access point rejoins the controller (or a standby controller), all clients are disconnected and are authenticated again. In the controller software 7.0.116.0 and later releases, this functionality has been enhanced and the connection between the clients and the FlexConnect access points are maintained intact and the clients experience seamless connectivity. This feature can be used only when both the access point and the controller have the same configuration.

- Clients that are centrally authenticated are reauthenticated.

- Client connections are restored only for locally switched clients that are in the RUN state when the access point moves from standalone mode to connected mode. After the access point moves from the standalone mode to the connected mode, the access point’s radio is also reset.

- The configuration on the controller must be the same between the time the access point went into standalone mode and the time the access point came back to connected mode. Similarly, if the access point is falling back to a secondary or backup controller, the configuration between the primary and secondary or backup controller must be the same.

- Session timeout and reauthentication is performed when the access point establishes a connected to the controller.

- After the client connection has been established, the controller does not restore the original attributes of the client. The client username, current rate and supported rates, and listen interval values are reset to the default values only after the session timer expires.

- There is no deployment restriction on the number of FlexConnect access points per location. However, the minimum bandwidth restriction remains 128 kbps with the roundtrip latency no greater than 300 ms and the maximum transmission unit (MTU) no smaller than 500 bytes.

- A newly connected access point cannot be booted in FlexConnect mode.

- The controller can send multicast packets in the form of unicast or multicast packets to the access point. In FlexConnect mode, the access point can receive multicast packets only in unicast form.

- To use CCKM fast roaming with FlexConnect access points, you must configure FlexConnect Groups.

- FlexConnect access points support a 1-1 network address translation (NAT) configuration. They also support port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option. FlexConnect access points 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 access points, 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 access point.
FlexConnect access points support multiple SSIDs. See the “Creating WLANs” section on page 8-3 for more information.

NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching. See the “Configuring NAC Out-of-Band Integration” section on page 8-70 for more information.

The primary and secondary controllers for a FlexConnect access point must have the same configuration. Otherwise, the access point might lose its configuration, and certain features (such as WLAN overrides, VLANs, static channel number, and so on) might not operate correctly. In addition, make sure to duplicate the SSID of the FlexConnect access point and its index number on both controllers.

The QoS profile per-user bandwidth contracts are not supported for FlexConnect locally switched WLANs. The QoS per-user bandwidth contracts are only supported for centrally switched WLANs and APs in the local mode.

Guest user configuration is not supported with FlexConnect local switching.

Do not connect access points in FlexConnect mode directly to a Cisco 2500 Series Controllers.

FlexConnect access points do not support client load balancing.

If you configure a FlexConnect access point with a syslog server configured on the access point, after the access point is reloaded and the native VLAN other than 1, at time of initialization, few syslog packets from the access point are tagged with VLAN ID 1. This is a known issue.

FlexConnect supports IPv6 clients by bridging the traffic to local VLAN, similar to the IPv4 operation. FlexConnect supports client mobility for a group of up to 50 Access Points.

FlexConnect does not support IPv6 ACLs, neighbor discovery caching, and DHCPv6 snooping of IPv6 NDP packets.

FlexConnect does not display any IPv6 client addresses within the client detail page.

FlexConnect Access Points with Locally Switched WLAN cannot perform IP Source Guard and prevent ARP spoofing. For Centrally Switched WLAN, the wireless controller performs the IP Source Guard and ARP Spoofing.

To prevent ARP spoofing attacks in FlexConnect AP with Local Switching, we recommend you to use ARP Inspection.

Configuring FlexConnect

This section contains the following topics:

- Configuring the Switch at the Remote Site, page 16-8
- Configuring the Controller for FlexConnect, page 16-8
- Configuring an Access Point for FlexConnect, page 16-12
- Connecting Client Devices to WLANs, page 16-15

Note: You must perform the procedures in the order listed.
Configuring the Switch at the Remote Site

**Step 1**
Attach the access point that will be enabled for FlexConnect to a trunk or access port on the switch.

*Note* The sample configuration in this procedure shows the FlexConnect access point connected to a trunk port on the switch.

**Step 2**
See the sample configuration in this procedure to configure the switch to support the FlexConnect access point.

In this sample configuration, the FlexConnect access point is connected to trunk interface FastEthernet 1/0/2 with native VLAN 100. The access point needs IP connectivity on the native VLAN. The remote site has local servers/resources on VLAN 101. A DHCP pool is created in the local switch for both VLANs in the switch. The first DHCP pool (NATIVE) is used by the FlexConnect access point, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched. The text in bold below shows these settings.

A sample local switch configuration is as follows:

```plaintext
ip dhcp pool NATIVE
   network 209.165.200.224 255.255.255.224
default-router 209.165.200.225
!
ip dhcp pool LOCAL-SWITCH
   network 209.165.200.224 255.255.255.224
default-router 209.165.200.225
!
interface FastEthernet1/0/1
   description Uplink port
   no switchport
   ip address 209.165.200.228 255.255.255.224
   spanning-tree portfast
!
interface FastEthernet1/0/2
   description the Access Point port
   switchport trunk encapsulation dot1q
   switchport trunk native vlan 100
   switchport trunk allowed vlan 100,101
   switchport mode trunk
   spanning-tree portfast
!
interface Vlan100
   ip address 209.165.200.225 255.255.255.224
   ip helper-address 209.165.201.227
!
interface Vlan101
   ip address 209.165.200.226 255.255.255.229
   ip helper-address 209.165.202.228
end
```

Configuring the Controller for FlexConnect

You can configure the controller for FlexConnect in two environments:

- Centrally switched WLAN
• Locally switched WLAN

Configuring the Controller for FlexConnect (GUI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Choose <strong>WLAN</strong>s to open the WLANs page.</td>
</tr>
<tr>
<td>2.</td>
<td>From the drop-down list, choose <strong>Create New</strong> and click <strong>Go</strong> to open the WLANs &gt; New page.</td>
</tr>
</tbody>
</table>

**Figure 16-2 WLANs > New Page**

- From the Type drop-down list, choose **WLAN**.
- In the Profile Name text box, enter a unique profile name for the WLAN.
- In the WLAN SSID text box, enter a name for the WLAN.
- From the WLAN ID drop-down list, choose the ID number for this WLAN.
- Click **Apply** to commit your changes. The WLANs > Edit page appears.
- You can configure the controller for FlexConnect in both centrally switched and locally switched WLANs:
  - To configure the controller for FlexConnect in a centrally switched WLAN:
    a. In the General tab, choose the **Status** check box to enable the WLAN.
    b. If you have enabled NAC and have created a quarantined VLAN and want to use it for this WLAN, select the interface from the Interface/Interface Group(G) drop-down list in the General tab.
    c. In the Security > Layer 2 tab, choose **WPA+WPA2** from the Layer 2 Security drop-down list and then set the WPA+WPA2 parameters as required.
  - To configure the controller for FlexConnect in a locally switched WLAN:
    a. In the General tab, select the **Status** check box to enable the WLAN.
    b. If you have enabled NAC and have created a quarantined VLAN and want to use it for this WLAN, select the interface from the Interface/Interface Group(G) drop-down list in the General tab.
    c. In the Security > Layer 2 tab, select **WPA+WPA2** from the **Layer 2 Security** drop-down list and then set the WPA+WPA2 parameters as required.
    d. In the Advanced tab, select the **FlexConnect Local Switching** check box to enable local switching for the WLAN.

**Note** When you enable local switching, any FlexConnect access point that advertises this WLAN is able to locally switch data packets (instead of tunneling them to the controller).
When you enable FlexConnect local switching, the controller is enabled to learn the client’s IP address by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client’s IP address, and the controller periodically drops the client. Disable the client IP address learning feature so that the controller maintains the client connection without waiting to learn the client’s IP address. The ability to disable this option is supported only with FlexConnect local switching; it is not supported with FlexConnect central switching.

For FlexConnect access points, the interface mapping at the controller for WLANs that is configured for FlexConnect local switching is inherited at the access point as the default VLAN tagging. This mapping can be changed per SSID and per FlexConnect access point. Non-FlexConnect access points tunnel all traffic back to the controller, and VLAN tagging is determined by each WLAN’s interface mapping.

Example Configuration of Controller for FlexConnect

The controller configuration for FlexConnect consists of creating centrally switched and locally switched WLANs. Table 16-1 shows three WLAN scenarios.

<table>
<thead>
<tr>
<th>WLAN</th>
<th>Security</th>
<th>Authentication</th>
<th>Switching</th>
<th>Interface Mapping (VLAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>employee</td>
<td>WPA1+WPA2</td>
<td>Central</td>
<td>Central</td>
<td>management (centrally switched VLAN)</td>
</tr>
<tr>
<td>employee-local</td>
<td>WPA1+WPA2 (PSK)</td>
<td>Local</td>
<td>Local</td>
<td>101 (locally switched VLAN)</td>
</tr>
<tr>
<td>guest-central</td>
<td>Web authentication</td>
<td>Central</td>
<td>Central</td>
<td>management (centrally switched VLAN)</td>
</tr>
<tr>
<td>employee-local-auth</td>
<td>WPA1+WPA2</td>
<td>Local</td>
<td>Local</td>
<td>101 (locally switched VLAN)</td>
</tr>
</tbody>
</table>

Guest user configuration is not supported with FlexConnect local switching.

Configuring the Controller for FlexConnect—For a Centrally Switched WLAN Used for Guest Access

Before you begin, you must have created guest user accounts. For more information about creating guest user accounts, see Chapter 12, “Managing User Accounts.”

Step 1 Choose WLANs to open the WLANs page.
Step 2 From the drop-down list, choose Create New and click Go to open the WLANs > New page.
Step 3 From the Type drop-down list, choose WLAN.
Step 4 In the Profile Name text box, enter guest-central (as per the example in Table 16-1).
Step 5 In the WLAN SSID text box, enter guest-central.
Step 6 From the WLAN ID drop-down list, choose and ID for the WLAN.
Step 7 Click Apply to commit your changes. The WLANs > Edit page appears.
Step 8 In the General tab, select the Status check box to enable the WLAN.
Step 9 In the Security > Layer 2 tab, choose None from the Layer 2 Security drop-down list.
Step 10 In the Security > Layer 3 tab:
   a. Choose None from the Layer 3 Security drop-down list.
   b. Select the Web Policy check box.
   c. Choose Authentication.

   Note If you are using an external web server, you must configure a preauthentication access
   control list (ACL) on the WLAN for the server and then choose this ACL as the WLAN
   preauthentication ACL on the Layer 3 tab. For more information about ACLs, see Chapter 7,
   “Configuring Security Solutions.”

Step 11 Click Apply to commit your changes.
Step 12 Click Save Configuration to save your changes.

   Note For more information about adding a local user to a WLAN and to customize the content and appearance
   of the login page for guest users when they access the WLAN, follow the instructions in Chapter 7,
   “Configuring Security Solutions.”

Configuring the Controller for FlexConnect (CLI)

- config wlan flexconnect local-switching wlan_id enable—Configures the WLAN for local
  switching.

   Note When you enable FlexConnect local switching, the controller waits to learn the client IP
   address by default. However, if the client is configured with Fortress Layer 2 encryption, the
   controller cannot learn the client IP address, and the controller periodically drops the client.
   Use the config wlan flexconnect learn-ipaddr wlan_id disable command to disable the
   client IP address learning feature so that the controller maintains the client connection
   without waiting to learn the client’s IP address. The ability to disable this feature is
   supported only with FlexConnect local switching; it is not supported with FlexConnect
   central switching. To enable this feature, enter the config wlan flexconnect learn-ipaddr
   wlan_id enable command.

- config wlan flexconnect local-switching wlan_id disable—Configures the WLAN for central
  switching. This is the default value.
Commands Related to Configuring the Controller for FlexConnect

Use these commands to get FlexConnect information:

- `show ap config general Cisco_AP`—Shows VLAN configurations.
- `show wlan wlan_id`—Shows whether the WLAN is locally or centrally switched.
- `show client detail client_mac`—Shows whether the client is locally or centrally switched.

Use these commands to obtain debug information:

- `debug flexconnect aaa {event | error} {enable | disable}`—Enables or disables debugging of FlexConnect backup RADIUS server events or errors.
- `debug flexconnect cckm {enable | disable}`—Enables or disables debugging of FlexConnect CCKM.
- `debug flexconnect {enable | disable}`—Enables or disables debugging of FlexConnect Groups.
- `debug pem state {enable | disable}`—Enables or disables debugging of the policy manager state machine.
- `debug pem events {enable | disable}`—Enables or disables debugging of policy manager events.

Configuring an Access Point for FlexConnect

This section contains the following topics:

- Configuring an Access Point for FlexConnect (GUI), page 16-12
- Configuring an Access Point for FlexConnect (CLI), page 16-13

Configuring an Access Point for FlexConnect (GUI)

Ensure that the access point has been physically added to your network.

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

**Step 2** Click the name of the desired access point. The All APs > Details page appears.

Figure 16-3 All APs Page

**Step 3** Choose FlexConnect from the AP Mode drop-down list to enable FlexConnect for this access point.
Note The last parameter in the Inventory tab indicates whether the access point can be configured for FlexConnect.

Step 4 Click Apply to commit your changes and to cause the access point to reboot.

Step 5 Choose the FlexConnect tab to open the All APs > Details for (FlexConnect) page.

If the access point belongs to a FlexConnect group, the name of the group appears in the FlexConnect Name text box.

Step 6 Select the VLAN Support check box and enter the number of the native VLAN on the remote network (such as 100) in the Native VLAN ID text box.

Note By default, a VLAN is not enabled on the FlexConnect access point. After FlexConnect is enabled, the access point inherits the VLAN ID associated to the WLAN. This configuration is saved in the access point and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per FlexConnect access point in a VLAN-enabled domain. Otherwise, the access point cannot send and receive packets to and from the controller.

Note To preserve the VLAN mappings in the access point after an upgrade or downgrade, it is necessary that the access point join is restricted to the controller for which it is primed. That is, no other discoverable controller with a different configuration should be available by other means. Similarly, at the time the access point joins, if it moves across controllers which have different VLAN mappings, the VLAN mappings at the access point may get mismatched.

Step 7 Click Apply to commit your changes. The access point temporarily loses its connection to the controller while its Ethernet port is reset.

Step 8 Click the name of the same access point and then select the FlexConnect tab.

Step 9 Click VLAN Mappings to open the All APs > Access Point Name > VLAN Mappings page.

Step 10 Enter the number of the VLAN from which the clients will get an IP address when doing local switching (VLAN 101, in this example) in the VLAN ID text box.

Step 11 Click Apply to commit your changes.

Step 12 Click Save Configuration to save your changes.

Note Repeat this procedure for any additional access points that need to be configured for FlexConnect at the remote site.

Configuring an Access Point for FlexConnect (CLI)

- `config ap mode flexconnect Cisco_AP`—Enables FlexConnect for this access point.
- `config ap flexconnect radius auth set {primary | secondary} ip_address auth_port secret Cisco_AP`—Configures a primary or secondary RADIUS server for a specific FlexConnect access point.
Note: Only the Session Timeout RADIUS attribute is supported in standalone mode. All other attributes as well as RADIUS accounting are not supported.

Note: To delete a RADIUS server that is configured for a FlexConnect access point, enter the `config ap flexconnect radius auth delete {primary | secondary} Cisco_AP` command.

- `config ap flexconnect vlan wlan wlan_id vlan-id Cisco_AP`—Enables you to assign a VLAN ID to this FlexConnect access point. By default, the access point inherits the VLAN ID associated to the WLAN.

- `config ap flexconnect vlan {enable | disable} Cisco_AP`—Enables or disables VLAN tagging for this FlexConnect access point. By default, VLAN tagging is not enabled. Once VLAN tagging is enabled on the FlexConnect access point, WLANs enabled for local switching inherit the VLAN assigned at the controller.

- `config ap flexconnect vlan native vlan-id Cisco_AP`—Enables you to configure a native VLAN for this FlexConnect access point. By default, no VLAN is set as the native VLAN. One native VLAN must be configured per FlexConnect access point (when VLAN tagging is enabled). Make sure the switch port to which the access point is connected has a corresponding native VLAN configured as well. If the FlexConnect access point’s native VLAN setting and the upstream switchport native VLAN do not match, the access point cannot transmit packets to and from the controller.

Note: To save the VLAN mappings in the access point after an upgrade or downgrade, you should restrict the access point join is restricted to the controller for which it is primed. No other discoverable controller with a different configuration should be available by other means. Similarly, at the time the access point joins, if it moves across controllers that have different VLAN mappings, the VLAN mappings at the access point might get mismatched.

### Commands Related to Configuring the Access Point for FlexConnect

Use these commands on the FlexConnect access point to get status information:

- `show capwap reap status`—Shows the status of the FlexConnect access point (connected or standalone).

- `show capwap reap association`—Shows the list of clients associated to this access point and their SSIDs.

Use these commands on the FlexConnect access point to get debug information:

- `debug capwap reap`—Shows general FlexConnect activities.

- `debug capwap reap mgmt`—Shows client authentication and association messages.

- `debug capwap reap load`—Shows payload activities, which is useful when the FlexConnect access point boots up in standalone mode.

- `debug dot11 mgmt interface`—Shows 802.11 management interface events.

- `debug dot11 mgmt msg`—Shows 802.11 management messages.

- `debug dot11 mgmt ssid`—Shows SSID management events.

- `debug dot11 mgmt state-machine`—Shows the 802.11 state machine.

- `debug dot11 mgmt station`—Shows client events.
Configuring an Access Point for Local Authentication on a WLAN (GUI)

**Step 1** Choose WLANs to open the WLANs page.

**Step 2** Click the ID of the WLAN. The WLANs > Edit page appears.

**Step 3** Click the Advanced tab to open the WLANs > Edit (WLAN Name) page.

**Step 4** Select the FlexConnect Local Switching check box to enable FlexConnect local switching.

**Step 5** Select the FlexConnect Local Auth check box to enable FlexConnect local authentication.

⚠️ **Caution** Do not connect access points in FlexConnect mode directly to Cisco 2500 Series Controllers.

**Step 6** Click Apply to commit your changes.

Configuring an Access Point for Local Authentication on a WLAN (CLI)

Before you begin, you must have enabled local switching on the WLAN where you want to enable local authentication for an access point. For instructions on how to enable local switching on the WLAN, see the “Configuring the Controller for FlexConnect (CLI)” section on page 16-11.

- `config wlan flexconnect ap-auth wlan_id {enable | disable}`—Configures the access point to enable or disable local authentication on a WLAN.

⚠️ **Caution** Do not connect the access points in FlexConnect mode directly to Cisco 2500 Series Controllers.

- `show wlan wlan-id` — Displays the configuration for the WLAN. If local authentication is enabled, the following information appears:
  
  
  Web Based Authentication...................... Disabled
  Web-Passthrough............................... Disabled
  Conditional Web Redirect..................... Disabled
  Splash-Page Web Redirect..................... Disabled
  Auto Anchor..................................... Disabled
  FlexConnect Local Switching.................. Enabled
  FlexConnect Local Authentication............... Enabled
  FlexConnect Learn IP Address.................. Enabled
  Client MFP...................................... Optional
  Tkip MIC Countermeasure Hold-down Timer...... 60
  Call Snooping.................................... Disabled
  Roamed Call Re-Anchor Policy.................. Disabled
  

Connecting Client Devices to WLANs

Follow the instructions for your client device to create profiles to connect to the WLANs you created in the “Configuring the Controller for FlexConnect” section on page 16-8.
In the example scenarios (see Table 16-1), there are three profiles on the client:

1. To connect to the “employee” WLAN, create a client profile that uses WPA/WPA2 with PEAP-MSCHAPV2 authentication. After the client becomes authenticated, the client gets an IP address from the management VLAN of the controller.

2. To connect to the “local-employee” WLAN, create a client profile that uses WPA/WPA2 authentication. After the client becomes authenticated, the client gets an IP address from VLAN 101 on the local switch.

3. To connect to the “guest-central” WLAN, create a client profile that uses open authentication. After the client becomes authenticated, the client gets an IP address from VLAN 101 on the network local to the access point. After the client connects, the local user can type any http address in the web browser. The user is automatically directed to the controller to complete the web-authentication process. When the web login page appears, the user enters the username and password.

To determine if a client’s data traffic is being locally or centrally switched, choose Monitor > Clients on the controller GUI, click the Detail link for the desired client, and look at the Data Switching parameter under AP Properties.

Configuring FlexConnect ACLs

This section contains the following topics:

- Information About Access Control Lists, page 16-16
- Guidelines and Limitations, page 16-16
- Configuring FlexConnect ACLs, page 16-17

Information About Access Control Lists

An access control list (ACL) is a set of rules that are 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). ACLs enable access control of network traffic. After ACLs are configured on the controller and subsequently pushed to the FlexConnect access point, you can apply them to the access point’s VLAN interface. ACLs enable you to control data traffic to and from wireless clients. You can configure ACLs on the FlexConnect access points to enable effective usage and access control of locally switched data traffic on an access point.

Guidelines and Limitations

- FlexConnect ACLs can only be applied to FlexConnect access points. The configurations applied are per AP, per VLAN.
- The FlexConnect ACLs can be applied to VLAN interfaces on access points in both the Ingress and Egress mode.
- Existing interfaces on an access point can be mapped to ACLs. The interfaces can be created configuring a WLAN-VLAN mapping on the FlexConnect access point.
- The FlexConnect ACLs can be applied to an access point’s VLAN only if VLAN support is enabled on the FlexConnect access point.
- Non-FlexConnect ACLs configured on the controller cannot be applied to a FlexConnect AP.
FlexConnect ACLs do not support direction per rule. Unlike normal ACLs, Flexconnect ACLs cannot be configured with a direction. An ACL as a whole needs to be applied to an interface as Ingress or Egress.

You can define up to 512 FlexConnect ACLs, each with up to 64 rules (or filters). 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.

ACLs in your network might need to be modified if CAPWAP uses different ports than LWAPP.

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 FlexConnect access point.

FlexConnect ACLs cannot be combined with Local mode ACLs on the same WLAN. If ACLs are needed for both FlexConnect and Local mode APs, you can apply two different WLANs to support the use of ACLs in both operating modes (one WLAN for FlexConnect APs and the other WLAN for Local mode APs).

ACLs mapping on the VLANs which are created on the AP using WLAN-VLAN mapping, must be done on a per AP basis only. VLANs can be created on a FlexConnect group for AAA override. These VLANs will not have any mapping for a WLAN. ACLs for VLANs created on the FlexConnect group, must be mapped on the FlexConnect group only. In case the same VLAN is present on the AP as well as the Flexconnect group, AP VLAN will take priority. This means if no ACL is mapped on the AP, the VLAN will not have any ACL, even if the ACL is mapped to the VLAN on the FlexConnect group.

### Configuring FlexConnect ACLs

This section contains the following topics:

- Configuring FlexConnect ACLs (GUI), page 16-17
- Configuring FlexConnect ACLs (CLI), page 16-19
- Viewing and Debugging FlexConnect ACLs (CLI), page 16-20

### Configuring FlexConnect ACLs (GUI)

**Step 1**  
Choose **Security > Access Control Lists > FlexConnect ACLs.**

**Figure 16-4 FlexConnect ACLs Page**

This page lists all FlexConnect ACLs created and configured on the controller. To remove an ACL, hover your mouse over the blue drop-down arrow and choose **Remove.**

**Step 2**  
Add a new ACL by clicking **New.**
The Access Control Lists > New page appears.

**Step 3**
In the Access Control List Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

**Step 4**
Click **Apply**.
When the Access Control Lists page reappears, click the name of the new ACL.

**Step 5**
When the Access Control Lists > Edit page appears, click **Add New Rule**.
The Access Control Lists > Rules > New page appears.

**Step 6**
Configure a rule for this ACL as follows:

a. The controller supports up to 64 rules for each ACL. These rules are listed in order from 1 to 64. In the Sequence text box, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL.

\[
\text{Note} \quad \text{If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number for a rule, the sequence numbers for other rules adjust to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.}
\]

b. From the Source drop-down list, choose one of these options to specify the source of the packets to which this ACL applies:
   - **Any**—Any source (this is the default value).
   - **IP Address**—A specific source. If you choose this option, enter the IP address and netmask of the source in the text boxes.

c. From the Destination drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:
   - **Any**—Any destination (this is the default value).
   - **IP Address**—A specific destination. If you choose this option, enter the IP address and netmask of the destination in the text boxes.

d. From the Protocol drop-down list, choose the protocol ID of the IP packets to be used for this ACL. The protocol options that you can choose are as follows:
   - **Any**—Any protocol (this is the default value)
   - **TCP**—Transmission Control Protocol
   - **UDP**—User Datagram Protocol
   - **ICMP**—Internet Control Message Protocol
   - **ESP**—IP Encapsulating Security Payload
   - **AH**—Authentication Header
   - **GRE**—Generic Routing Encapsulation
   - **IP in IP**—Internet Protocol (IP) in IP (permits or denies IP-in-IP packets)
   - **Eth Over IP**—Ethernet-over-Internet Protocol
   - **OSPF**—Open Shortest Path First
   - **Other**—Any other Internet Assigned Numbers Authority (IANA) protocol
Chapter 16      Configuring FlexConnect

Configuring FlexConnect ACLs

Note

If you choose Other, enter the number of the desired protocol in the Protocol text box. You can find the list of available protocols in the INAI website.

The access point can permit or deny only IP packets in an ACL. Other types of packets (such as ARP packets) cannot be specified.

If you chose TCP or UDP, two additional parameters appear: Source Port and Destination Port. These parameters enable you to choose a specific source port and destination port or port ranges. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications such as Telnet, SSH, HTTP, and so on.

e. From the DSCP drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header text box that can be used to define the quality of service across the Internet.
   • Any—Any DSCP (this is the default value)
   • Specific—A specific DSCP from 0 to 63, which you enter in the DSCP edit box

f. From the Action drop-down list, choose Deny to cause this ACL to block packets or Permit to cause this ACL to allow packets. The default value is Deny.

g. Click Apply to commit your changes. The Access Control Lists > Edit page reappears, showing the rules for this ACL.

h. Repeat this procedure to add any additional rules for this ACL.

Step 7        Click Save Configuration to save your changes.

Configuring FlexConnect ACLs (CLI)

• config flexconnect acl create name—Creates an ACL on a FlexConnect access point. The name must be an IPv4 ACL name of up to 32 characters.

• config flexconnect acl delete name—Deletes a FlexConnect ACL.

• config flexconnect acl rule action acl-name rule-index {permit |deny}—Permits or denies an ACL.

• config flexconnect acl rule add acl-name rule-index—Adds an ACL rule.

• config flexconnect acl rule change index acl-name old-index new-index—Changes the index value for an ACL rule.

• config flexconnect acl rule delete name—Deletes an ACL rule.

• config flexconnect acl rule dscp acl-name rule-index {0-63 | any }—Specifies the differentiated services code point (DSCP) value of this rule index. DSCP is an IP header that can be used to define the quality of service across the Internet. Enter a value between 0 and 63 or ‘any’. The default is ‘any’.

• config flexconnect acl rule protocol acl-name rule-index {0-255 | any }—Assigns the rule index to an ACL rule. Specify a value between 0 and 255 or any. The default is any.

• config flexconnect acl rule destination address acl-name rule-index ipv4-addr subnet-mask—Configures a rule’s destination IP address, netmask and port range.

• config flexconnect acl rule destination port range acl-name rule-index start-port end-port—Configures a rule’s destination port range.
• **config flexconnect acl rule source address acl-name rule-index ipv4-addr subnet-mask**—Configures a rule’s source IP address and netmask.

• **config flexconnect acl rule source port range acl-name rule-index start-port end-port**—Configures a rule’s source port range.

• **config flexconnect acl apply acl-name**—Applies the ACL to the FlexConnect access point.

• **config flexconnect acl rule swap acl-name index-1 index-2**—Swaps the index values of two rules.

• **config ap flexconnect vlan add acl vlan-id ingress-acl-name egress-acl-name ap-name**—Maps an ACL to an existing VLAN configured through WLAN-VLAN mapping.

### Viewing and Debugging FlexConnect ACLs (CLI)

• **show flexconnect acl summary**—Displays a summary of the access control lists.

• **show flexconnect acl detailed acl-name**—Displays the detailed ACL information for the access control list.

• **debug flexconnect acl {enable | disable}**—Enables or disables FlexConnect ACL. Use this command to troubleshoot.

• **debug capwap reap**—Displays the debug messages for the FlexConnect ACLs on a FlexConnect access point.

### Configuring FlexConnect Groups

This section contains the following topics:

• Information About FlexConnect Groups, page 16-20

• Configuring FlexConnect Groups, page 16-22

### Information About FlexConnect Groups

To organize and manage your FlexConnect access points, you can create FlexConnect Groups and assign specific access points to them.

All of the FlexConnect access points in a group share the same backup RADIUS server, CCKM, and local authentication configuration information. This feature is helpful if you have multiple FlexConnect access points in a remote office or on the floor of a building and you want to configure them all at once. For example, you can configure a backup RADIUS server for a FlexConnect rather than having to configure the same server on each access point. Figure 16-5 shows a typical FlexConnect deployment with a backup RADIUS server in the branch office.
FlexConnect Groups and Backup RADIUS Servers

You can configure the controller to allow a FlexConnect access point in standalone mode to perform full 802.1X authentication to a backup RADIUS server. You can configure a primary backup RADIUS server or both a primary and secondary backup RADIUS server. These servers can be used when the FlexConnect access point is in one of these two modes: standalone or connected.

FlexConnect Groups and CCKM

FlexConnect Groups are required for CCKM fast roaming to work with FlexConnect access points. CCKM 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 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 cache for all 100 clients is not practical. If you create a FlexConnect that includes 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 cache is distributed among those four access points only when the clients associate to one of them.

Note

CCKM fast roaming among FlexConnect and non-FlexConnect access points is not supported. See the “Configuring WPA1 +WPA2” section on page 8-26 for information on configuring CCKM.

FlexConnect Groups and Opportunistic Key Caching

Starting in the 7.0.116.0 release, FlexConnect groups enable Opportunistic Key Caching (OKC) to enable fast roaming of clients. OKC facilitates fast roaming by using PMK caching in access points that are in the same FlexConnect group.
This feature prevents the need to perform a full authentication as the client roams from one access point
to another. Whenever a client roams from one FlexConnect access point to another, the FlexConnect
group access point calculates the PMKID using the cached PMK.

To see the PMK cache entries at the FlexConnect access point, use the `show capwap reap pmk`
command. This feature is supported on Cisco FlexConnect access points.

**Note**
The FlexConnect access point must be in connected mode when the PMK is derived during
WPA2/802.1x authentication.

When using FlexConnect groups for OKC or CCKM, the PMK-cache is shared only across the access
points that are part of the same FlexConnect group and are associated to the same controller. If the access
points are in the same FlexConnect group but are associated to different controllers that are part of the
same mobility group, the PMK cache is not updated and CCKM roaming will fail.

**FlexConnect Groups and Local Authentication**

You can configure the controller to allow a FlexConnect access point in standalone mode to perform
LEAP or EAP-FAST authentication for up to 100 statically configured users. The controller sends the
static list of usernames and passwords to each FlexConnect access point when it joins the controller.
Each access point in the group authenticates only its own associated clients.

This feature is ideal for customers who are migrating from an autonomous access point network to a
lightweight FlexConnect access point 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
autonomous access point.

**Note**
This feature can be used with the FlexConnect backup RADIUS server feature. If a FlexConnect is
configured with both a backup RADIUS server and local authentication, the FlexConnect access point
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 FlexConnect access
point itself (if the primary and secondary are not reachable).

The number of FlexConnect groups and access point support depends on the platform that you are using.
You can configure the following:

- Up to 100 FlexConnect groups for a Cisco 5500 Series Controller
- Up to 1000 FlexConnect groups for a Cisco Flex 7500 Series Controller. The Cisco Flex 7500 Series
  Controller can accommodate up to 50 access points per FlexConnect group.
- Up to 20 FlexConnect groups with up to 25 access points per group for the remaining platforms.

**Configuring FlexConnect Groups**

This section contains the following topics:

- Configuring FlexConnect Groups (GUI), page 16-23
- Configuring FlexConnect Groups (CLI), page 16-25
Chapter 16 Configuring FlexConnect

Configuring FlexConnect Groups (GUI)

Step 1 Choose Wireless > FlexConnect Groups to open the FlexConnect Groups page.

![Figure 16-6 FlexConnect Groups Page](image)

This page lists any FlexConnect groups that have already been created.

**Note** If you want to delete an existing group, hover your cursor over the blue drop-down arrow for that group and choose Remove.

Step 2 Click New to create a new FlexConnect Group.

Step 3 On the FlexConnect Groups > New page, enter the name of the new group in the Group Name text box. You can enter up to 32 alphanumeric characters.

Step 4 Click Apply to commit your changes. The new group appears on the FlexConnect Groups page.

Step 5 To edit the properties of a group, click the name of the desired group. The FlexConnect Groups > Edit page appears.

Step 6 If you want to configure a primary RADIUS server for this group (for example, the access points are using 802.1X authentication), choose the desired server from the Primary RADIUS Server drop-down list. Otherwise, leave the text box set to the default value of None.

Step 7 If you want to configure a secondary RADIUS server for this group, choose the server from the Secondary RADIUS Server drop-down list. Otherwise, leave the field set to the default value of None.

Step 8 To add an access point to the group, click Add AP. Additional fields appear on the page under Add AP.

Step 9 Perform one of the following tasks:

- To choose an access point that is connected to this controller, select the Select APs from Current Controller check box and choose the name of the access point from the AP Name drop-down list.

  **Note** If you choose an access point on this controller, the MAC address of the access point is automatically entered in the Ethernet MAC text box to prevent any mismatches from occurring.

- To choose an access point that is connected to a different controller, leave the Select APs from Current Controller check box unselected and enter its MAC address in the Ethernet MAC text box.
If the FlexConnect access points within a group are connected to different controllers, all of the controllers must belong to the same mobility group.

Step 10 Click Add to add the access point to this FlexConnect group. The access point’s MAC address, name, and status appear at the bottom of the page.

Note If you want to delete an access point, hover your cursor over the blue drop-down arrow for that access point and choose Remove.

Step 11 Click Apply to commit your changes.

Step 12 Repeat Step 9 through Step 11 if you want to add more access points to this FlexConnect Group.

Step 13 Enable local authentication for a FlexConnect Group as follows:

a. Ensure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to None.

b. Select the Enable AP Local Authentication check box to enable local authentication for this FlexConnect Group. The default value is unselected.

c. Click Apply to commit your changes.

d. Click the Local Authentication tab to open the FlexConnect > Edit (Local Authentication > Local Users) page.

e. To add clients that you want to be able to authenticate using LEAP or EAP-FAST, perform one of the following:

   • Upload a comma-separated values (CSV) file by selecting the Upload CSV File check box, clicking the Browse button to browse to a CSV file that contains usernames and passwords (each line of the file needs to be in the following format: username, password), and clicking Add to upload the CSV file. The clients’ names appear on the left side of the page under the “User Name” heading.

   • Add clients individually by entering the client’s username in the User Name text box and a password for the client in the Password and Confirm Password text boxes, and clicking Add to add this client to the list of supported local users. The client name appears on the left side of the page under the “User Name” heading.

   Note You can add up to 100 clients.

f. Click Apply to commit your changes.

g. Click the Protocols tab to open the FlexConnect > Edit (Local Authentication > Protocols) page.

h. To allow a FlexConnect access point to authenticate clients using LEAP, select the Enable LEAP Authentication check box and then go to Step i.

i. To allow a FlexConnect access point to authenticate clients using EAP-FAST, select the Enable EAP-FAST Authentication check box and then go to the next step. The default value is unselected.

j. Perform one of the following, depending on how you want protected access credentials (PACs) to be provisioned:

   • To use manual PAC provisioning, enter the server key used to encrypt and decrypt PACs in the Server Key and Confirm Server Key text boxes. The key must be 32 hexadecimal characters.
To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the **Enable Auto Key Generation** check box.

k. In the Authority ID text box, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

l. In the Authority Info text box, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.

m. To specify a PAC timeout value, select the **PAC Timeout** check box and enter the number of seconds for the PAC to remain viable in the text box. The default value is unselected, and the valid range is 2 to 4095 seconds when enabled.

n. Click **Apply** to commit your changes.

**Step 14** Click **Save Configuration** to save your changes.

**Step 15** Repeat this procedure if you want to add more FlexConnects.

---

**Note**

To see if an individual access point belongs to a FlexConnect Group, you can choose **Wireless > Access Points > All APs** > the name of the desired access point in the FlexConnect tab. If the access point belongs to a FlexConnect, the name of the group appears in the FlexConnect Name text box.

---

### Configuring FlexConnect Groups (CLI)

**Step 1** Add or delete a FlexConnect Group by entering this command:

```plaintext
config flexconnect group_name { add | delete }
```

**Step 2** Configure a primary or secondary RADIUS server for the FlexConnect Group by entering this command:

```plaintext
config flexconnect group_name radius server { add | delete } { primary | secondary } server_index
```

**Step 3** Add an access point to the FlexConnect Group by entering this command:

```plaintext
config flexconnect group_name ap { add | delete } ap_mac
```

**Step 4** Configure local authentication for a FlexConnect group as follows:

a. Make sure that a primary and secondary RADIUS server are not configured for the FlexConnect Group.

b. To enable or disable local authentication for this FlexConnect group, enter this command:

```plaintext
config flexconnect group_name radius ap { enable | disable }
```

c. To enter the username and password of a client that you want to be able to authenticate using LEAP or EAP-FAST, enter this command:

```plaintext
config flexconnect group_name radius ap user add username password password
```

**Note** You can add up to 100 clients.

d. To allow a FlexConnect access point to authenticate clients using LEAP or to disable this behavior, enter this command:

```plaintext
config flexconnect group_name radius ap leap { enable | disable }
```
e. To allow a FlexConnect access point to authenticate clients using EAP-FAST or to disable this behavior, enter this command:

```
config flexconnect group_name radius ap eap-fast { enable | disable }
```

e. Enter one of the following commands, depending on how you want PACs to be provisioned:

- **config flexconnect group_name radius ap server-key key**—Specifies the server key used to encrypt and decrypt PACs. The key must be 32 hexadecimal characters.
- **config flexconnect group_name radius ap server-key auto**—Allows PACs to be sent automatically to clients that do not have one during PAC provisioning.

g. To specify the authority identifier of the EAP-FAST server, enter this command:

```
config flexconnect group_name radius ap authority id id
```

where *id* is 32 hexadecimal characters.

h. To specify the authority identifier of the EAP-FAST server in text format, enter this command:

```
config flexconnect group_name radius ap authority info info
```

where *info* is up to 32 hexadecimal characters.

i. To specify the number of seconds for the PAC to remain viable, enter this command:

```
config flexconnect group_name radius ap pac-timeout timeout
```

where *timeout* is a value between 2 and 4095 seconds (inclusive) or 0. A value of 0, which is the default value, disables the PAC timeout.

---

**Step 5**

Save your changes by entering this command:

```
save config
```

**Step 6**

See the current list of FlexConnect Groups by entering this command:

```
show flexconnect summary
```

Information similar to the following appears:

```
flexconnect Summary: Count 2
```

```
Group Name # Aps
Group 1 1
Group 2 1
```

**Step 7**

See the details for a specific FlexConnect Groups by entering this command:

```
show flexconnect group detail group_name
```

Information similar to the following appears:

```
Number of Ap's in Group: 3

00:1d:45:12:f2:24  AP1240.EW3.f224  Joined
00:1d:45:12:f7:12  AP1240.10.f712  Joined
00:1d:a1:ed:9f:84  AP1131.23.9f84  Joined

Group Radius Servers Settings:
Primary Server Index......................... Disabled
Secondary Server Index..................... Disabled

Group Radius AP Settings:
AP RADIUS server.................... Enabled
EAP-FAST Auth......................... Enabled
LEAP Auth......................... Enabled
Server Key Auto Generated... No
```
Server Key: <hidden>
Authority ID: 436973636f0000000000000000000000
Authority Info: Cisco A_ID
PAC Timeout: 0
Number of Users in Group: 20

1cisco        2cisco
3cisco        4cisco
cisco         test1
test10        test11
test12        test13
test14        test15
test2         test3
test4         test5
test6         test7
test8         test9

Configuring VLAN-ACL Mapping on FlexConnect Groups (GUI)

Step 1 Choose Wireless > FlexConnect Groups.
The FlexConnect Groups page appears. This page lists the access points associated with the controller.

Step 2 Click the Group Name link of the FlexConnect Group for which you want to configure VLAN-ACL mapping.

Step 3 Click the VLAN-ACL Mapping tab.
The VLAN-ACL Mapping page for that FlexConnect group is displayed.

Step 4 Enter the Native VLAN ID in the VLAN ID text box.

Step 5 From the Ingress ACL drop-down list, choose the Ingress ACL.

Step 6 From the Egress ACL drop-down list, choose the Egress ACL.

Step 7 Click Add to add this mapping to the FlexConnect Group.
The VLAN ID is mapped with the required ACLs. To remove the mapping, hover your mouse over the blue drop-down arrow and choose Remove.

Configuring VLAN-ACL Mapping on FlexConnect Groups (CLI)

- config flexconnect group group-name vlan add vlan-id acl ingress-acl egress-acl—Adds a VLAN to a FlexConnect group and maps the ingress and egress ACLs.

Viewing VLAN-ACL Mappings (CLI)

- show flexconnect group detail group-name—Displays the FlexConnect group details.
- show ap config general ap-name—Displays the VLAN-ACL mappings on the access point. An output similar to the following is displayed:
  ..
  
  FlexConnect Vlan mode: Enabled
Configuring AAA Overrides for FlexConnect

This section contains the following topics:

- Information About AAA Overrides, page 16-28
- Guidelines and Limitations, page 16-29
- Configuring AAA Override for FlexConnect on an Access Point (GUI), page 16-29
- Configuring VLAN Overrides for FlexConnect on an Access Point (CLI), page 16-30

Information About AAA Overrides

The Allow AAA Override option of a WLAN enables you to configure the WLAN for authentication. It enables you to apply VLAN tagging to individual clients based on the returned RADIUS attribute from the AAA server.

AAA overrides for FlexConnect access points introduce a dynamic VLAN assignment for locally switched clients. AAA overrides for FlexConnect also supports fast roaming (OKC/CCKM) of overridden clients.

- The VLAN with least priority—Specifies the least priority VLANs from the list of VLANs added to the access point using the WLAN-VLAN mapping. If the a VLAN is added and if it exceeds the maximum allowed VLANs (16) on the AP, the VLAN specified in this section is replaced.

- FlexConnect VLAN ACL Mappings—Refers to the configuration of VLANs done using WLAN-VLAN mappings on a per-AP basis using the `config ap flexconnect vlan add` command.

- Group VLAN ACL Mappings—Refers to the configuration of VLAN and the corresponding Ingress and Egress ACLs on a FlexConnect group that is pushed to the access point using the `config flexconnect group group-name vlan add` command.
Guidelines and Limitations

- VLAN overrides for FlexConnect is applicable for both centrally and locally authenticated clients.
- Before configuring an AAA override, the VLAN must be created on the access points. These VLANs can be created on the access points by using the existing WLAN-VLAN mappings.
- VLANs can be configured on FlexConnect groups. VLANs are pushed to the access points belonging to the FlexConnect group.
- At any given point, an AP has a maximum of 16 VLANs. The VLANs are selected based on the WLAN-VLAN mapping in the AP. The remaining VLANs will be pushed from the FlexConnect group in the order that they are configured/shown in the Flexconnect group. If the VLAN slots are full, an error message is logged.
- If the VLAN on the AP is configured using the WLAN-VLAN, the AP configuration of the ACL is applied.
- If the VLAN is configured using the FlexConnect group, the ACL configured on the FlexConnect group is applied.
- If the same VLAN is configured on the FlexConnect group and also at the AP, the AP configuration with its ACL takes precedence.
- If there is no slot for a new VLAN from the WLAN-VLAN mapping, the latest FlexConnect group VLAN is replaced.
- If the VLAN that was returned from the AAA is not present on the AP, the client falls back to the default VLAN configured for the WLAN.
- AAA for locally switched clients only supports VLAN overrides.
- AAA Override for FlexConnect is supported through IETF parameters in the ACS. The following parameters must be configured with the specified values as defined below for a user:
  - [064] Tunnel-Type : Tag 1 value VLAN
  - [065] Tunnel-Medium Type : Tag1 value 802
  - [081] Tunnel-Private-Group-ID : Tag1 value : Overridden VLAN ID.
- Dynamic VLAN assignment is not supported for web authentication from a controller with ACS.

Note

To know more about how to configure IETF parameters, refer to the documentation of ACS server you are using.

Configuring AAA Override for FlexConnect on an Access Point (GUI)

Step 1 Choose Wireless > All APs.

The All APs appears. This page lists the access points associated with the controller.

Step 2 Click the AP name link of the access point for which you want to configure VLAN Override.

Step 3 Click the FlexConnect tab.

Step 4 Enter the Native VLAN ID.

Step 5 Click the VLAN Mappings button to configure the AP VLANs mappings. This page displays the following parameters:
• AP Name—The access point name.
• Base Radio MAC—The base radio of the AP.
• WLAN-SSID-VLAN ID Mappings—For each WLAN configured on the controller, the corresponding SSID and VLAN IDs are listed. Change the WLAN-VLAN ID mappings by editing the VLAN ID column for a WLAN.
• Centrally Switched WLANs—If centrally switched WLANs are configured, the WLAN–VLAN mapping is listed.
• AP Level VLAN ACL Mapping—Change the ingress ACL and egress ACL mappings by choosing the mappings from the drop-down list for each ACL type. The following parameters are available:
  - VLAN ID—The VLAN ID.
  - Ingress ACL—The ingress ACL that corresponds to the VLAN.
  - Egress ACL—The egress ACL that corresponds to the VLAN.
• Group Level VLAN ACL Mappings—The following group level VLAN ACL mapping parameters are available:
  - VLAN ID—The VLAN ID.
  - Ingress ACL—The ingress ACL for this VLAN.
  - Egress ACL—The egress ACL for this VLAN.

Step 6  Click Apply.

---

**Configuring VLAN Overrides for FlexConnect on an Access Point (CLI)**

**Step 1**  Add a VLAN to a FlexConnect group and map the ingress and egress ACLs:

```
config flexconnect group group-name vlan add vlan-id acl ingress-acl egress-acl
```

**Note**  Use the `none` keyword in place of ‘ingress-acl’ or ‘egress-acl’ If you do not want to set a value to the ACL You can also use the `none` keyword to clear the ACL.

**Step 2**  Enable AAA override on the WLAN using the following command:

```
config wlan aaa-override enable wlan_id
```

---

**Configuring Efficient AP Image Upgrades for FlexConnect Access Points**

This section contains the following topics:

• Information About Efficient AP Image Upgrades, page 16-31
• Guidelines and Limitations, page 16-31
• Configuring Efficient AP Image Upgrades on FlexConnect APs (GUI), page 16-31
Information About Efficient AP Image Upgrades

Normally, when upgrading the image of an AP, you can use the preimage download feature to reduce the amount of time that the AP is unavailable to serve clients. However, it also increases the downtime because the access point cannot serve clients during an upgrade. The preimage download feature can be used to reduce this downtime. However, in the case of a branch office setup, the upgrade images are still downloaded to each access point over the WAN link, which has a higher latency.

A more efficient way is to use the Efficient AP Image Upgrade feature. When the Efficient Image Upgrade feature is enabled, one access point of each model in the local network first downloads the upgrade image over the WAN link. The process is similar to the master-slave or client-server model. This access point then becomes the master for the remaining access point of the similar model. The remaining access points then download the upgrade image from the master access point using the preimage download feature over the local network, which reduces the WAN latency.

Guidelines and Limitations

- The primary and secondary controllers in the network must have the same set of primary and backup images.
- If you configured a FlexConnect group, all access points in that group must be within the same subnet or must be accessible through NAT.

Configuring Efficient AP Image Upgrades on FlexConnect APs (GUI)

Step 1  Choose Wireless > FlexConnect Groups.

The FlexConnect Groups page appears. This page lists the FlexConnect Groups configured on the controller.

Step 2  Click the Group Name link on which you want to configure the image upgrade.

Step 3  Click the Image Upgrade tab.

Step 4  Select the FlexConnect AP Upgrade check box to enable efficient FlexConnect AP Upgrade.

Step 5  If you enabled FlexConnect AP Upgrade in the previous step, you must enable the following parameters:

- **Slave Maximum Retry Count**—The number of attempts that the slave access point must try to connect to the master access point for downloading the upgrade image. If the image download does not occur for the configured retry attempts, the image is upgraded over the WAN.
- **Upgrade Image**—Upgrade image that you can choose. The options are Primary and Backup, and Abort.

Step 6  Click FlexConnect Upgrade to upgrade.

Step 7  You can manually assign master access points in the FlexConnect group by selecting the access points from the AP Name drop-down list. Click Add Master to add the master access point.

Step 8  Click Apply.
Chapter 16      Configuring FlexConnect

Configuring Efficient AP Image Upgrades (CLI)

- `config flexconnect group group-name predownload {enable | disable}`—Enables or disables the efficient AP upgrade image.
- `config flexconnect group group-name predownload master ap-name`—Manually assigns an access point as the master access point.
- `config flexconnect group group-name predownload slave retry-count ap-name`—Sets the access point as a slave access point with a retry count.
- `config flexconnect group group-name predownload start`—Initiates the image download on the access points in the FlexConnect group.
- `config ap image predownload {abort | primary | backup}`—Assigns the image type that must be downloaded for the preimage upgrade.
- `show flexconnect group group-name`—Displays the summary of the FlexConnect group configuration.
- `show ap image all`—Displays the details of the images on the access point.
Configuring Mobile Concierge

This chapter contains the following sections:

- Information About 802.11u, page 17-1
- Information About Hotspot 2.0, page 17-10

Information About 802.11u

Mobile Concierge is a solution that enables 802.1X capable clients to interwork with external networks. The Mobile Concierge feature provides service availability information to clients and can help them to connect available networks.

The services offered by the network can be classified into two protocols:

- 802.11u MSAP
- 802.11u Hotspot 2.0

Guidelines and Limitations

- Mobile Concierge is not supported on FlexConnect access points.
- 802.11u configuration upload is not supported. If you perform a configuration upgrade and upload a configuration on the controller, the Hotspot configuration on the WLANs will be lost.

Configuring 802.11u

This section contains the following topics:

- Configuring 802.11u (GUI), page 17-2
- Configuring 802.11u (CLI), page 17-3
- Configuring Venue Details on Access Points (GUI), page 17-6
- Configuring Venue Details on Access Points (CLI), page 17-7
Configuring 802.11u (GUI)

Step 1  Choose WLAN to open the WLANs page.

Step 2  Hover your mouse over the blue drop-down arrow for the desired WLAN on which you want to configure the 802.11u parameters and choose 802.11u. The 802.11u page appears.

Step 3  Select the 802.11u Status check box to enable 802.11u on the WLAN.

Step 4  Select the Internet Access check box to enable this WLAN to provide Internet services.

Step 5  From the Network Type drop-down list, choose the network type that best describes the 802.11u you want to configure on this WLAN:
- Private Network
- Private Network with Guest Access
- Chargeable Public Network
- Free Public Network
- Emergency Services Only Network
- Personal Device Network
- Test or Experimental
- Wildcard

Step 6  Choose the authentication type that you want to configure for the 802.11u parameters on this network.
- Not configured
- Acceptance of Terms and Conditions
- Online Enrollment
- HTTP/HTTPS Redirection

Step 7  In the HESSID field, enter the HESSID (Homogenous Extended Service Set Identifier) value. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.

Step 8  In the OUI List section, enter the following details:
• OUI name
• Is Beacon
• OUI Index

Click Add to add the OUI (Organizationally Unique Identifier) entry to this WLAN. To remove this entry, hover your mouse pointer over the blue drop-down image and choose Remove.

**Step 9**
In the Domain List section, enter the following details:
• Domain Name—Domain name operating in the 802.11 access network.
• Domain Index—Domain index from the drop-down list.

Click Add to add the domain entry to this WLAN. To remove this entry, hover your mouse pointer over the blue drop-down image and choose Remove.

**Step 10**
In the Realm List section, enter the Realms on this network:
• Realm Name—The realm name.
• Realm Index—The realm index.

Click Add to add the realm name and index to this WLAN. To remove this entry, hover your mouse pointer over the blue drop-down image and choose Remove.

**Step 11**
In the Cellular Network Information list, enter the following:
• Country Code
• Cellular Index
• Network Code

Click Add to add the country network information to this WLAN. To remove this entry, hover your mouse pointer over the blue drop-down image and choose Remove.

**Step 12**
Click Apply.

---

### Configuring 802.11u (CLI)

- **config wlan mobile-concierge dot11u {enable | disable}**—Enables or disables the mobile concierge feature.
- **config wlan mobile-concierge dot11u 3gpp-info {add | delete}**—Adds or deletes a 3GPP cellular network information.
- **config wlan mobile-concierge dot11u domain {add | delete | modify}**—Configures the domain for the entity operating in the 802.11u network.
- **config wlan mobile-concierge dot11u hessid hessid wlan-id**—Assigns a HESSID to a WLAN ID. The HESSID must be a valid MAC address.
- **config wlan mobile-concierge dot11u ip-addr-type add ipv4type-id ipv6type-id wlanid**—Configures the IP address availability type for the IPv4 and IPv6 IP addresses on the WLAN.

- **ipv4type-id** can have one of the following values:
  - 0—IPv4 address not available.
  - 1—Public IPv4 address available.
  - 2—Port-restricted IPv4 address available.
- 3—Single NAT configured private IPv4 address available.
- 4—Double NAT configured private IPv4 address available.
- 5—Port-restricted IPv4 address and single NAT configured IPv4 address available.
- 6—Port-restricted IPv4 address and double NAT configured IPv4 address available.
- 7—Availability of the IPv4 address is not known.

`ipv6type-id` can have one of the following values:
- 0—IPv6 address is not available.
- 1—IPv6 address available.
- 2—Availability of the IPv6 address is not known.

- `config wlan mobile-concierge dot11u ip-addr-type delete wlan-id`—Deletes the IP address type availability on a WLAN.
- `config wlan mobile-concierge dot11u net-auth-type network-auth-type`—Configures the network authentication type.

`network-auth-type` can have one of the following values:
- 0—Acceptance of terms and conditions
- 1—Online enrollment
- 2—HTTP/HTTPS redirection

- `config wlan mobile-concierge dot11u oui {add | modify} wlan-id oui-index oui is-beacon`—Configures the Organizationally Unique Identifier (OUI) for a WLAN. The values are as follows:
  - `wlanid`—The WLAN ID.
  - `oui-index`—The OUI index. The OUI index can contain a value between 1 and 32.
  - `oui`—The OUI identifier of vendor. The OUI must be a valid 6-digit number.
  - `is-beacon`—Beacon information. This field can have a value of 0 (disable) or 1 (enable).

- `config wlan mobile-concierge dot11u oui delete wlan-id oui-index`—Deletes the OUI from the WLAN.

- `config wlan mobile-concierge dot11u params wlan-id network-type internet-bit`—Configures the 802.11u parameters on a WLAN. `wlan-id` is the WLAN ID and the `network-type` field can have one of the following values:
  - 0—Private Network
  - 1—Private Network with Guest Access
  - 2—Chargeable Public Network
  - 3—Free Public Network
  - 4—Personal Device Network
  - 5—Emergency Services Only Network
  - 14—Test or Experimental
  - 15—Wildcard

`internet-bit` field specifies the availability of the Internet. This field can have one of the following values:
- 0—Non-availability of internet.
- 1—Internet Available.

- **config wlan mobile-concierge dot11u realm** \{add | modify\} **auth-method** wlan-id realm-index eap-index auth-index auth-method auth-parameter—Adds or modifies an auth-method realm in a WLAN.
  
  - wlan-id—The WLAN ID of the WLAN on which you want to configure this realm.
  
  - realm-index—The realm index. The range is from 1 to 32.
  
  - eap-index—The EAP index. The range is from 1 to 4.
  
  - auth-index—The authentication index value. The range is from 1 to 10.
  
  - auth-method—The authentication method to be used. The range is 1 to 4. See **Table 17-1**.
  
  - auth-parameter—This value depends on the auth-method used.

- **config wlan mobile-concierge dot11u realm** \{add | modify\} **eap-method** wlan-id realm-index eap-index eap-method—Adds an EAP method for a realm in a WLAN.
  
  - wlan-id—The WLAN ID of the WLAN on which you want to configure this realm.
  
  - realm-index—The realm-index. The range is 1 to 32.
  
  - eap-index—The EAP index. The range is 1 to 4.
  
  - eap-method—The EAP method. The range is 0 to 7. See **Table 17-2**.

- **config wlan mobile-concierge dot11u realm** \{add | modify\} **realm-name** wlan-id realm-index realm—Adds or modifies the realm parameters for 802.11u on a WLAN.

**Table 17-1  Authentication Method Mappings**

<table>
<thead>
<tr>
<th>Auth Method</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-EAP Inner Method</td>
<td>1</td>
</tr>
<tr>
<td>Inner Auth Method</td>
<td>2</td>
</tr>
<tr>
<td>Credential Type</td>
<td>3</td>
</tr>
<tr>
<td>Tunneled EAP Method Cred Type</td>
<td>4</td>
</tr>
</tbody>
</table>

**Table 17-2  EAP Method Mappings**

<table>
<thead>
<tr>
<th>EAP Method</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Applicable.</td>
<td>0</td>
</tr>
<tr>
<td>LEAP</td>
<td>1</td>
</tr>
<tr>
<td>PEAP</td>
<td>2</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>3</td>
</tr>
<tr>
<td>EAP-FAST</td>
<td>4</td>
</tr>
<tr>
<td>EAP-SIM</td>
<td>5</td>
</tr>
<tr>
<td>EAP-TTLS</td>
<td>6</td>
</tr>
<tr>
<td>EAP-AKA</td>
<td>7</td>
</tr>
</tbody>
</table>
Configuring Venue Details on Access Points (GUI)

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

**Step 2**  Click the AP Name link to configure the Hotspot parameters on the desired access point. The AP Details page appears.

**Figure 17-2**  AP Configuration Parameters for Hotspot

**Step 3**  Under the General Tab, configure the following parameters:

- Venue Group—The venue category that this access point belongs to. The following options are available:
  - Unspecified
  - Assembly
  - Business
  - Educational
  - Factory and Industrial
  - Institutional
  - Mercantile
  - Residential
  - Storage
  - Utility and Misc
  - Vehicular
  - Outdoor

- Venue Type—Depending on the venue category selected above, the venue type drop-down list displays options for the venue type.

- Venue Name—Venue name that you can provide to the access point. This name is associated with the BSS. This name is used in cases where the SSID does not provide enough information about the venue.
• Language—Language used. An ISO-14962-1997 encoded string defining the language. This is a three character language code. Enter the first three letters of the language in English (For example: eng for English).

Step 4 Click Apply.

Configuring Venue Details on Access Points (CLI)

• **config ap venue add** *venue-name* *venue-group* *venue-type* *lang-code* *ap-name*—Adds the venue details to the access point indicating support for Hotspot2. The values are as follows:
  where:
  - *venue-name*—The name of the venue where this access point is located.
  - *venue-group*—The category of the venue. See Table 17-3.
  - *venue-type*—The type of the venue. Depending on the venue-group chosen, choose the venue type. See Table 17-3.
  - *lang-code*—The language used. An ISO-14962-1997 encoded string defining the language. This is a three character language code. Enter the first three letters of the language in English (for example, eng for English)
  - *ap-name*—The access point name.

Tip Press the **tab** key after entering a keyword or argument to get a list of valid values for the command.

• **config ap venue delete** *ap-name*—Deletes the venue related information from the access point.
### Table 17-3 Venue Group Mapping

<table>
<thead>
<tr>
<th>Venue Group Name</th>
<th>Value</th>
<th>Venue Type for Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNSPECIFIED</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
| ASSEMBLY         | 1     | 0—UNSPECIFIED ASSEMBLY  
|                  |       | 1—ARENA               
|                  |       | 2—STADIUM              
|                  |       | 3—PASSENGER TERMINAL  
|                  |       | (E.G., AIRPORT, BUS, FERRY,  
|                  |       | TRAIN STATION)         
|                  |       | 4—AMPITHEATER          
|                  |       | 5—AMUSEMENT PARK       
|                  |       | 6—PLACE OF WORSHIP     
|                  |       | 7—CONVENTION CENTER    
|                  |       | 8—LIBRARY              
|                  |       | 9—MUSEUM               
|                  |       | 10—RESTAURANT          
|                  |       | 11—THEATER             
|                  |       | 12—BAR                 
|                  |       | 13—COFFEE SHOP         
|                  |       | 14—ZOO OR AQUARIUM     
|                  |       | 15—EMERGENCY           
|                  |       | COORDINATION CENTER    |
| BUSINESS         | 2     | 0—UNSPECIFIED BUSINESS  
|                  |       | 1—DOCTOR OR DENTIST OFFICE  
|                  |       | 2—BANK                 
|                  |       | 3—FIRE STATION          
|                  |       | 4—POLICE STATION        
|                  |       | 6—POST OFFICE           
|                  |       | 7—PROFESSIONAL OFFICE   
|                  |       | 8—RESEARCH AND          
|                  |       | DEVELOPMENT FACILITY    
<p>|                  |       | 9—ATTORNEY OFFICE       |</p>
<table>
<thead>
<tr>
<th>Venue Group Name</th>
<th>Value</th>
<th>Venue Type for Group</th>
</tr>
</thead>
</table>
| EDUCATIONAL            | 3     | • 0—UNSPECIFIED EDUCATIONAL  
|                        |       | • 1—SCHOOL, PRIMARY  
|                        |       | • 2—SCHOOL, SECONDARY  
|                        |       | • 3—UNIVERSITY OR COLLEGE  |
| FACTORY-INDUSTRIAL     | 4     | • 0—UNSPECIFIED FACTORY AND INDUSTRIAL  
|                        |       | • 1—FACTORY  |
| INSTITUTIONAL          | 5     | • 0—UNSPECIFIED INSTITUTIONAL  
|                        |       | • 1—HOSPITAL  
|                        |       | • 2—LONG-TERM CARE FACILITY (E.G., NURSING HOME, HOSPICE, ETC.)  
|                        |       | • 3—ALCOHOL AND DRUG RE-HABILITATION CENTER  
|                        |       | • 4—GROUP HOME  
|                        |       | • 5—PRISON OR JAIL  |
| MERCANTILE             | 6     | • 0—UNSPECIFIED MERCANTILE  
|                        |       | • 1—RETAIL STORE  
|                        |       | • 2—GROCERY MARKET  
|                        |       | • 3—AUTOMOTIVE SERVICE STATION  
|                        |       | • 4—SHOPPING MALL  
|                        |       | • 5—GAS STATION  |
| RESIDENTIAL            | 7     | • 0—UNSPECIFIED RESIDENTIAL  
|                        |       | • 1—PRIVATE RESIDENCE  
|                        |       | • 2—HOTEL OR MOTEL  
|                        |       | • 3—DORMITORY  
|                        |       | • 4—BOARDING HOUSE  |
| STORAGE                | 8     | UNSPECIFIED STORAGE  |
Information About Hotspot 2.0

This feature enables IEEE 802.11 devices to interwork with external networks. This feature is found in hotspots or other public networks irrespective of whether the service is subscription based or free.

The interworking service helps network discovery and selection, enabling information transfer from external networks. It provides information to the stations about the networks prior to association. Interworking will not only help users within home, enterprise, and public access, but also assist manufacturers and operators to provide common components and services for IEEE 802.11 customers. These services are configured on a per WLAN basis on the controller.

Configuring Hotspot 2.0

This section contains the following topics:

- Configuring Hotspot 2.0 (GUI), page 17-11
- Configuring Hotspot 2.0 (CLI), page 17-12

<table>
<thead>
<tr>
<th>Venue Group Name</th>
<th>Value</th>
<th>Venue Type for Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTILITY-MISC</td>
<td>9</td>
<td>0—UNSPECIFIED UTILITY AND MISCELLANEOUS</td>
</tr>
<tr>
<td>VEHICULAR</td>
<td>10</td>
<td>1—AUTOMOBILE OR TRUCK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2—AIRPLANE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3—BUS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4—FERRY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5—SHIP OR BOAT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6—TRAIN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7—MOTOR BIKE</td>
</tr>
<tr>
<td>OUTDOOR</td>
<td>11</td>
<td>0—UNSPECIFIED OUTDOOR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1—MUNI-MESH NETWORK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2—CITY PARK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3—REST AREA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4—TRAFFIC CONTROL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5—BUS STOP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6—KIOSK</td>
</tr>
</tbody>
</table>
Configuring Hotspot 2.0 (GUI)

Step 1 Choose WLAN to open the WLANs page.

Step 2 Hover your mouse over the blue drop-down arrow for the desired WLAN on which you want to configure the Hotspot parameters and choose Hotspot. The WLAN > Hot Spot page appears.

Step 3 From the Hotspot2 Enable drop-down list, choose the Enable option.

Step 4 In the Operator Name List section, specify the following:
   • Operator Name—Specify the name of the 802.11 operator.
   • Operator Index—Select an operator index. The range is from 1 to 32.
   • Language Code—An ISO-14962-1997 encoded string defining the language. This string is a three character language code.

Click Add to add the operator details. The operator details are displayed in a tabular form. To remove an operator, hover your mouse pointer over the blue drop-down arrow and choose Remove.

Step 5 In the Port Config List, specify the following:
   • IP Protocol—The IP protocol that you want to enable. The following options are available:
     - ICMP
     - FTP/SSH/TLS/PPTP VPN/VoIP
     - IKEv2 (IPSec VPN/VoIP/ESP)
   • Port No—The Port number that is enabled on this WLAN. The following options are available:
     - ICMPPr
     - FTP
     - SSH
     - TLS VPN
     - PPTP VPN
     - VoIP
     - IKEv2
     - ESP
   • Status—The status of the port. You can choose from the following options:
- Closed
- Open
- Unknown

- Index—The index value of the port configuration. The range is from 1 to 10.

Click **Add** to add the Port Config parameters. To remove a port configuration list, hover your mouse pointer over the blue drop-down arrow and choose **Remove**.

**Step 6**

Click **Apply**.

---

## Configuring Hotspot 2.0 (CLI)

- **config wlan mobile-concierge hotspot2 {enable | disable} wlan-id**—Enables or disables Hotspot2 on a WLAN.

- **config wlan mobile-concierge hotspot2 operator-name {add | modify} wlan-id index operator-name lang-code**—Configures the operator name on a WLAN. The following options are available:
  - **wlan-id**—The WLAN ID on which you want to configure the operator name.
  - **index**—The operator index of the operator. The range is from 1 to 32.
  - **operator-name**—The name of the 802.11an operator.
  - **lang-code**—The language used. An ISO-14962-1997 encoded string defining the language. This is a three character language code. Enter the first three letters of the language in English (for example, eng for English).

  **Tip**
  
  Press the **tab** key after entering a keyword or argument to get a list of valid values for the command.

- **config wlan mobile-concierge hotspot2 operator-name delete wlan-id index**—Deletes the operator-name with the specified index on the WLAN.

- **config wlan mobile-concierge hotspot2 port-config {add | modify} wlan-id index ip-protocol**—Configures the port configuration parameters. The **ip-protocol** argument can have one of the following values:
  - 1—ICMP
  - 6—FTP/SSH/TLS/PPTP-VPN/VoIP
  - 17—IKEv2 (IPSec-VPN/VoIP/ESP)
  - 50—ESP (IPSec-VPN)

  **Tip**
  
  Press the **tab** key after entering a keyword or argument to get a list of valid values for the command.

- **config wlan mobile-concierge hotspot2 wan-metrics add wlan-id link-status symet-link downlink-speed uplink-speed**—Configures the WAN metrics for a WLAN configured with Hotspot2.
where
- `link-status`—The link status. The valid range is 1–3.
- `symet-link`—The symmetric link status. For example, you can configure the uplink and downlink to have different speeds or same speeds.
- `downlink-speed`—The downlink speed. The maximum value is 4,194,304 kbps.
- `uplink-speed`—The uplink speed. The maximum value is 4,194,304 kbps.

Tip  Press the `tab` key after entering a keyword or argument to get a list of valid values for the command.

- `config wlan mobile-concierge hotspot2 wan-metrics delete wlan-id`—Deletes the WAN metrics on the configured WLAN.
Troubleshooting

This appendix contains the following sections:

- Information About Troubleshooting, page 18-1
- Interpreting LEDs, page 18-2
- System Messages, page 18-3
- Viewing System Resources, page 18-6
- Using the CLI to Troubleshoot Problems, page 18-8
- Configuring System and Message Logging, page 18-9
- Viewing Access Point Event Logs, page 18-16
- Uploading Logs and Crash Files, page 18-17
- Uploading Core Dumps from the Controller, page 18-20
- Uploading Packet Capture Files, page 18-23
- Monitoring Memory Leaks, page 18-26
- Troubleshooting CCXv5 Client Devices, page 18-27
- Using the Debug Facility, page 18-42
- Configuring Wireless Sniffing, page 18-47
- Troubleshooting Access Points Using Telnet or SSH, page 18-49
- Debugging the Access Point Monitor Service, page 18-52
- Troubleshooting OfficeExtend Access Points, page 18-53
- Troubleshooting Mesh Access Points, page 18-55

Information About Troubleshooting

This appendix lists system messages that can appear on the Cisco UWN solution interfaces, describes the LED patterns on controllers and lightweight access points, and provides CLI commands that can be used to troubleshoot problems on the controller. It contains these sections:
Interpreting LEDs

Information About Interpreting LEDs

This section describes how to interpret controller LEDs and lightweight access point LEDs.

This section contains the following topics:

- Interpreting Controller LEDs, page 18-2
- Interpreting Lightweight Access Point LEDs, page 18-2
- Interpreting OfficeExtend LEDs, page 18-53

Interpreting Controller LEDs


Interpreting Lightweight Access Point LEDs

See the quick start guide or hardware installation guide for your specific access point for a description of the LED patterns. See the list of access points and the respective documentation at http://www.cisco.com/en/US/products/hw/wireless/index.html.
System Messages

Information About System Messages

Table 18-1 lists some common system messages and their descriptions. For a complete list of system messages, see the Cisco Wireless LAN Controller System Message Guide.

Table 18-1 System Messages and Descriptions

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apf_utils.c 680: Received a CIF field without the protected bit set from mobile xx:xx:xx:xx:xx</td>
<td>A client is sending an association request on a security-enabled WLAN with the protected bit set to 0 (in the Capability field of the association request). As designed, the controller rejects the association request, and the client sees an association failure.</td>
</tr>
<tr>
<td>dtl_arp.c 480: Got an idle-timeout message from an unknown client xx:xx:xx:xx:xx</td>
<td>The controller’s network processing unit (NPU) sends a timeout message to the central processing unit (CPU) indicating that a particular client has timed out or aged out. This situation typically occurs when the CPU has removed a wireless client from its internal database but has not notified the NPU. Because the client remains in the NPU database, it ages out on the network processor and notifies the CPU. The CPU finds the client that is not present in its database and then sends this message.</td>
</tr>
<tr>
<td>STATION_DISASSOCIATE</td>
<td>The client may have intentionally terminated usage or may have experienced a service disruption.</td>
</tr>
<tr>
<td>STATION_DEAUTHENTICATE</td>
<td>The client may have intentionally terminated usage or this message could indicate an authentication issue.</td>
</tr>
<tr>
<td>STATION_AUTHENTICATION_FAIL</td>
<td>Check disable, key mismatch, or other configuration issues.</td>
</tr>
<tr>
<td>STATION_ASSOCIATE_FAIL</td>
<td>Check the load on the Cisco radio or signal quality issues.</td>
</tr>
<tr>
<td>LRAD_ASSOCIATED</td>
<td>The associated lightweight access point is now managed by this controller.</td>
</tr>
<tr>
<td>LRAD_DISASSOCIATED</td>
<td>The lightweight access point may have associated to a different controller or may have become completely unreachable.</td>
</tr>
<tr>
<td>LRAD_UP</td>
<td>The lightweight access point is operational; no action is required.</td>
</tr>
<tr>
<td>LRAD_DOWN</td>
<td>The lightweight access point may have a problem or is administratively disabled.</td>
</tr>
<tr>
<td>LRADIF_UP</td>
<td>The Cisco radio is UP.</td>
</tr>
<tr>
<td>Error Message</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LRADIF_DOWN</td>
<td>The Cisco radio may have a problem or is administratively disabled.</td>
</tr>
<tr>
<td>LRADIF_LOAD_PROFILE_FAILED</td>
<td>The client density may have exceeded the system capacity.</td>
</tr>
<tr>
<td>LRADIF_NOISE_PROFILE_FAILED</td>
<td>The non-802.11 noise has exceeded the configured threshold.</td>
</tr>
<tr>
<td>LRADIF_INTERFERENCE_PROFILE_FAILED</td>
<td>802.11 interference has exceeded the threshold limits on the channel; check channel assignments.</td>
</tr>
<tr>
<td>LRADIF_COVERAGE_PROFILE_FAILED</td>
<td>A possible coverage hole has been detected. Check the lightweight access point history to see if it is a common problem and add lightweight access points if necessary.</td>
</tr>
<tr>
<td>LRADIF_LOAD_PROFILE_PASSED</td>
<td>The load is now within threshold limits.</td>
</tr>
<tr>
<td>LRADIF_NOISE_PROFILE_PASSED</td>
<td>The detected noise is now less than threshold limits.</td>
</tr>
<tr>
<td>LRADIF_INTERFERENCEPROFILE_PASSED</td>
<td>The detected interference is now less than threshold limit.</td>
</tr>
<tr>
<td>LRADIF_COVERAGE_PROFILE_PASSED</td>
<td>The number of clients receiving a poor signal are within threshold limit.</td>
</tr>
<tr>
<td>LRADIF_CURRENT_TXPOWER_CHANGED</td>
<td>Informational message.</td>
</tr>
<tr>
<td>LRADIF_CURRENT_CHANNEL_CHANGED</td>
<td>Informational message.</td>
</tr>
<tr>
<td>LRADIF_RTS_THRESHOLD_CHANGED</td>
<td>Informational message.</td>
</tr>
<tr>
<td>LRADIF_ED_THRESHOLD_CHANGED</td>
<td>Informational message.</td>
</tr>
<tr>
<td>LRADIF_FRAGMENTATION_THRESHOLD_CHANGED</td>
<td>Informational message.</td>
</tr>
<tr>
<td>RRM_DOT11_A_GROUPING_DONE</td>
<td>Informational message.</td>
</tr>
<tr>
<td>RRM_DOT11_B_GROUPING_DONE</td>
<td>Informational message.</td>
</tr>
<tr>
<td>ROGUE_AP_DETECTED</td>
<td>May be a security issue. Use maps and trends to investigate.</td>
</tr>
<tr>
<td>ROGUE_AP_REMOVED</td>
<td>A detected rogue access point has timed out. The unit might have shut down or moved out of the coverage area.</td>
</tr>
<tr>
<td>AP_MAX_ROGUE_COUNT_EXCEEDED</td>
<td>The current number of active rogue access points has exceeded system threshold limit.</td>
</tr>
<tr>
<td>LINK_UP</td>
<td>Positive confirmation message.</td>
</tr>
<tr>
<td>LINK_DOWN</td>
<td>A port may have a problem or is administratively disabled.</td>
</tr>
<tr>
<td>LINK_FAILURE</td>
<td>A port may have a problem or is administratively disabled.</td>
</tr>
<tr>
<td>AUTHENTICATION_FAILURE</td>
<td>An attempted security breach has occurred. Investigate.</td>
</tr>
</tbody>
</table>
### Table 18-1 System Messages and Descriptions (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP_NEWROOT</td>
<td>Informational message.</td>
</tr>
<tr>
<td>STP_TOPOLOGY_CHANGE</td>
<td>Informational message.</td>
</tr>
<tr>
<td>IPSEC_ESP_AUTH_FAILURE</td>
<td>Check WLAN IPsec configuration.</td>
</tr>
<tr>
<td>IPSEC_ESP_REPLAY_FAILURE</td>
<td>Check for an attempt to spoof an IP address.</td>
</tr>
<tr>
<td>IPSEC_ESP_POLICY_FAILURE</td>
<td>Check for an IPsec configuration mismatch between the WLAN and client.</td>
</tr>
<tr>
<td>IPSEC_ESP_INVALID_SPI</td>
<td>Informational message.</td>
</tr>
<tr>
<td>IPSEC_OTHER_POLICY_FAILURE</td>
<td>Check for an IPsec configuration mismatch between the WLAN and client.</td>
</tr>
<tr>
<td>IPSEC_IKE_NEG_FAILURE</td>
<td>Check for an IPsec IKE configuration mismatch between the WLAN and client.</td>
</tr>
<tr>
<td>IPSEC_SUITE_NEG_FAILURE</td>
<td>Check for an IPsec IKE configuration mismatch between the WLAN and client.</td>
</tr>
<tr>
<td>IPSEC_INVALID_COOKIE</td>
<td>Informational message.</td>
</tr>
<tr>
<td>RADIOS_EXCEEDED</td>
<td>The maximum number of supported Cisco radios has been exceeded. Check for a controller failure in the same Layer 2 network or add another controller.</td>
</tr>
<tr>
<td>SENSED_TEMPERATURE_HIGH</td>
<td>Check fan, air conditioning, and/or other cooling arrangements.</td>
</tr>
<tr>
<td>SENSED_TEMPERATURE_LOW</td>
<td>Check the room temperature and/or other reasons for low temperature.</td>
</tr>
<tr>
<td>TEMPERATURESENSORFAILURE</td>
<td>Replace the temperature sensor as soon as possible.</td>
</tr>
<tr>
<td>TEMPERATURESENSORCLEAR</td>
<td>The temperature sensor is operational.</td>
</tr>
<tr>
<td>POE_CONTROLLER_FAILURE</td>
<td>Check ports; a possible serious failure has been detected.</td>
</tr>
<tr>
<td>MAX_ROGUE_COUNT_EXCEEDED</td>
<td>The current number of active rogue access points has exceeded system threshold limit.</td>
</tr>
<tr>
<td>SWITCH_UP</td>
<td>The controller is responding to SNMP polls.</td>
</tr>
<tr>
<td>SWITCH_DOWN</td>
<td>The controller is not responding to SNMP polls; check controller and SNMP settings.</td>
</tr>
<tr>
<td>RADIUS_SERVERS_FAILED</td>
<td>Check the network connectivity between RADIUS and the controller.</td>
</tr>
<tr>
<td>CONFIG_SAVED</td>
<td>The running configuration has been saved to flash; it will be active after a reboot.</td>
</tr>
<tr>
<td>MULTIPLE_USERS</td>
<td>Another user with the same username has logged in.</td>
</tr>
<tr>
<td>FAN_FAILURE</td>
<td>Monitor the controller temperature to avoid overheating.</td>
</tr>
<tr>
<td>POWER_SUPPLY_CHANGE</td>
<td>Check for a power-supply malfunction.</td>
</tr>
</tbody>
</table>
Viewing System Resources

This section contains the following topics:

- Information About Viewing System Resources, page 18-6
- Guidelines and Limitations, page 18-6
- Viewing System Resources (GUI), page 18-6
- Viewing System Resources (CLI), page 18-7

Information About Viewing System Resources

You can determine the amount of system resources being used by the controller such as the current controller CPU usage, system buffers, and web server buffers.

Guidelines and Limitations

The Cisco 5500 Series Controllers have multiple CPUs, so you can view individual CPU usage. For each CPU, you can see the percentage of the CPU in use and the percentage of the CPU time spent at the interrupt level (for example, 0%/3%).

Viewing System Resources (GUI)


<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COLD_START</td>
<td>The controller may have been rebooted.</td>
</tr>
<tr>
<td>WARM_START</td>
<td>The controller may have been rebooted.</td>
</tr>
</tbody>
</table>
Viewing System Resources (CLI)

On the controller CLI, enter these commands:

- **show cpu**
  
  Information similar to the following appears:

  
  ```plaintext
  Current CPU(s) load: 0%
  Individual CPU load: 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%
  
  Where the first number is the CPU percentage that the controller spent on the user application and the second number is the CPU percentage that the controller spent on the OS services.
  
- **show tech-support**
  
  Information similar to the following appears:

  ```plaintext
  System Information
  Manufacturer's Name.............................. Cisco Systems Inc.
  Product Name..................................... Cisco Controller
  Product Version............................... 6.0.165.0
  ...                        
  Current CPU(s) Load......................... 0%
  Individual CPU Load......................... 0%/3%, 0%/1%, 0%/1%, 0%/1%, 0%/0%, 0%/1%  
  
  System Buffers
  Max Free Buffers......................... 4608
  Free Buffers............................... 4596
  Buffers In Use............................. 12
  
  Web Server Resources
  Descriptors Allocated................... 259
  ```
Using the CLI to Troubleshoot Problems

If you experience any problems with your controller, you can use the commands in this section to gather information and debug issues.

1. **show process cpu**—Shows how various tasks in the system are using the CPU at that instant in time. This command is helpful in understanding if any single task is monopolizing the CPU and preventing other tasks from being performed.

   Information similar to the following appears:

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>CPU Use</th>
<th>Reaper</th>
</tr>
</thead>
<tbody>
<tr>
<td>reaperWatcher</td>
<td>(3/124)</td>
<td>0 %</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>osapiReaper</td>
<td>(10/121)</td>
<td>0 %</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>TempStatus</td>
<td>(255/1)</td>
<td>0 %</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>emWeb</td>
<td>(255/1)</td>
<td>0 %</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>cliWebTask</td>
<td>(255/1)</td>
<td>0 %</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>UtilTask</td>
<td>(255/1)</td>
<td>0 %</td>
<td>(0/0)% I</td>
</tr>
</tbody>
</table>

   In the example above, the following fields provide information:
   
   - The Name field shows the tasks that the CPU is to perform.
   - The Priority field shows two values: 1) the original priority of the task that was created by the actual function call and 2) the priority of the task divided by a range of system priorities.
   - The CPU Use field shows the CPU usage of a particular task.
   - The Reaper field shows three values: 1) the amount of time for which the task is scheduled in user mode operation, 2) the amount of time for which the task is scheduled in system mode operation, and 3) whether the task is being watched by the reaper task monitor (indicated by a “T”). If the task is being watched by the reaper task monitor, this field also shows the timeout value (in seconds) before which the task needs to alert the task monitor.

   **Note** If you want to see the total CPU usage as a percentage, enter the `show cpu` command.

2. **show process memory**—Shows the allocation and deallocation of memory from various processes in the system at that instant in time.

   Information similar to the following appears:

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>BytesInUse</th>
<th>BlocksInUse</th>
<th>Reaper</th>
</tr>
</thead>
<tbody>
<tr>
<td>reaperWatcher</td>
<td>(3/124)</td>
<td>0</td>
<td>0</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>osapiReaper</td>
<td>(10/121)</td>
<td>0</td>
<td>0</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>TempStatus</td>
<td>(255/1)</td>
<td>308</td>
<td>1</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>emWeb</td>
<td>(255/1)</td>
<td>294440</td>
<td>4910</td>
<td>(0/0)% T 300</td>
</tr>
<tr>
<td>cliWebTask</td>
<td>(255/1)</td>
<td>738</td>
<td>2</td>
<td>(0/0)% I</td>
</tr>
<tr>
<td>UtilTask</td>
<td>(255/1)</td>
<td>308</td>
<td>1</td>
<td>(0/0)% T 300</td>
</tr>
</tbody>
</table>

   In the example above, the following fields provide information:
• The Name field shows the tasks that the CPU is to perform.
• The Priority field shows two values: 1) the original priority of the task that was created by the actual function call and 2) the priority of the task divided by a range of system priorities.
• The BytesInUse field shows the actual number of bytes used by dynamic memory allocation for a particular task.
• The BlocksInUse field shows the chunks of memory that are assigned to perform a particular task.
• The Reaper field shows three values: 1) the amount of time for which the task is scheduled in user mode operation, 2) the amount of time for which the task is scheduled in system mode operation, and 3) whether the task is being watched by the reaper task monitor (indicated by a “T”). If the task is being watched by the reaper task monitor, this field also shows the timeout value (in seconds) before which the task needs to alert the task monitor.

3. `show tech-support`—Shows information related to the state of the system, including the current configuration, last crash file, CPU utilization, and memory utilization.

4. `show run-config`—Shows the complete configuration of the controller. To exclude access point configuration settings, use the `show run-config no-ap` command.

   **Note**  
   If you want to see the passwords in clear text, enter the `config passwd-cleartext enable` command. To execute this command, you must enter an admin password. This command is valid only for this particular session. It is not saved following a reboot.

5. `show run-config commands`—Shows the list of configured commands on the controller. This command shows only values configured by the user. It does not show system-configured default values.

### Configuring System and Message Logging

This section contains the following topics:

- **Information About System and Message Logging**, page 18-9
- **Configuring System and Message Logging (GUI)**, page 18-10
- **Viewing Message Logs (GUI)**, page 18-12
- **Configuring System and Message Logging (CLI)**, page 18-12

### Information About System and Message Logging

System logging allows controllers to log their system events to up to three remote syslog servers. The controller sends a copy of each syslog message as it is logged to each syslog server configured on the controller. Being able to send the syslog messages to multiple servers ensures that the messages are not lost due to the temporary unavailability of one syslog server. Message logging allows system messages to be logged to the controller buffer or console.
Configuring System and Message Logging (GUI)

Step 1
Choose Management > Logs > Config. The Syslog Configuration page appears.

![Syslog Configuration Page](image)

Step 2
In the Syslog Server IP Address text box, enter the IP address of the server to which to send the syslog messages and click Add. You can add up to three syslog servers to the controller. The list of syslog servers that have already been added to the controller appears below this text box.

**Note** If you want to remove a syslog server from the controller, click Remove to the right of the desired server.

Step 3
To set the severity level for filtering syslog messages to the syslog servers, choose one of the following options from the Syslog Level drop-down list:

- **Emergencies** = Severity level 0—System is unusable
- **Alerts** = Severity level 1 (default value)—Immediate action required
- **Critical** = Severity level 2—Critical condition
- **Errors** = Severity level 3—Error condition
- **Warnings** = Severity level 4—Warning condition
- **Notifications** = Severity level 5—Normal but significant condition
- **Informational** = Severity level 6—Informational message
- **Debugging** = Severity level 7—Message that appears during debugging

If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the syslog servers. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the syslog servers.

Step 4
You can set the facility for outgoing syslog messages to the syslog servers. The facility level is used to specify what type of program is logging the message. Choose one of the following options from the Syslog Facility drop-down list:
Step 5 Click **Apply** to commit your changes.

Step 6 To set the severity level for logging messages to the controller buffer and console, choose one of the following options from both the Buffered Log Level and Console Log Level drop-down lists:

- **Emergencies** = Severity level 0
- **Alerts** = Severity level 1
- **Critical** = Severity level 2
- **Errors** = Severity level 3 (default value)
- **Warnings** = Severity level 4
- **Notifications** = Severity level 5
- **Informational** = Severity level 6
- **Debugging** = Severity level 7
- **Disable**— This option is available only for the Console Log level. Select this option to disable console logging.

If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the controller. For example, if you set the logging level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are logged.

- **Kernel** = Facility level 0—Kernel messages
- **User Process** = Facility level 1—User-level messages
- **Mail** = Facility level 2—Mail System messages
- **System Daemons** = Facility level 3—System Daemons messages
- **Authorization** = Facility level 4—Security and Authorization messages
- **Syslog** = Facility level 5 (default value)—Syslog Daemon messages
- **Line Printer** = Facility level 6—Line Printer subsystem
- **USENET** = Facility level 7—User-initiated processes or application messages
- **Unix-to-Unix Copy** = Facility level 8—UNIX-to-UNIX Copy system messages
- **Cron** = Facility level 9—Cron Daemon messages
- **FTP Daemon** = Facility level 11—FTP Daemon messages
- **System Use 1** = Facility level 12—Reserved for system messages
- **System Use 2** = Facility level 13—Reserved for system messages
- **System Use 3** = Facility level 14—Reserved for system messages
- **System Use 4** = Facility level 15—Reserved for system messages
- **Local Use 0** = Facility level 16—Reserved for local use
- **Local Use 1** = Facility level 17—Reserved for local use
- **Local Use 2** = Facility level 18—Reserved for local use
- **Local Use 3** = Facility level 19—Reserved for local use
- **Local Use 4** = Facility level 20—Reserved for local use
- **Local Use 5** = Facility level 21—Reserved for local use
- **Local Use 6** = Facility level 22—Reserved for local use
- **Local Use 7** = Facility level 23—Reserved for local use
Step 7 Select the File Info check box if you want the message logs to include information about the source file. The default value is enabled.

Step 8 Select the Trace Info check box if you want the message logs to include traceback information. The default value is disabled.

Step 9 Click Apply to commit your changes.

Step 10 Click Save Configuration to save your changes.

Viewing Message Logs (GUI)

To view message logs using the controller GUI, choose Management > Logs > Message Logs. The Message Logs page appears.

Note To clear the current message logs from the controller, click Clear.

Configuring System and Message Logging (CLI)

To configure system and message logging using the controller CLI, follow these steps:

Step 1 To enable system logging and set the IP address of the syslog server to which to send the syslog messages, enter this command:

```
config logging syslog host server_IP_address
```

You can add up to three syslog servers to the controller.
To remove a syslog server from the controller, enter this command:

```
config logging syslog host server_IP_address delete
```

**Step 2**

To set the severity level for filtering syslog messages to the syslog server, enter this command:

```
config logging syslog level severity_level
```

where `severity_level` is one of the following:

- emergencies = Severity level 0
- alerts = Severity level 1
- critical = Severity level 2
- errors = Severity level 3
- warnings = Severity level 4
- notifications = Severity level 5
- informational = Severity level 6
- debugging = Severity level 7

**Note**

As an alternative, you can enter a number from 0 through 7 for the `severity_level` parameter.

**Note**

If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the syslog server. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the syslog server.

**Step 3**

To set the severity level for filtering syslog messages for a particular access point or for all access points, enter this command:

```
config ap logging syslog level severity_level {Cisco_AP | all}
```

where `severity_level` is one of the following:

- emergencies = Severity level 0
- alerts = Severity level 1
- critical = Severity level 2
- errors = Severity level 3
- warnings = Severity level 4
- notifications = Severity level 5
- informational = Severity level 6
- debugging = Severity level 7

**Note**

If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the access point. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the access point.

**Step 4**

To set the facility for outgoing syslog messages to the syslog server, enter this command:
**config logging syslog facility** *facility_code*

where *facility_code* is one of the following:

- **authorization** = Authorization system. Facility level = 4.
- **auth-private** = Authorization system (private). Facility level = 10.
- **cron** = Cron/at facility. Facility level = 9.
- **daemon** = System daemons. Facility level = 3.
- **ftp** = FTP daemon. Facility level = 11.
- **kern** = Kernel. Facility level = 0.
- **local0 =** Local use. Facility level = 16.
- **local1** = Local use. Facility level = 17.
- **local2** = Local use. Facility level = 18.
- **local3** = Local use. Facility level = 19.
- **local4** = Local use. Facility level = 20.
- **local5** = Local use. Facility level = 21.
- **local6** = Local use. Facility level = 22.
- **local7** = Local use. Facility level = 23.
- **lpr** = Line printer system. Facility level = 6.
- **mail** = Mail system. Facility level = 2.
- **news** = USENET news. Facility level = 7.
- **sys12** = System use. Facility level = 12.
- **sys13** = System use. Facility level = 13.
- **sys14** = System use. Facility level = 14.
- **sys15** = System use. Facility level = 15.
- **syslog** = The syslog itself. Facility level = 5.
- **user** = User process. Facility level = 1.
- **uucp** = Unix-to-Unix copy system. Facility level = 8.

**Step 5**

To set the severity level for logging messages to the controller buffer and console, enter these commands:

- **config logging buffered** *severity_level*
- **config logging console** *severity_level*

where *severity_level* is one of the following:

- **emergencies** = Severity level 0
- **alerts** = Severity level 1
- **critical** = Severity level 2
- **errors** = Severity level 3
- **warnings** = Severity level 4
- **notifications** = Severity level 5
- **informational** = Severity level 6
- **debugging** = Severity level 7
Note As an alternative, you can enter a number from 0 through 7 for the severity_level parameter.

Note If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the controller. For example, if you set the logging level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are logged.

Step 6 To save debug messages to the controller buffer, the controller console, or a syslog server, enter these commands:

- `config logging debug buffered {enable | disable}`
- `config logging debug console {enable | disable}`
- `config logging debug syslog {enable | disable}`

By default, the console command is enabled, and the buffered and syslog commands are disabled.

Step 7 To cause the controller to include information about the source file in the message logs or to prevent the controller from displaying this information, enter this command:

`config logging fileinfo {enable | disable}`

The default value is enabled.

Step 8 To cause the controller to include process information in the message logs or to prevent the controller from displaying this information, enter this command:

`config logging procinfo {enable | disable}`

The default value is disabled.

Step 9 To cause the controller to include traceback information in the message logs or to prevent the controller from displaying this information, enter this command:

`config logging traceinfo {enable | disable}`

The default value is disabled.

Step 10 To enable or disable timestamps in log messages and debug messages, enter these commands:

- `config service timestamps log {datetime | disable}`
- `config service timestamps debug {datetime | disable}`

where

- `datetime` = Messages are timestamped with the standard date and time. This is the default value.
- `disable` = Messages are not timestamped.

Step 11 To save your changes, enter this command:

`save config`

**Viewing System and Message Logs (CLI)**

To see the logging parameters and buffer contents, enter this command:

`show logging`
Information similar to the following appears:

Logging to buffer:
- Logging of system messages to buffer:
  - Logging filter level.......................... errors
  - Number of system messages logged.............. 8716
  - Number of system messages dropped............ 2906
- Logging of debug messages to buffer ........... Disabled
  - Number of debug messages logged............ 0
  - Number of debug messages dropped............ 0

Logging to console:
- Logging of system messages to console:
  - Logging filter level.......................... errors
  - Number of system messages logged............ 0
  - Number of system messages dropped............ 11622
- Logging of debug messages to console .......... Enabled
  - Number of debug messages logged............ 0
  - Number of debug messages dropped............ 0

Logging to syslog:
- Syslog facility................................ local0
  - Logging of system messages to syslog:
    - Logging filter level.......................... errors
    - Number of system messages logged............ 8716
    - Number of system messages dropped........... 0
    - Number of remote syslog hosts.............. 0
      - Host 1...................................... Not Configured
      - Host 2...................................... Not Configured
  - Logging of traceback.......................... Disabled
  - Logging of process information................ Disabled
  - Logging of source file informational......... Enabled
  - Timestamping of messages....................... Enabled
    - Timestamping of system messages.............. Enabled
      - Timestamp format.......................... Date and Time
    - Timestamping of debug messages.............. Enabled
      - Timestamp format.......................... Date and Time

Logging buffer (8722 logged, 2910 dropped)

*Mar 26 09:23:13.574: %MM-3-INVALID_PKT_RECVD: mm_listen.c:5508 Received an invalid packet from 1.100.163.144. Source member:0.0.0.0. source member unknown.
*Mar 26 09:23:13.574: %MM-3-INVALID_PKT_RECVD: mm_listen.c:5508 Received an invalid packet from 1.100.163.144. Source member:0.0.0.0. source member unknown.
Previous message occurred 2 times.
*Mar 26 09:22:44.925: %MM-3-INVALID_PKT_RECVD: mm_listen.c:5508 Received an invalid packet from 1.100.163.144. Source member:0.0.0.0. source member unknown.

Viewing Access Point Event Logs

This section contains the following topics:

- Information About Access Point Event Logs, page 18-17
- Viewing Access Point Event Logs (CLI), page 18-17
Information About Access Point Event Logs

Access points log all system messages (with a severity level greater than or equal to notifications) to the access point event log. The event log can contain up to 1024 lines of messages, with up to 128 characters per line. When the event log becomes filled, the oldest message is removed to accommodate a new event message. The event log is saved in a file on the access point flash, which ensures that it is saved through a reboot cycle. To minimize the number of writes to the access point flash, the contents of the event log are written to the event log file during normal reload and crash scenarios only.

Viewing Access Point Event Logs (CLI)

Use these CLI commands to view or clear the access point event log from the controller:

- To see the contents of the event log file for an access point that is joined to the controller, enter this command:
  
  `show ap eventlog Cisco_AP`

  Information similar to the following appears:

  AP event log download has been initiated
  Waiting for download to complete

  AP event log download completed.

  AP Event log Contents 

  *Sep 22 11:44:00.573: %CAPWAP-5-CHANGED: CAPWAP changed state to IMAGE
  *Sep 22 11:44:01.514: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to down
  *Sep 22 11:44:01.519: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed state to down
  *Mar 1 00:00:39.078: %CAPWAP-3-ERRORLOG: Did not get log server settings from DHCP.
  *Mar 1 00:00:42.142: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
  *Mar 1 00:00:42.151: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
  *Mar 1 00:00:42.158: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
  *Mar 1 00:00:48.078: %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER
  *Mar 1 00:00:48.078: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
  *Mar 1 00:01:48.122: %CAPWAP-3-CLIENTERRORLOG: Set Transport Address: no more AP manager IP addresses remain

- To delete the existing event log and create an empty event log file for a specific access point or for all access points joined to the controller, enter this command:

  `clear ap-eventlog {specific Cisco_AP | all}`

Uploading Logs and Crash Files

This section contains the following topics:
Prerequisites to Upload Logs and Crash Files

Follow the instructions in this section to upload logs and crash files from the controller. However, before you begin, ensure you have a TFTP or FTP server available for the file upload. Follow these guidelines when setting up a TFTP or FTP server:

- If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are uploading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Uploading Logs and Crash Files (GUI)

Step 1 Choose Command > Upload File. The Upload File from Controller page appears.

Step 2 From the File Type drop-down list, choose one of the following:

- Event Log
- Message Log
- Trap Log
- Crash File

Step 3 From the Transfer Mode drop-down list, choose TFTP or FTP.

Step 4 In the IP Address text box, enter the IP address of the TFTP or FTP server.
Uploading Logs and Crash Files

Step 5 In the File Path text box, enter the directory path of the log or crash file.

Step 6 In the File Name text box, enter the name of the log or crash file.

Step 7 If you chose FTP as the Transfer Mode, follow these steps:
   a. In the Server Login Username text box, enter the FTP server login name.
   b. In the Server Login Password text box, enter the FTP server login password.
   c. In the Server Port Number text box, enter the port number of the FTP server. The default value for
      the server port is 21.

Step 8 Click Upload to upload the log or crash file from the controller. A message appears indicating the status
   of the upload.

Uploading Logs and Crash Files (CLI)

Step 1 To transfer the file from the controller to a TFTP or FTP server, enter this command:
   `transfer upload mode {tftp | ftp}`

Step 2 To specify the type of file to be uploaded, enter this command:
   `transfer upload datatype datatype`
   where `datatype` is one of the following options:
   - `crashfile`—Uploads the system’s crash file.
   - `errorlog`—Uploads the system’s error log.
   - `panic-crash-file`—Uploads the kernel panic information if a kernel panic occurs.
   - `systemtrace`—Uploads the system’s trace file.
   - `traplog`—Uploads the system’s trap log.
   - `watchdog-crash-file`—Uploads the console dump resulting from a software-watchdog-initiated
     reboot of the controller following a crash. The software watchdog module periodically checks the
     integrity of the internal software and makes sure that the system does not stay in an inconsistent or
     nonoperational state for a long period of time.

Step 3 To specify the path to the file, enter these commands:
   - `transfer upload serverip server_ip_address`
   - `transfer upload path server_path_to_file`
   - `transfer upload filename filename`

Step 4 If you are using an FTP server, also enter these commands:
   - `transfer upload username username`
   - `transfer upload password password`
   - `transfer upload port port`

   Note The default value for the `port` parameter is 21.

Step 5 To see the updated settings, enter this command:
Step 6  When prompted to confirm the current settings and start the software upload, answer y.

Uploading Core Dumps from the Controller

This section contains the following topics:

- Information About Uploading Core Dumps from the Controller, page 18-20
- Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (GUI), page 18-20
- Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (CLI), page 18-21

Information About Uploading Core Dumps from the Controller

To help troubleshoot controller crashes, you can configure the controller to automatically upload its core dump file to an FTP server after experiencing a crash. You cannot upload the core dump file directly to an FTP or TFTP server but you can upload a crash file to an FTP or TFTP server. The controllers save the core dump file to flash memory following a crash.

Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (GUI)

Step 1  Choose Management > Tech Support > Core Dump to open the Core Dump page.
Step 2 To enable the controller to generate a core dump file following a crash, select the Core Dump Transfer check box.

Step 3 To specify the type of server to which the core dump file is uploaded, choose FTP from the Transfer Mode drop-down list.

Step 4 In the IP Address text box, enter the IP address of the FTP server.

Note The controller must be able to reach the FTP server.

Step 5 In the File Name text box, enter the name that the controller uses to label the core dump file.

Step 6 In the User Name text box, enter the username for FTP login.

Step 7 In the Password text box, enter the password for FTP login.

Step 8 Click Apply to commit your changes.

Step 9 Click Save Configuration to save your changes.

Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (CLI)

Step 1 To enable or disable the controller to generate a core dump file following a crash, enter this command:

```
config coredump {enable | disable}
```

Step 2 To specify the FTP server to which the core dump file is uploaded, enter this command:

```
config coredump ftp server_ip_address filename
```

where

- `server_ip_address` is the IP address of the FTP server to which the controller sends its core dump file.

  Note The controller must be able to reach the FTP server.

- `filename` is the name that the controller uses to label the core dump file.

Step 3 To specify the username and password for FTP login, enter this command:

```
config coredump username ftp_username password ftp_password
```

Step 4 To save your changes, enter this command:

```
save config
```

Step 5 To see a summary of the controller’s core dump file, enter this command:

```
show coredump summary
```

Information similar to the following appears:

```
Core Dump is enabled
FTP Server IP................................. 10.10.10.17
FTP Filename...................................... file1
FTP Username..................................... ftputer
```
Uploading Core Dumps from Controller to a TFTP or FTP Server (CLI)

Note
This procedure is not applicable for Cisco 2106 and 4400 controllers.

Step 1
To see information about the core dump file in flash memory, enter this command:

```bash
show coredump summary
```

Information similar to the following appears:

Core Dump is disabled
Core Dump file is saved on flash

Sw Version: 6.0.83.0
File Size: 9081788
File Name Suffix: filename.gz

Step 2
To transfer the file from the controller to a TFTP or FTP server, enter these commands:

- `transfer upload mode {tftp | ftp}`
- `transfer upload datatype coredump`
- `transfer upload serverip server_ip_address`
- `transfer upload path server_path_to_file`
- `transfer upload filename filename`

Note After the file is uploaded, it ends with a .gz suffix. If desired, you can upload the same core dump file multiple times with different names to different servers.

Step 3
If you are using an FTP server, also enter these commands:

- `transfer upload username username`
- `transfer upload password password`
- `transfer upload port port`

Note The default value for the `port` parameter is 21.

Step 4
To view the updated settings, enter this command:

`transfer upload start`

Step 5
When prompted to confirm the current settings and start the software upload, answer `y`. 
Uploading Packet Capture Files

This section contains the following topics:
- Information About Uploading Packet Capture Files, page 18-23
- Guidelines and Limitations, page 18-24
- Uploading Packet Capture Files (GUI), page 18-24
- Uploading Packet Capture Files (CLI), page 18-25

Information About Uploading Packet Capture Files

When a Cisco 5500 Series Controller’s data plane crashes, it stores the last 50 packets that the controller received in flash memory. This information can be useful in troubleshooting the crash.

When a crash occurs, the controller generates a new packet capture file (*.pcap) file, and a message similar to the following appears in the controller crash file:

Last 5 packets processed at each core are stored in "last_received_pkts.pcap" captured file.
- Frame 36,38,43,47,49, processed at core #0.
- Frame 14,27,30,42,45, processed at core #1.
- Frame 15,18,20,32,48, processed at core #2.
- Frame 11,29,34,37,46, processed at core #3.
- Frame 7,8,12,31,35, processed at core #4.
- Frame 21,25,39,41,50, processed at core #5.
- Frame 16,17,19,22,33, processed at core #6.
- Frame 6,10,13,23,26, processed at core #7.
- Frame 9,24,28,40,44, processed at core #8.
- Frame 1,2,3,4,5, processed at core #9.

You can use the controller GUI or CLI to upload the packet capture file from the controller. You can then use Wireshark or another standard packet capture tool to view and analyze the contents of the file. Figure 18-6 shows a sample output of a packet capture file in Wireshark.
Guidelines and Limitations

- Only Cisco 5500 Series Controllers generate packet capture files. This feature is not available on other controller platforms.

- Ensure that you have a TFTP or FTP server available for the file upload. Follow these guidelines when setting up a TFTP or FTP server:
  - If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are uploading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Uploading Packet Capture Files (GUI)

Step 1  Choose **Commands > Upload File** to open the Upload File from Controller page.
Step 2  From the File Type drop-down list, choose **Packet Capture**.

Step 3  From the Transfer Mode drop-down list, choose **TFTP** or **FTP**.

Step 4  In the IP Address text box, enter the IP address of the TFTP or FTP server.

Step 5  In the File Path text box, enter the directory path of the packet capture file.

Step 6  In the File Name text box, enter the name of the packet capture file. These files have a `.pcap` extension.

Step 7  If you are using an FTP server, follow these steps:
   a. In the Server Login Username text box, enter the username to log into the FTP server.
   b. In the Server Login Password text box, enter the password to log into the FTP server.
   c. In the Server Port Number text box, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 8  Click **Upload** to upload the packet capture file from the controller. A message appears indicating the status of the upload.

Step 9  Use Wireshark or another standard packet capture tool to open the packet capture file and see the last 50 packets that were received by the controller.

### Uploading Packet Capture Files (CLI)

Step 1  Log on to the controller CLI.

Step 2  Enter the `transfer upload mode` ([tftp | ftp] command.

Step 3  Enter the `transfer upload datatype packet-capture` command.

Step 4  Enter the `transfer upload serverip server-ip-address` command.

Step 5  Enter the `transfer upload path server-path-to-file` command.

Step 6  Enter the `transfer upload filename last_received_pkts.pcap` command.

Step 7  If you are using an FTP server, enter these commands:
   - `transfer upload username username`
   - `transfer upload password password`
   - `transfer upload port port`
Monitoring Memory Leaks

This section provides instructions for troubleshooting hard-to-solve or hard-to-reproduce memory problems.

Caution

The commands in this section can be disruptive to your system and should be run only when you are advised to do so by the Cisco Technical Assistance Center (TAC).

Monitoring Memory Leaks (CLI)

Step 1

To enable or disable monitoring for memory errors and leaks, enter this command:

```
config memory monitor errors {enable | disable}
```

The default value is disabled.

Note

Your changes are not saved across reboots. After the controller reboots, it uses the default setting for this feature.

Step 2

If you suspect that a memory leak has occurred, enter this command to configure the controller to perform an auto-leak analysis between two memory thresholds (in kilobytes):

```
config memory monitor leaks low_thresh high_thresh
```

If the free memory is lower than the `low_thresh` threshold, the system crashes, generating a crash file. The default value for this parameter is 10000 kilobytes, and you cannot set it below this value.
Set the high\_thresh threshold to the current free memory level or higher so that the system enters auto-leak-analysis mode. After the free memory reaches a level lower than the specified high\_thresh threshold, the process of tracking and freeing memory allocation begins. As a result, the debug memory events enable command shows all allocations and frees, and the show memory monitor detail command starts to detect any suspected memory leaks. The default value for this parameter is 30000 kilobytes.

**Step 3**

To see a summary of any discovered memory issues, enter this command:

`show memory monitor`

Information similar to the following appears:

Memory Leak Monitor Status:
low\_threshold(10000), high\_threshold(30000), current status(disabled)

Memory Error Monitor Status:
Crash-on-error flag currently set to (disabled)
No memory error detected.

**Step 4**

To see the details of any memory leaks or corruption, enter this command:

`show memory monitor detail`

Information similar to the following appears:

Memory error detected. Details:
-------------------------------------------------------------------------------
- Corruption detected at pmalloc entry address: 0x179a7ec0
- Corrupt entry: headerMagic(0xdeadf00d), trailer(0xabcdef), entrysize(128), bytes(100), thread(Unknown task name, task id = (332096592)), file(pmalloc.c), line(1736), time(1027)

Previous 1K memory dump from error location.
-------------------------------------------------------------------------------

(179a7ac0): 00000000 00000000 00000000 ceeff00d readf00d 00000080 00000000 00000000
(179a7ae0): 17958b20 00000000 1175608c 00000078 00000000 readceef 179a7af0 00000001
(179a7b00): 00000003 00000006 00000001 00000004 00000001 00000001 00000009 00000009 0000002d
(179a7b20): 00000001 00000002 00000002 00000002 00000001 00000001 00000004 00000000 00000000 5d7b9aba
(179a7b40): cbddf004 179f4b65e 7791acc8 e5032242 5365788c a1b7cee6 00000000 00000000
(179a7b60): 00000000 00000000 00000000 00000000 00000000 00000000 ceeff00d readf00d 00000080
(179a7b80): 00000000 00000000 00000000 17958d50 00000000 1175608c 00000078 00000000 readceef
(179a7ba0): 179a7ba4 00000001 00000003 00000006 00000001 00000001 00000004 00000001 0003763
(179a7bc0): 00000002 00000002 00000010 00000001 00000002 00000000 00000000 00000000 00000000 00000000 00000000 00000000 5d7b9aba
(179a7be0): 0000001a 00000089 00000000 00000000 00000000 00000008 00000000 00000000 00000000 00000000 00000000 00000000 00000000 17222194
(179a7c00): 1722246c 1722246c 00000000 00000000 00000000 00000000 00000000 00000000 00000000 ceeff00d
(179a7c20): 179a7b78 00000000 00000000 00000000 00000000 00000000 00000000 00000000

**Step 5**

If a memory leak occurs, enter this command to enable debugging of errors or events during memory allocation:

`debug memory {errors | events} {enable | disable}`

---

**Troubleshooting CCXv5 Client Devices**

This section contains the following topics:

- Information About Troubleshooting CCXv5 Client Devices, page 18-28
Information About Troubleshooting CCXv5 Client Devices

The controller supports three features designed to help troubleshoot communication problems with CCXv5 clients: diagnostic channel, client reporting, and roaming and real-time diagnostics. See the “Configuring Cisco Client Extensions” section on page 8-57 for more information on CCX.

Guidelines and Limitations

These features are supported only on CCXv5 clients. They are not supported for use with non-CCX clients or with clients running an earlier version of CCX.

Configuring Diagnostic Channel

The diagnostic channel feature enables you to troubleshoot problems regarding client communication with a WLAN. The client and access points can be put through a defined set of tests in an attempt to identify the cause of communication difficulties the client is experiencing and then allow corrective measures to be taken to make the client operational on the network. You can use the controller GUI or CLI to enable the diagnostic channel, and you can use the controller CLI or WCS to run the diagnostic tests.

Note

We recommend that you enable the diagnostic channel feature only for nonanchored SSIDs that use the management interface.

Configuring the Diagnostic Channel (GUI)

Step 1  Choose WLANs to open the WLANs page.

Step 2  Create a new WLAN or click the ID number of an existing WLAN.

Note

We recommend that you create a new WLAN on which to run the diagnostic tests.

Step 3  When the WLANs > Edit page appears, choose the Advanced tab to open the WLANs > Edit (Advanced) page.
Step 4 If you want to enable diagnostic channel troubleshooting on this WLAN, select the Diagnostic Channel check box. Otherwise, leave this check box unselected, which is the default value.

Note You can use the CLI to initiate diagnostic tests on the client. See the “Configuring the Diagnostic Channel (CLI)” section on page 18-29 for details.

Step 5 Click Apply to commit your changes.

Step 6 Click Save Configuration to save your changes.

Configuring the Diagnostic Channel (CLI)

Step 1 To enable diagnostic channel troubleshooting on a particular WLAN, enter this command:

```
config wlan diag-channel {enable | disable} wlan_id
```

Step 2 To verify that your change has been made, enter this command:

```
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier................................. 1
Profile Name........................................ employee
Network Name (SSID)............................. employee
Status............................................. Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override............................ Disabled
Number of Active Clients....................... 0
Exclusionlist Timeout........................... 60 seconds
Session Timeout.................................. Infinity
Interface......................................... virtual
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required.............. Disabled
Quality of Service.............................. Silver (best effort)
```
Step 3  To send a request to the client to perform the DHCP test, enter this command:

```
config client ccx dhcp-test client_mac_address
```

**Note**  This test does not require the client to use the diagnostic channel.

Step 4  To send a request to the client to perform the default gateway ping test, enter this command:

```
config client ccx default-gw-ping client_mac_address
```

**Note**  This test does not require the client to use the diagnostic channel.

Step 5  To send a request to the client to perform the DNS server IP address ping test, enter this command:

```
config client ccx dns-ping client_mac_address
```

**Note**  This test does not require the client to use the diagnostic channel.

Step 6  To send a request to the client to perform the DNS name resolution test to the specified hostname, enter this command:

```
config client ccx dns-resolve client_mac_address host_name
```

**Note**  This test does not require the client to use the diagnostic channel.

Step 7  To send a request to the client to perform the association test, enter this command:

```
config client ccx test-association client_mac_address ssid bssid {802.11a | 802.11b | 802.11g} channel
```

Step 8  To send a request to the client to perform the 802.1X test, enter this command:

```
config client ccx test-dot1x client_mac_address profile_id bssid {802.11a | 802.11b | 802.11g} channel
```

Step 9  To send a request to the client to perform the profile redirect test, enter this command:

```
config client ccx test-profile client_mac_address profile_id
```

The **profile_id** should be from one of the client profiles for which client reporting is enabled.

**Note**  Users are redirected back to the parent WLAN, not to any other profile. The only profile shown is the user’s parent profile. However, parent WLAN profiles can have one child diagnostic WLAN.

Step 10  Use these commands if necessary to abort or clear a test:

- To send a request to the client to abort the current test, enter this command:

```
config client ccx test-abort client_mac_address
```

Only one test can be pending at a time, so this command aborts the current pending test.
To clear the test results on the controller, enter this command:

```
config client ccx clear-results client_mac_address
```

**Step 11**  
To send a message to the client, enter this command:

```
config client ccx send-message client_mac_address message_id
```

where `message_id` is one of the following:

- 1 = The SSID is invalid.
- 2 = The network settings are invalid.
- 3 = There is a WLAN credibility mismatch.
- 4 = The user credentials are incorrect.
- 5 = Please call support.
- 6 = The problem is resolved.
- 7 = The problem has not been resolved.
- 8 = Please try again later.
- 9 = Please correct the indicated problem.
- 10 = Troubleshooting is refused by the network.
- 11 = Retrieving client reports.
- 12 = Retrieving client logs.
- 13 = Retrieval complete.
- 14 = Beginning association test.
- 15 = Beginning DHCP test.
- 16 = Beginning network connectivity test.
- 17 = Beginning DNS ping test.
- 18 = Beginning name resolution test.
- 19 = Beginning 802.1X authentication test.
- 20 = Redirecting client to a specific profile.
- 21 = Test complete.
- 22 = Test passed.
- 23 = Test failed.
- 24 = Cancel diagnostic channel operation or select a WLAN profile to resume normal operation.
- 25 = Log retrieval refused by the client.
- 26 = Client report retrieval refused by the client.
- 27 = Test request refused by the client.
- 28 = Invalid network (IP) setting.
- 29 = There is a known outage or problem with the network.
- 30 = Scheduled maintenance period.
- 31 = The WLAN security method is not correct.
- 32 = The WLAN encryption method is not correct.
- 33 = The WLAN authentication method is not correct.
Step 12 To see the status of the last test, enter this command:

```
show client ccx last-test-status client_mac_address
```

Information similar to the following appears for the default gateway ping test:

```
Test Type........................................ Gateway Ping Test
Test Status.................................... Pending/Success/Timeout
Dialog Token.................................... 15
Timeout.......................................... 15000 ms
Request Time................................... 1329 seconds since system boot
```

Step 13 To see the status of the last test response, enter this command:

```
show client ccx last-response-status client_mac_address
```

Information similar to the following appears for the 802.1X authentication test:

```
Test Status..................................... Success
Response Dialog Token.......................... 87
Response Status.................................. Successful
Response Test Type............................. 802.1X Authentication Test
Response Time.................................. 3476 seconds since system boot
```

Step 14 To see the results from the last successful diagnostics test, enter this command:

```
show client ccx results client_mac_address
```

Information similar to the following appears for the 802.1X authentication test:

```
dot1x Complete................................. Success
EAP Method...................................... *1,Host OS Login Credentials
dot1x Status.................................... 255
```

Step 15 To see the relevant data frames captured by the client during the previous test, enter this command:

```
show client ccx frame-data client_mac_address
```

Information similar to the following appears:

```
LOG Frames:
Frame Number:.................................... 1
Last Frame Number:............................. 1120
Direction:...................................... 1
Timestamp:...................................... 0d 00h 50m 39s 863954us
Frame Length:................................... 197
Frame Data:
```00000000: 80 00 00 00 ff ff ff ff ff ff 00 12 44 bd bd b0 ............D...```
```00000010: 00 12 44 bd bd b0 f0 af 43 70 00 f2 82 01 00 00 ..D.....Cp......```
```00000020: 64 00 11 08 00 01 00 01 08 8c 12 98 24 b0 48 60 d...........$.H```
```00000030: 6c 05 04 01 02 00 00 00 1e 00 00 89 00 0f 00 ff l.............```
```00000040: 01 19 00 41 50 32 3d 32 33 32 3d 31 30 00 00 00 00 00 00 ..AP23-10........```
```00000050: 00 00 00 00 00 00 00 26 96 06 00 40 96 00 ff ff df ........&....```
```00000060: 18 00 50 f2 01 00 00 50 f2 01 00 00 50 f2 01 00 00 50 f2 P...P..P```
```00000070: 05 01 00 00 40 96 00 28 00 dd 06 00 40 96 01 01 ....@...(.....```
```00000080: dd 05 00 40 96 03 04 dd 16 00 40 96 04 00 02 ........@......```
```00000090: 07 a4 00 00 23 a4 00 00 42 43 00 00 62 32 00 00 ...."...BC..b2..```
```000000a0: dd 05 00 40 96 0b 01 dd 18 00 50 f2 02 01 01 82 ........P....```
```000000b0: 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62 32 2f ...."...BC^..b2/```
```
LOG Frames:
Frame Number:.................................... 2
```
Configuring Client Reporting

The client reporting protocol is used by the client and the access point to exchange client information. Client reports are collected automatically when the client associates. You can use the controller GUI or CLI to send a client report request to any CCXv5 client any time after the client associates. There are four types of client reports:

- Client profile—Provides information about the configuration of the client.
- Operating parameters—Provides the details of the client’s current operational modes.
- Manufacturers’ information—Provides data about the wireless LAN client adapter in use.
- Client capabilities—Provides information about the client’s capabilities.

Configuring Client Reporting (GUI)

Step 1
Choose Monitor > Clients to open the Clients page.
Step 2  Click the MAC address of the desired client. The Clients > Detail page appears.

**Figure 18-9  Clients > Detail Page**

![Clients > Detail Page](image)

- **Step 3**  Click **Send CCXV5 Req** to send a report request to the client.
**Note** You must create a Trusted Profile using ACAU for Cisco CB21AG or equivalent software from your CCXv5 vendor.

**Step 4** Click **Display** to view the parameters from the client. The Client Reporting page appears.

**Figure 18-10 Client Reporting Page**

This page lists the client profiles and indicates if they are currently in use. It also provides information on the client’s operating parameters, manufacturer, and capabilities.
Step 5  Click the link for the desired client profile. The Profile Details page appears.

**Figure 18-11  Profile Details Page**

This page shows the client profile details, including the SSID, power save mode, radio channel, data rates, and 802.11 security settings.

**Configuring Client Reporting (CLI)**

**Step 1**  To send a request to the client to send its profiles, enter this command:

```
config client ccx get-profiles client_mac_address
```

**Step 2**  To send a request to the client to send its current operating parameters, enter this command:

```
config client ccx get-operating-parameters client_mac_address
```

**Step 3**  To send a request to the client to send the manufacturer’s information, enter this command:

```
config client ccx get-manufacturer-info client_mac_address
```

**Step 4**  To send a request to the client to send its capability information, enter this command:

```
config client ccx get-client-capability client_mac_address
```

**Step 5**  To clear the client reporting information, enter this command:

```
config client ccx clear-reports client_mac_address
```

**Step 6**  To see the client profiles, enter this command:
show client ccx profiles client_mac_address

Information similar to the following appears:

Number of Profiles............................... 1
Current Profile.................................. 1

Profile ID....................................... 1
Profile Name..................................... wifiEAP
SSID............................................. wifiEAP
Security Parameters[EAP Method,Credential]...... EAP-TLS,Host OS Login Credentials
Auth Method...................................... EAP
Key Management.................................. WPA2+CCM
Encryption....................................... AES-CCMP
Power Save Mode.................................. Constantly Awake

Radio Configuration:
Radio Type....................................... DSSS
Preamble Type.................................. Long preamble
CCA Method..................................... Energy Detect + Carrier
Detect/Correlation
Data Retries...................................... 6
Fragment Threshold............................. 2342
Radio Channels.................................. 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode.................................. Automatic
Rate List (MB)b.................................... 1.0 2.0

Radio Type....................................... HRDSSS(802.11b)
Preamble Type.................................. Long preamble
CCA Method..................................... Energy Detect + Carrier
Detect/Correlation
Data Retries...................................... 6
Fragment Threshold............................. 2342
Radio Channels.................................. 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode.................................. Automatic
Rate List (MB)b.................................... 5.5 11.0

Radio Type....................................... ERP(802.11g)
Preamble Type.................................. Long preamble
CCA Method..................................... Energy Detect + Carrier
Detect/Correlation
Data Retries...................................... 6
Fragment Threshold............................. 2342
Radio Channels.................................. 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode.................................. Automatic
Rate List (MB)b.................................... 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Radio Type....................................... OFDM(802.11a)
Preamble Type.................................. Long preamble
CCA Method..................................... Energy Detect + Carrier
Detect/Correlation
Data Retries...................................... 6
Fragment Threshold............................. 2342
Radio Channels.................................. 36 40 44 48 52 56 60 64 149 153 157 161 165
Tx Power Mode.................................. Automatic
Rate List (MB)b.................................... 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Step 7
To see the client operating parameters, enter this command:

show client ccx operating-parameters client_mac_address

Information similar to the following appears:

Client Mac....................................... 00:40:96:b2:8d:5e
Radio Type....................................... OFDM(802.11a)
Step 8
To see the client manufacturer information, enter this command:

```plaintext
show client ccx manufacturer-info client_mac_address
```

Information similar to the following appears:

- **Manufacturer OUI**: 00:40:96
- **Manufacturer ID**: Cisco
- **Manufacturer Model**: Cisco Aironet 802.11a/b/g Wireless
- **Adapter**: FOC1046N3SX
- **Mac Address**: 00:40:96:b2:8d:5e
- **Radio Type**: DSSS OFDM(802.11a) HRDSSS(802.11b) ERP(802.11g)
- **Antenna Type**: Omni-directional diversity
- **Antenna Gain**: 2 dBi
- **Rx Sensitivity**:
  - **Radio Type**: DSSS
  - **Rate**: 1.0 Mbps, MinRssi:-95, MaxRssi:-30
  - **Rate**: 2.0 Mbps, MinRssi:-95, MaxRssi:-30
  - **Radio Type**: HRDSSS(802.11b)
  - **Rate**: 5.5 Mbps, MinRssi:-95, MaxRssi:-30
  - **Rate**: 11.0 Mbps, MinRssi:-95, MaxRssi:-30
  - **Radio Type**: ERP(802.11g)
  - **Rate**: 6.0 Mbps, MinRssi:-95, MaxRssi:-30
  - **Rate**: 9.0 Mbps, MinRssi:-95, MaxRssi:-30
  - **Rate**: 12.0 Mbps, MinRssi:-95, MaxRssi:-30
  - **Rate**: 18.0 Mbps, MinRssi:-95, MaxRssi:-30

Step 9
To see the client’s capability information, enter this command:
show client ccx client-capability client_mac_address

Note This command displays the client’s available capabilities, not current settings for the capabilities.

Information similar to the following appears:

Service Capability............... Voice, Streaming(uni-directional) Video, Interactive(bi-directional) Video
Radio Type.......................... DSSS OFDM(802.11a) HRDSSS(802.11b) ERP(802.11g)

Radio Type.......................... DSSS
Radio Channels...................... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode........................ Automatic
Rate List (MB)........................ 1.0 2.0

Radio Type.......................... HRDSSS(802.11b)
Radio Channels...................... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode........................ Automatic
Rate List (MB)........................ 5.5 11.0

Radio Type.......................... ERP(802.11g)
Radio Channels...................... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode........................ Automatic
Rate List (MB)........................ 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Radio Type.......................... OFDM(802.11a)
Radio Channels...................... 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
Tx Power Mode........................ Automatic
Rate List (MB)........................ 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

---

Configuring Roaming and Real-Time Diagnostics

You can use roaming and real-time logs and statistics to solve system problems. The event log enables you to identify and track the behavior of a client device. It is especially useful when attempting to diagnose difficulties that a user may be having on a WLAN. The event log provides a log of events and reports them to the access point. There are three categories of event logs:

- Roaming log—This log provides a historical view of the roaming events for a given client. The client maintains a minimum of five previous roaming events including failed attempts and successful roams.
- Robust Security Network Association (RSNA) log—This log provides a historical view of the authentication events for a given client. The client maintains a minimum of five previous authentication attempts including failed attempts and successful ones.
- Syslog—This log provides internal system information from the client. For example, it may indicate problems with 802.11 operation, system operation, and so on.

The statistics report provides 802.1X and security information for the client. You can use the controller CLI to send the event log and statistics request to any CCXv5 client any time after the client associates.
Configuring Roaming and Real-Time Diagnostics (CLI)

**Step 1**  
To send a log request, enter this command:

```
config client cxx log-request log_type client_mac_address
```

where *log_type* is roam, rsna, or syslog.

**Step 2**  
To view a log response, enter this command:

```
show client cxx log-response log_type client_mac_address
```

where *log_type* is roam, rsna, or syslog.

Information similar to the following appears for a log response with a *log_type* of roam:

<table>
<thead>
<tr>
<th>Time</th>
<th>Log ID</th>
<th>Status</th>
<th>Event Timestamp</th>
<th>Source BSSID</th>
<th>Target BSSID</th>
<th>Transition Time</th>
<th>Reason</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue Jun 26 18:28:48 2007</td>
<td>133</td>
<td>Successful</td>
<td>0d 00h 00m 13s 322396us</td>
<td>00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2,</td>
<td>00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2,</td>
<td>3125 (ms)</td>
<td>Normal roam, poor link</td>
<td>Success</td>
</tr>
<tr>
<td>Transition Time</td>
<td>3125 (ms)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tue Jun 26 18:28:48 2007</td>
<td>133</td>
<td>Successful</td>
<td>0d 00h 00m 16s 599006us</td>
<td>00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2,</td>
<td>00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2,</td>
<td>3235 (ms)</td>
<td>Normal roam, poor link</td>
<td>Success</td>
</tr>
<tr>
<td>Transition Time</td>
<td>3235 (ms)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tue Jun 26 18:28:48 2007</td>
<td>133</td>
<td>Successful</td>
<td>0d 00h 00m 26s 637084us</td>
<td>00:0b:85:81:06:d2, Target BSSID=00:0b:85:81:06:d2,</td>
<td>00:0b:85:81:06:d2, Target BSSID=00:0b:85:81:06:d2,</td>
<td>3281 (ms)</td>
<td>First association to WLAN</td>
<td>Success</td>
</tr>
<tr>
<td>Transition Time</td>
<td>3281 (ms)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tue Jun 26 18:24:09 2007</td>
<td>132</td>
<td>Successful</td>
<td>0d 00h 00m 08s 815477us</td>
<td>00:14:1b:58:86:cd</td>
<td>00:14:1b:58:86:cd</td>
<td>246578us</td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>RSNA Version</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Cipher Suite</td>
<td>00-0f-ac-02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pairwise Cipher Suite Count</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARM Suite Count</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARM Suite</td>
<td>00-0f-ac-01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSNA Capability</td>
<td>0x0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSNA Result</td>
<td>Success</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Information similar to the following appears for a log response with a *log_type* of rsna:

<table>
<thead>
<tr>
<th>Time</th>
<th>Log ID</th>
<th>Status</th>
<th>Event Timestamp</th>
<th>Source BSSID</th>
<th>Target BSSID</th>
<th>Transition Time</th>
<th>Reason</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue Jun 26 18:24:09 2007</td>
<td>132</td>
<td>Successful</td>
<td>0d 00h 00m 00s 246578us</td>
<td>00:14:1b:58:86:cd</td>
<td>00:14:1b:58:86:cd</td>
<td>246578us</td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>RSNA Version</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>Group Cipher Suite</td>
<td>00-0f-ac-02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>Pairwise Cipher Suite Count</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>ARM Suite Count</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>ARM Suite</td>
<td>00-0f-ac-01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>RSNA Capability</td>
<td>0x0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>RSNA Result</td>
<td>Success</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
</tbody>
</table>

Information similar to the following appears for a log response with a *log_type* of syslog:

<table>
<thead>
<tr>
<th>Time</th>
<th>Log ID</th>
<th>Status</th>
<th>Event Timestamp</th>
<th>Source BSSID</th>
<th>Target BSSID</th>
<th>Transition Time</th>
<th>Reason</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue Jun 26 18:24:09 2007</td>
<td>132</td>
<td>Successful</td>
<td>0d 00h 00m 00s 246578us</td>
<td>00:14:1b:58:86:cd</td>
<td>00:14:1b:58:86:cd</td>
<td>246578us</td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>RSNA Version</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>Group Cipher Suite</td>
<td>00-0f-ac-02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>Pairwise Cipher Suite Count</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>ARM Suite Count</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>ARM Suite</td>
<td>00-0f-ac-01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>RSNA Capability</td>
<td>0x0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
<tr>
<td>RSNA Result</td>
<td>Success</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00-0f-ac-01</td>
<td>00-0f-ac-02</td>
</tr>
</tbody>
</table>
AKM Suite 0 = 00-0f-ac-01
RSN Capability = 0x0
RSNA Result: Success

Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
Event Timestamp=0d 00h 00m 01s 624375us
Target BSSID=00:14:1b:58:86:cd
RSNA Version=1
Group Cipher Suite=00-0f-ac-02
Pairwise Cipher Suite Count = 1
Pairwise Cipher Suite 0 = 00-0f-ac-04
AKM Suite Count = 1
AKM Suite 0 = 00-0f-ac-01
RSN Capability = 0x0
RSNA Result: Success

Information similar to the following appears for a log response with a log_type of syslog:

Event Timestamp=0d 00h 19m 42s 278987us
Client SysLog = '<11> Jun 19 11:49:47 uraval3777 Mandatory
elements missing in the OID response'
Event Timestamp=0d 00h 19m 42s 278990us
Client SysLog = '<11> Jun 19 11:49:50 uraval3777 Mandatory
elements missing in the OID response'

Step 3
To send a request for statistics, enter this command:

```plaintext
config client ccx stats-request measurement_duration stats_name client_mac_address
```

where stats_name is dot11 or security.

Step 4
To view the statistics response, enter this command:

```plaintext
show client ccx stats-report client_mac_address
```

Information similar to the following appears:

Measurement duration = 1

dot11TransmittedFragmentCount = 1
dot11MulticastTransmittedFrameCount = 2
dot11FailedCount = 3
dot11RetryCount = 4
dot11MultipleRetryCount = 5
dot11FrameDuplicateCount = 6
Using the Debug Facility

This section contains the following topics:

- Information About Using the Debug Facility, page 18-42
- Configuring the Debug Facility (CLI), page 18-43

Information About Using the Debug Facility

The debug facility enables you to display all packets going to and from the controller CPU. You can enable it for received packets, transmitted packets, or both. By default, all packets received by the debug facility are displayed. However, you can define access control lists (ACLs) to filter packets before they are displayed. Packets not passing the ACLs are discarded without being displayed.

Each ACL includes an action (permit, deny, or disable) and one or more fields that can be used to match the packet. The debug facility provides ACLs that operate at the following levels and on the following values:

- Driver ACL
  - NPU encapsulation type
  - Port

- Ethernet header ACL
  - Destination address
  - Source address
  - Ethernet type
  - VLAN ID

- IP header ACL
  - Source address
  - Destination address
  - Protocol
  - Source port (if applicable)
  - Destination port (if applicable)

- EoIP payload Ethernet header ACL
  - Destination address
  - Source address

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot11RTSSuccessCount</td>
<td>7</td>
</tr>
<tr>
<td>dot11RTSFailureCount</td>
<td>8</td>
</tr>
<tr>
<td>dot11ACKFailureCount</td>
<td>9</td>
</tr>
<tr>
<td>dot11ReceivedFragmentCount</td>
<td>10</td>
</tr>
<tr>
<td>dot11MulticastReceivedFrameCount</td>
<td>11</td>
</tr>
<tr>
<td>dot11FCSErrorCount</td>
<td>12</td>
</tr>
<tr>
<td>dot11TransmittedFrameCount</td>
<td>13</td>
</tr>
</tbody>
</table>
- Ethernet type
- VLAN ID

- **EoIP payload IP header ACL**
  - Source address
  - Destination address
  - Protocol
  - Source port (if applicable)
  - Destination port (if applicable)

- **CAPWAP payload 802.11 header ACL**
  - Destination address
  - Source address
  - BSSID
  - SNAP header type

- **CAPWAP payload IP header ACL**
  - Source address
  - Destination address
  - Protocol
  - Source port (if applicable)
  - Destination port (if applicable)

At each level, you can define multiple ACLs. The first ACL that matches the packet is the one that is selected.

### Configuring the Debug Facility (CLI)

**Step 1**
To enable the debug facility, enter this command:

```
dbglkes type

EoIP payload IP header ACL
- Source address
- Destination address
- Protocol
- Source port (if applicable)
- Destination port (if applicable)

CAPWAP payload 802.11 header ACL
- Destination address
- Source address
- BSSID
- SNAP header type

CAPWAP payload IP header ACL
- Source address
- Destination address
- Protocol
- Source port (if applicable)
- Destination port (if applicable)
```

At each level, you can define multiple ACLs. The first ACL that matches the packet is the one that is selected.

**Step 2**
Configure packet-logging ACLs by entering these commands:

- `debug packet logging acl driver rule_index action npu_encap port`

**Note**
To disable the debug facility, enter `debug packet logging disable` command.
- `rule_index` is a value between 1 and 6 (inclusive).
- `action` is permit, deny, or disable.
- `npu_encap` specifies the NPU encapsulation type, which determines how packets are filtered. The possible values include dhcp, dot11-mgmt, dot11-probe, dot1x, eoip-pong, iapp, ip, lwapp, multicast, orphan-from-sta, orphan-to-sta, rscp, wired-guest, or any.
- `port` is the physical port for packet transmission or reception.

**debug packet logging acl eth** `rule_index action dst src type vlan`

where
- `rule_index` is a value between 1 and 6 (inclusive).
- `action` is permit, deny, or disable.
- `dst` is the destination MAC address.
- `src` is the source MAC address.
- `type` is the two-byte type code (such as 0x800 for IP, 0x806 for ARP). This parameter also accepts a few common string values such as “ip” (for 0x800) or “arp” (for 0x806).
- `vlan` is the two-byte VLAN ID.

**debug packet logging acl ip** `rule_index action src dst proto src_port dst_port`

where
- `proto` is a numeric or any string recognized by getprotobyname(). The controller supports the following strings: ip, icmp, igmp, ggp, ipencap, st, tcp, egp, pup, udp, hmp, xns-idp, rdp, iso-tp4, xtp, dtp, idpr-cmtip, rsmtp, vmtip, ospf, ipip, and encap.
- `src_port` is the UDP/TCP two-byte source port (for example, telnet, 23) or “any.” The controller accepts a numeric or any string recognized by getservbyname(). The controller supports the following strings: tcpmux, echo, discard, syslog, daytime, netstat, qotd, msp, chargen, ftp-data, ftp, fsp, ssh, telnet, smtp, time, rlp, nameserver, whois, re-mail-ck, domain, smtp, bootp, bootpc, tftp, gopher, rje, finger, www, link, kerberos, supdup, hostnames, iso-tsap, csnet-ns, 3com-tsmux, rtelnet, pop-2, pop-3, sunrpc, auth, sftp, uucp-path, nntp, rtp, netbios-ns, netbios-dgm, netbios-ssn, imap2, smtp, smtp-trap, smtp-man, smtp-agent, xdmcp, nextstep, bgp, prospero, irc, smux, at-rmmp, at-nbnp, at-echo, at-zis, qmtp, z3950, ipx, imap3, ulistserv, https, snmp, saft, npmp-local, npmp-gui, and hmmp-ind.
- `dst_port` is the UDP/TCP two-byte destination port (for example, telnet, 23) or “any.” The controller supports the same strings as those for the `src_port`.

**debug packet logging acl eoip-eth** `rule_index action dst src type vlan`

**debug packet logging acl eoip-ip** `rule_index action src dst proto src_port dst_port`

**debug packet logging acl lwapp-dot11** `rule_index action dst src bssid snap_type`

where
- `bssid` is the Basic Service Set Identifier.
- `snap_type` is the Ethernet type.

**debug packet logging acl lwapp-ip** `rule_index action src dst proto src_port dst_port`

---

**Note** To remove all configured ACLs, enter `debug packet logging acl clear-all` command.
**Step 3**

To configure the format of the debug output, enter this command:

```
debug packet logging format {hex2pcap | text2pcap}
```

The debug facility supports two output formats: `hex2pcap` and `text2pcap`. The standard format used by IOS supports the use of `hex2pcap` and can be decoded using an HTML front end. The `text2pcap` option is provided as an alternative so that a sequence of packets can be decoded from the same console log file. Figure 18-12 shows an example of `hex2pcap` output, and Figure 18-13 shows an example of `text2pcap` output.

**Figure 18-12 Sample Hex2pcap Output**

```
x len=118, encap=n/a, port=1
[0000]: 00c31e8 7fe0000 c5400000 0000500 ..in.....0...E.
[0010]: 0060000 4001008 5e0e164 6e0e164 .h...0...>..dl...d
[0020]: 0000000 0000000 0000000 0000000 1...Ye....
[0030]: 0000000 0000000 0000000 0000000 0000000 ............
[0040]: 181f32b1 2232a25 24274a29 2a2e2c2d ..."#&*"(*)*+-,-
[0050]: 222f3031 32333435 36373839 3a3e3c3d ./0123456789;<=
[0060]: 303f4041 42434445 46474849 4a4b4c4d ?>#ABCDFGHIJKLMNOP
[0070]: 4e4f5051 5253 NOPQRS
```

`tx len=118, encap=n/a, port=1`

**Figure 18-13 Sample Text2pcap Output**

```
x len=118, encap=n/a, port=1
[0000] 00 0c 31 6e 7f 80 00 0e 65 40 08 c0 08 00 45 00 ..in.....0...E.
[0010] 00 60 00 00 40 00 40 01 6f de 01 64 6c de 01 64 .h...0...>..dl...d
[0020] 00 60 01 08 00 00 00 65 00 00 00 00 00 00 l...Ye....
[0030] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 l...Ye....
[0040] 18 1f 2f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d ..."#&*"(*)*+-,-
[0050] 22 2f 30 31 32 33 34 35 36 37 38 39 3a 3e 3c 3d ./0123456789;<=
[0060] 30 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d ?>#ABCDFGHIJKLMNOP
[0070] 4e 4f 50 51 52 53 NOPQRS
```

**Step 4**

To determine why packets might not be displayed, enter this command:

```
debug packet error {enable | disable}
```

**Step 5**

To display the status of packet debugging, enter this command:

```
show debug packet
```
Information similar to the following appears:

Status........................................... disabled
Number of packets to display..................... 25
Bytes/packet to display.......................... 0
Packet display format............................ text2pcap

Driver ACL:
  [1]: disabled
  [2]: disabled
  [3]: disabled
  [4]: disabled
  [5]: disabled
  [6]: disabled

Ethernet ACL:
  [1]: disabled
  [2]: disabled
  [3]: disabled
  [4]: disabled
  [5]: disabled
  [6]: disabled

IP ACL:
  [1]: disabled
  [2]: disabled
  [3]: disabled
  [4]: disabled
  [5]: disabled
  [6]: disabled

EoIP-Ethernet ACL:
  [1]: disabled
  [2]: disabled
  [3]: disabled
  [4]: disabled
  [5]: disabled
  [6]: disabled

EoIP-IP ACL:
  [1]: disabled
  [2]: disabled
  [3]: disabled
  [4]: disabled
  [5]: disabled
  [6]: disabled

LWAPP-Dot11 ACL:
  [1]: disabled
  [2]: disabled
  [3]: disabled
  [4]: disabled
  [5]: disabled
  [6]: disabled

LWAPP-IP ACL:
  [1]: disabled
  [2]: disabled
  [3]: disabled
  [4]: disabled
  [5]: disabled
  [6]: disabled
Configuring Wireless Sniffing

This section contains the following topics:

- Information About Wireless Sniffing, page 18-47
- Guidelines and Limitations, page 18-28
- Prerequisites for Wireless Sniffing, page 18-47
- Configuring Sniffing on an Access Point (GUI), page 18-48
- Configuring Sniffing on an Access Point (CLI), page 18-49

Information About Wireless Sniffing

The controller enables you to configure an access point as a network “sniffer,” which captures and forwards all the packets on a particular channel to a remote machine that runs packet analyzer software. These packets contain information on time stamps, signal strength, packet sizes, and so on. Sniffers allow you to monitor and record network activity and to detect problems.

Guidelines and Limitations

- Supported third-party network analyzer software applications are as follows:
  - Wildpackets Omnipeek or Airopeek
  - AirMagnet Enterprise Analyzer
  - Wireshark
- The latest version of Wireshark can decode the packets by going to the Anaylze mode. Select decode as, and switch UDP5555 to decode as AIROPEEK.
- You must disable IP-MAC address binding in order to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller, or a controller network module that runs software release 6.0 or later releases. To disable IP-MAC address binding, enter the config network ip-mac-binding disable command in the controller CLI. For more information, see the “Configuring IP-MAC Address Binding” section on page 4-64.
- You must enable WLAN 1 in order to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller, or a controller network module that runs software release 6.0 or later releases. If WLAN 1 is disabled, the access point cannot send packets.

Prerequisites for Wireless Sniffing

To perform wireless sniffing, you need the following hardware and software:

- A dedicated access point—An access point configured as a sniffer cannot simultaneously provide wireless access service on the network. To avoid disrupting coverage, use an access point that is not part of your existing wireless network.
- A remote monitoring device—A computer capable of running the analyzer software.
- Windows XP or Linux operating system—The controller supports sniffing on both Windows XP and Linux machines.
Configuring Sniffing on an Access Point (GUI)

Step 1
Choose Wireless > Access Points > All APs to open the All APs page.

Step 2
Click the name of the access point that you want to configure as the sniffer. The All APs > Details for page appears.

Figure 18-14  All APs > Details for Page

Step 3
From the AP Mode drop-down list, choose Sniffer.

Step 4
Click Apply to commit your changes.

Step 5
Click OK when warned that the access point will be rebooted.

Step 6
Choose Wireless > Access Points > Radios > 802.11a/n (or 802.11b/g/n) to open the 802.11a/n (or 802.11b/g/n) Radios page.

Step 7
Hover your cursor over the blue drop-down arrow for the desired access point and choose Configure. The 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page appears.

Step 8
Select the Sniff check box to enable sniffing on this access point, or leave it unselected to disable sniffing. The default value is unchecked.

Step 9
If you enabled sniffing in Step 8, follow these steps:

a. From the Channel drop-down list, choose the channel on which the access point sniffs for packets.

b. In the Server IP Address text box, enter the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark.

Step 10
Click Apply to commit your changes.

Step 11
Click Save Configuration to save your changes.
Configuring Sniffing on an Access Point (CLI)

Step 1  To configure the access point as a sniffer, enter this command:

```plaintext
config ap mode sniffer Cisco_AP
```
where `Cisco_AP` is the access point configured as the sniffer.

Step 2  When warned that the access point will be rebooted and asked if you want to continue, enter `Y`. The access point reboots in sniffer mode.

Step 3  To enable sniffing on the access point, enter this command:

```plaintext
config ap sniff {802.11a | 802.11b} enable channel server_IP_address Cisco_AP
```
where
- `channel` is the radio channel on which the access point sniffs for packets. The default values are 36 (802.11a/n) and 1 (802.11b/g/n).
- `server_IP_address` is the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark.
- `Cisco_AP` is the access point configured as the sniffer.

**Note**  To disable sniffing on the access point, enter the `config ap sniff {802.11a | 802.11b} disable Cisco_AP` command.

Step 4  To save your changes, enter this command:

```plaintext
save config
```

Step 5  To view the sniffer configuration settings for an access point, enter this command:

```plaintext
show ap config {802.11a | 802.11b} Cisco_AP
```
Information similar to the following appears:

```
Cisco AP Identifier.......................... 17
Cisco AP Name................................. AP131:46f2.98ac
... 
AP Mode ........................................ Sniffer
Public Safety .................................. Global: Disabled, Local: Disabled
Sniffing ........................................ No
... 
```

Troubleshooting Access Points Using Telnet or SSH

This section contains the following topics:

- Information About Troubleshooting Access Points Using Telnet or SSH, page 18-50
- Guidelines and Limitations, page 18-50
- Troubleshooting Access Points Using Telnet or SSH (GUI), page 18-50
- Troubleshooting Access Points Using Telnet or SSH (CLI), page 18-51
Information About Troubleshooting Access Points Using Telnet or SSH

The controller supports the use of the Telnet and Secure Shell (SSH) protocols to troubleshoot lightweight access points. Using these protocols makes debugging easier, especially when the access point is unable to connect to the controller.

- To avoid potential conflicts and security threats to the network, the following commands are unavailable while a Telnet or SSH session is enabled: `config terminal`, `telnet`, `ssh`, `rsh`, `ping`, `traceroute`, `clear`, `clock`, `crypto`, `delete`, `fsck`, `lwapp`, `mkdir`, `radius`, `release`, `reload`, `rename`, `renew`, `rmdir`, `save`, `set`, `test`, `upgrade`.

- Commands available during a Telnet or SSH session include `debug`, `disable`, `enable`, `help`, `led`, `login`, `logout`, `more`, `no debug`, `show`, `systat`, `undebug`, and `where`.

Note

For instructions on configuring Telnet or SSH sessions on the controller, see the “Configuring Telnet and SSH Sessions” section on page 3-35.

Guidelines and Limitations

You can configure Telnet or SSH by using the controller CLI in software release 5.0 or later releases or using the controller GUI in software release 6.0 or later releases.

Troubleshooting Access Points Using Telnet or SSH (GUI)

Step 1  Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2  Click the name of the access point for which you want to enable Telnet or SSH.

Step 3  Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.
Step 4 Select the Telnet check box to enable Telnet connectivity on this access point. The default value is unchecked.

Step 5 Select the SSH check box to enable SSH connectivity on this access point. The default value is unchecked.

Step 6 Click Apply to commit your changes.

Step 7 Click Save Configuration to save your changes.

Troubleshooting Access Points Using Telnet or SSH (CLI)

Step 1 To enable Telnet or SSH connectivity on an access point, enter this command:

```
config ap {telnet | ssh} enable Cisco_AP
```

The default value is disabled.

Note To disable Telnet or SSH connectivity on an access point, enter the `config ap {telnet | ssh} disable Cisco_AP` command.

Step 2 To save your changes, enter this command:

```
save config
```

Step 3 To see whether Telnet or SSH is enabled on an access point, enter this command:

```
show ap config general Cisco_AP
```

Information similar to the following appears:

```
Cisco AP Identifier.............................. 5
Cisco AP Name.................................... AP33
Country code..................................... Multiple Countries:US,AE,AR,AT,AU,BH
```
Debugging the Access Point Monitor Service

This section contains the following topics:

- Information About Debugging the Access Point Monitor Service, page 18-52
- Debugging Access Point Monitor Service Issues (CLI), page 18-52

Information About Debugging the Access Point Monitor Service

The controller sends access point status information to the Cisco 3300 Series Mobility Services Engine (MSE) using the access point monitor service.

The MSE sends a service subscription and an access point monitor service request to get the status of all access points currently known to the controller. When any change is made in the status of an access point, a notification is sent to the MSE.

Debugging Access Point Monitor Service Issues (CLI)

If you experience any problems with the access point monitor service, enter this command:

dbg service ap-monitor {all | error | event | nmsp | packet} {enable | disable}

where

- all configures debugging of all access point status messages.
- error configures debugging of access point monitor error events.
- event configures debugging of access point monitor events.
- nmsp configures debugging of access point monitor NMSP events.
- packet configures debugging of access point monitor packets.
- enable enables the debug service ap-monitor mode.
- disable disables the debug service ap-monitor mode.
Troubleshooting OfficeExtend Access Points

This section contains the following topics:

- Information About Troubleshooting OfficeExtend Access Points, page 18-53
- Troubleshooting Common Problems, page 18-53

Information About Troubleshooting OfficeExtend Access Points

This section provides troubleshooting information if you experience any problems with your OfficeExtend access points.

Interpreting OfficeExtend LEDs

The LED patterns are different for 1130 series and 1140 series OfficeExtend access points. See the Cisco OfficeExtend Access Point Quick Start Guide for a description of the LED patterns. You can find this guide at this URL:


Positioning OfficeExtend Access Points for Optimal RF Coverage

When positioning your OfficeExtend access point, consider that its RF signals are emitted in a cone shape spreading outward from the LED side of the access point. Be sure to mount the access point so that air can flow behind the metal back plate and prevent the access point from overheating.

Troubleshooting Common Problems

Most of the problems experienced with OfficeExtend access points are one of the following:

- The access point cannot join the controller because of network or firewall issues.

  Resolution: Follow the instructions in the “Viewing Access Point Join Information (GUI)” section on page 9-40 to view join statistics for the OfficeExtend access point, or find the access point’s public IP address and perform pings of different packet sizes from inside the company.
• The access point joins but keeps dropping off. This behavior usually occurs because of network problems or when the network address translation (NAT) or firewall ports close because of short timeouts.

**Resolution:** Ask the teleworker for the LED status.

• Clients cannot associate because of NAT issues.

Resolution: Ask the teleworker to perform a speed test and a ping test. Some servers do not return big packet pings.

• Clients keep dropping data. This behavior usually occurs because the home router closes the port because of short timeouts.

Resolution: Perform client troubleshooting in WCS to determine if the problem is related to the OfficeExtend access point or the client.

• The access point is not broadcasting the enterprise WLAN.

**Resolution:** Ask the teleworker to check the cables, power supply, and LED status. If you still cannot identify the problem, ask the teleworker to try the following:

- Connect to the home router directly and see if the PC is able to connect to an Internet website such as http://www.cisco.com/. If the PC cannot connect to the Internet, check the router or modem. If the PC can connect to the Internet, check the home router configuration to see if a firewall or MAC-based filter is enabled that is blocking the access point from reaching the Internet.

- Log on to the home router and check to see if the access point has obtained an IP address. If it has, the access point’s LED normally blinks orange.

• The access point cannot join the controller, and you cannot identify the problem.

**Resolution:** A problem could exist with the home router. Ask the teleworker to check the router manual and try the following:

- Assign the access point a static IP address based on the access point’s MAC address.

- Put the access point in a demilitarized zone (DMZ), which is a small network inserted as a neutral zone between a company’s private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.

- If problems still occur, contact your company’s IT department for assistance.

• The teleworker experiences problems while configuring a personal SSID on the access point.

**Resolution:** Clear the access point configuration and return it to the factory-default settings by clicking Clear Config on the access point GUI or by entering the clear ap config Cisco_AP command and then follow the steps in the “Configuring a Personal SSID on an OfficeExtend Access Point” section on page 9-67 to try again. If problems still occur, contact your company’s IT department for assistance.

• The home network needs to be rebooted.

**Resolution:** Ask the teleworker to follow these steps:

a. Leave all devices networked and connected, and then power down all the devices.

b. Turn on the cable or DSL modem, and then wait for 2 minutes. (Check the LED status.)

c. Turn on the home router, and then wait for 2 minutes. (Check the LED status.)

d. Turn on the access point, and then wait for 5 minutes. (Check the LED status.)

e. Turn on the client.
Troubleshooting Mesh Access Points

Mesh MAP Backhaul Deselection on Ethernet Backhaul at Runtime

When a mesh access point that joined the controller uses radio backhaul with the intent to use Ethernet as mesh backhaul, an inappropriate operation sequence could occur, when you enter the flapping mac-address.

**Note**

This troubleshooting tip is not applicable if Ethernet is not used for mesh AP backhaul.

To configure a mesh map Ethernet port (on the same subnet or VLAN of the Mesh RAP) as the mesh backhaul at runtime, follow these steps:

**Step 1**

Choose Configure > Access Points > All APs > select the AP name, click on Reset AP Now to reset mesh AP.

**Step 2**

Connect the Ethernet cable between the switch and the mesh AP.
Numerics

11n Mode parameter 4-28
1250 series access points
and PoE Status field 8-112
operating modes when using PoE 8-110
transmit power settings when using PoE 8-111
3DES IPSec data encryption 6-9
7920 AP CAC parameter 7-48
7920 Client CAC parameter 7-48
7920 support mode
configuring 7-47
described 7-47
7921 support mode 7-47
802.11a (or 802.11b) > Client Roaming page 4-60
802.11a (or 802.11b) > Voice Parameters page 4-74, 4-78, 4-84
802.11a (or 802.11b/g) > EDCA Parameters page 4-88
802.11a (or 802.11b/g) Global Parameters > Auto RF page 12-31
802.11a (or 802.11b/g) Global Parameters page 4-23, 12-45
802.11a (or 802.11b/g) Network Status parameter 4-24, 4-32, 4-33
802.11a/n (4.9 GHz) > Configure page 9-126
802.11a/n (or 802.11b/g/n) Cisco APs > Configure page 12-34
802.11a/n (or 802.11b/g/n) Radios page 4-80, 12-33
802.11a/n Radios page (from Monitor Menu) 8-14
802.11a/n Radios page (from Wireless Menu) 8-15
802.11a > RRM > Coverage page 12-15
802.11a > RRM > DCA page 12-11
802.11a > RRM > Dynamic Channel Assignment (DCA) page 12-11
802.11a > RRM > General page 12-16
802.11b/g/n Cisco APs > Configure page 8-98
802.11g Support parameter 4-24
802.11h, described 4-32
802.11h Global Parameters page 4-32
802.11n
   clients 8-116
   devices 4-27
802.11n (2.4 GHz) High Throughput page 4-28
802.1Q VLAN trunk port 3-4
802.1X
   configuring 7-28
   described 7-29
   dynamic key settings 7-28
802.1X+CCKM
   configuring 7-31
   described 7-30
802.1X authentication for access points
   configuring
      the switch 8-26
      using the CLI 8-24 to 8-26
   described 8-21
802.1x Authentication parameter 8-23
802.3 bridging
   configuring using the CLI 4-51
   configuring using the GUI 4-49 to 4-51
802.3 Bridging parameter 4-51
802.3 frames 4-50
802.3X flow control, enabling 4-49

A

Access Control List Name parameter 6-58
access control lists (ACLs)
   applying to a WLAN
      using the CLI 6-65
   applying to the controller CPU
      using the CLI 6-65
   configuring
      using the CLI 6-63 to 6-65
   counters
      configuring using the CLI 6-64
      configuring using the GUI 6-57
   described 6-56, 15-16
rules 6-56, 6-58, 6-64, 15-16, 15-17
Access Control Lists > Edit page 6-59, 15-19
Access Control Lists > New page 6-58
Access Control Lists page 6-57
Access Mode parameter 4-39, 4-41
access point
  assisted roaming, described 9-89
access point count, approved tiers for 5500 series controllers 4-4
access point event logs, viewing A-16
access point groups
  assigning access points to
    using the CLI 7-75
    using the GUI 7-74
  creating
    using the CLI 7-75
default group 7-72
  illustrated 7-71
  removing
    using the CLI 7-75
    using the GUI 7-73
  viewing 7-75 to 7-76
access point monitor service, debugging A-52
access point radios, searching for 8-14 to 8-16
access points
  20-MHz channelization 12-34
  40-MHz channelization 12-34
  assisted roaming 4-59
  authorization list 8-36
  authorizing
    using LSCs 8-31 to 8-35
    using MICs 8-31
    using SSCs 8-30
  converting to mesh access points 9-122
  embedded 8-26
  LEDs
    configuring 8-114
    interpreting A-2
  migrating from the -J regulatory domain to the -U regulatory domain 8-93 to 8-95
  number supported per controller 3-4
priming 8-8
supporting oversized images 8-51
troubleshooting
  the join process 8-38 to 8-43
  using Telnet or SSH A-50 to A-52
VCI strings 8-37
verifying that they join the controller 8-8
viewing join information
  using the CLI 8-41 to 8-42
  using the GUI 8-40 to 8-41
Accounting Server parameters 7-85
ACL. See access control lists (ACLs)
ACL Name parameter 6-60, 6-61
ACS server configuration page 7-83
Action parameter 6-59, 15-19
active exploits 6-130
Add AAA Client page (on CiscoSecure ACS) 6-5, 6-20
Add AP button 15-23
Adding Mesh APs to the Controller Filter (GUI) 9-20
Add New Rule button 6-58
Add Web Server button 11-21
AdHoc Rogue AP parameter 6-85
administrator access 4-36
Admin Status parameter 3-24
Admission Control (ACM) parameter 4-75, 4-78
AES CBS IPSec data encryption 6-9
AES-CCMP 7-29
AES parameter 7-31
Aggregated MAC Protocol Data Unit (A-MPDU) 4-30
Aggregated MAC Service Data Unit (A-MSDU) 4-30
aggregation method, specifying 4-30
AirMagnet Enterprise Analyzer A-47
Aironet IE parameter 7-68
Airopeek A-47
Alarm Trigger Threshold parameter 12-42
All APs > Access Point Name > Link Details > Neighbor Name page 9-120
All APs > Access Point Name > Mesh Neighbor Stats page 9-120
All APs > Access Point Name > Neighbor Info page 9-119
All APs > Access Point Name > Statistics page 9-114
All APs > Access Point Name > VLAN Mappings page 15-13
All APs > Details for (Advanced) page 8-5, 8-46, A-51
    configuring link latency 8-106
    configuring PoE 8-112
All APs > Details for (Credentials) page 8-18, 8-23
All APs > Details for (FlexConnect) page 15-12
All APs > Details for (General) page 8-49, 15-12
All APs > Details for (High Availability) page 8-79, 8-83
All APs > Details for page A-48, A-53
All APs > Details page 9-22, 9-44, 9-76, 12-42
All APs page 8-9, 9-113, 9-118, 12-41, 15-12
AnchorTime parameter 9-62, 12-12
anonymous local authentication bind method 6-33, 6-34
Anonymous Provision parameter 6-41
Antenna Gain parameter 12-36
Antenna parameter 12-36
Antenna Type parameter 12-35
AP > Clients > Traffic Stream Metrics page 4-80
AP801 access point
    described 8-26
    using with a controller 8-27
AP Authentication Policy page 6-68, 12-42
AP Core Dump parameter 8-46
ap-count evaluation licenses, activating
    using the CLI 4-14 to 4-15
    using the GUI 4-12 to 4-14
AP Ethernet MAC Addresses parameter 8-33
AP Failover Priority parameter 8-83
AP Group Name parameter 7-73
AP Groups > Edit (APs) page 7-74
AP Groups > Edit (WLANs) page 7-92
AP Groups page 7-73, 7-91
AP Join Stats page 8-40
AP local authentication
    Using GUI 15-15
AP Local Authentication on a WLAN
    Using the CLI 15-15
AP-manager interface
    and dynamic interfaces 3-21
configuring
  using the GUI  3-6 to 3-8
described  3-10
illustration
  of four AP-manager interfaces  3-42
  of three AP-manager interfaces  3-40
  of two AP-manager interfaces  3-41
AP Mode parameter  8-62, 12-42, 15-12, A-48
AP Name parameter  7-74
Applying ACLs to a WLAN  6-61
Applying ACLs to the controller CPU  6-61
AP Policies page  8-35
AP Primary Discovery Timeout parameter  8-79, 9-25
ASLEAP detection  6-130
Assigning Channel and TPC Settings (GUI)  12-33
asymmetric tunneling
  described  14-24
  illustrated  14-25
authenticated local authentication bind method  6-33, 6-34
Authentication Protocol parameter  4-41
Auth Key Mgmt parameter  7-31
Authority ID Information parameter  6-41, 15-25, 15-26
Authority ID parameter  6-41, 15-24
Authorize LSC APs against auth-list parameter  8-35
Authorize MIC APs against auth-list or AAA parameter  8-35
auto-anchor mobility
  configuring
    using the GUI  14-20 to 14-21
  overview  14-19 to 14-20
auto-immune feature  6-109
AutoInstall
  described  2-26, 2-29
  example operation  2-29
  obtaining
    DHCP addresses for interfaces  2-27
    TFTP server information  2-27
    selecting configuration file  2-28
    using  2-26
Average Data Rate parameter  4-65, 4-69
Average Real-Time Rate parameter 4-65, 4-69
Avoid Cisco AP Load parameter 9-62, 12-12
Avoid Foreign AP Interference parameter 9-62, 12-12, 14-18
Avoid Non-802.11a (802.11b) Noise parameter 9-62, 12-12

B

Backhaul Client Access parameter 9-33, 9-125
backup controllers
configuring
using the CLI 9-28
using the GUI 9-24 to 9-26
described 8-77, 9-23
Back-up Primary Controller IP Address parameter 8-79, 9-25
Back-up Primary Controller Name field 8-79, 9-25
Back-up Secondary Controller IP Address parameter 8-79, 9-25
Back-up Secondary Controller Name parameter 8-79, 9-25
bandwidth-based CAC
described 4-72
enabling
using the CLI 4-77
using the GUI 4-75
for mesh networks 9-91
Base MAC Address parameter 3-29
Beacon Period parameter 4-24
Bind Password parameter 6-33
Bind Username parameter 6-33
bridge protocol data units (BPDUs) 3-27
browsers supported 2-17
Buffered Log Level parameter A-11
Burst Data Rate parameter 4-65, 4-69
Burst Real-Time Rate parameter 4-65, 4-69

C

CAC
configuring for 7920 phones 7-47
described 4-72
enabling
  using the CLI  4-79
  using the GUI  4-78
in mesh networks  9-91
viewing in mesh networks  9-98 to 9-100
viewing using the CLI  4-81
capacity adder license. See licenses
CAPWAP
  and mesh access points  9-11
cascading  12-27
CA Server URL parameter  8-32
Catalyst 3750G Integrated Wireless LAN Controller Switch
  ports  3-2, 3-4
CCKM
  configuring  7-31
  described  7-29
  FlexConnect groups  15-21
  with mobility  14-7
CCX
  configuring Aironet IEs
    using the CLI  7-70
  described  7-67
  link test  8-103
  viewing a client’s version
    using the CLI  7-70
    using the GUI  7-68 to 7-70
CCX Layer 2 client roaming
  configuring
    using the CLI  4-61
  debugging using the CLI  4-62
  described  4-59 to 4-60
  obtaining information using the CLI  4-62
CCX radio management
  features  12-44
  flexconnect considerations  12-44
CCX Radio Management (GUI)  12-45
CCXv5 clients
  enabling location presence  4-113
  troubleshooting  4-28 to A-42
CCXv5 Req button  A-34
CCX Version parameter  7-69
CDP > AP Neighbors > Detail page  4-97
CDP > Global Configuration page  4-94
CDP > Interface Neighbors > Detail page  4-97
CDP > Interface Neighbors page  4-96
CDP > Traffic Metrics page  4-98
CDP Advertisement Version parameter  4-94
CDP AP Neighbors page  4-97
CDP Protocol Status parameter  4-94
CDP State parameter  4-95
Certificate Authority (CA) certificates downloading
  using the CLI  10-24 to 10-25
  using the GUI  10-23
overview  10-22
  using with local EAP  6-38, 6-42
Certificate File Name parameter  11-8
Certificate File Path parameter  11-8
Certificate Issuer parameter  6-41
Certificate Password parameter  10-20, 11-8
Certificate Type parameter  8-35
Change Filter link  8-10, 8-15, 8-41
Change Rules Priority parameter  6-92
Channel Announcement parameter  4-33
Channel Assignment Leader parameter  9-62, 12-13
Channel Assignment Method parameter  9-61, 12-11
cost channel bonding in the 5-GHz band  12-35
Channel parameter  12-33, A-48
Channel Quiet Mode parameter  4-33
channels
  statically assigning using the CLI  12-37
Channel Scan Duration parameter  12-17
Channel Width Parameter  12-12
Channel Width parameter  9-62, 12-34
Check Against CA Certificates parameter  6-41
Check Certificate Date Validity parameter  6-41
chokepoints for RFID tag tracking  4-102
CIDS Sensor Add page  6-107
CIDS Shun List page 6-108

ciphers
  configuring 7-31, 7-32
  described 7-30
Cisco 2500 Series Controller 1-7
Cisco 28/37/38xx Integrated Services Router
  ports 3-2, 3-3, 4-114
  using 4-114
Cisco 3200 Series Mobile Access Router (MAR)
  described 9-124 to 9-125
  operating with mesh access points
    using the CLI to configure 9-126 to 9-127
    using the GUI to configure 9-125 to 9-126
Cisco 3300 Series Mobility Services Engine (MSE), using with wIPS 6-121
Cisco 4400 Series Wireless LAN Controllers
  AutoInstall interfaces 2-27
  described 1-8
Cisco 5500 Series Wireless LAN Controllers
  CPUs A-6
  described 1-8
  interface configuration example 3-45
  licenses. See licenses
  models 3-3
  multiple AP-manager interfaces 3-44 to 3-45
  ports 3-2, 3-3
    using the USB console port 3-32 to 3-33
Cisco 7920 Wireless IP Phones 7-47
Cisco 7921 Wireless IP Phones 7-47
Cisco Adaptive Wireless Path Protocol (AWPP) 9-11
Cisco AV-pairs 7-81, 7-82, 7-83
Cisco Centralized Key Management (CCKM). See CCKM
Cisco Clean Access (CCA) 7-87
Cisco CleanAir 13-1
Cisco Discovery Protocol (CDP)
  configuring
    using the CLI 4-95 to 4-96
    using the GUI 4-93 to 4-95
  described 4-91
  enabling using the GUI 4-94 to 4-95
sample network  4-93
supported devices  4-91
viewing neighbors
    using the CLI  4-98 to 4-99
    using the GUI  4-96 to 4-98
viewing traffic information
    using the CLI  4-98
    using the GUI  4-98
Cisco Discovery Protocol parameter  4-94
Cisco License Manager (CLM)
    and the controller license agent  4-20
    using to register PAKs  4-5
Cisco Licensing website  4-16
Cisco Logo parameter  11-13
Cisco NAC Appliance  7-87
CiscoSecure Access Control Server (ACS)  6-4
Cisco Spectrum Intelligence  13-25
Cisco Unified Wireless Network (UWN) Solution
    described  1-1 to 1-4
    illustrated  1-2
Cisco Wireless Control System (WCS)  1-2
Cisco WiSM
    ports  3-3
    SSC key-hash  8-29
CKIP
    described  7-35
CleanAir Benefits  13-2
CleanAir guidelines  13-5
Clear Config button  8-69
clear configuration
    AP  8-69
Clear Filter link  7-8, 8-12, 8-16, 8-41
Clear Stats button  14-18
Clear Stats on All APs button  8-41
CLI
    basic commands  2-25
    enabling wireless connections  2-38
    logging into  2-23 to 2-25
    logging out  2-25
navigating 2-25
troubleshooting commands A-8 to A-9
using 2-22 to 2-26
Client Certificate Required parameter 6-41
Client Exclusion Policies page 6-73
client location, using WCS 1-7
client MFP 6-66 to 6-67
Client Protection parameter 6-70
client reporting
described A-33
Client Reporting page A-35
client roaming, configuring 4-57 to 4-62
clients
connecting to WLANs 15-15
viewing
using the CLI 8-119
using the GUI 8-115 to 8-119
viewing CCX version
using the CLI 7-70
using the GUI 7-68 to 7-70
Clients > AP > Traffic Stream Metrics page 4-80
Clients > Detail page
configuring client reporting A-34
viewing a client’s CCX version 7-69
viewing client details 8-74, 8-118
viewing the status of workgroup bridges 8-74
Clients page
performing a link test 8-104
viewing clients 8-115
viewing the status of workgroup bridges 8-74
viewing voice and video settings 4-80
Client Type parameter 8-74
Commands > Reset to Factory Defaults page 4-115
comma-separated values (CSV) file, uploading 15-24
Community Name parameter 4-39
conditional web redirect 7-81
described 7-81
Conditional Web Redirect parameter 7-84
Configuration File Encryption parameter 10-31
configuration files
  downloading
    using the CLI 10-32 to 10-33
    using the GUI 10-32
  editing 10-34
  uploading
    using the CLI 10-31
configuration wizard
  CLI version 2-14 to 2-16
  described 2-1
Configuration Wizard - 802.11 Configuration page 2-11
Configuration Wizard Completed page 2-13
Configuration Wizard - Management Interface Configuration page 2-6
Configuration Wizard - Miscellaneous Configuration page 2-7
Configuration Wizard - Service Interface Configuration page 2-5
Configuration Wizard - Set Time page 2-12
Configuration Wizard - SNMP Summary page 2-4, 2-6
Configuration Wizard - System Information page 2-3
Configuration Wizard - Virtual Interface Configuration page 2-8
Configure 13-1
Configure Dynamic Anchoring of Static IP Clients
  Using the CLI 14-30
Configure option for RRM override 12-33
Configure RF Group
  Using CLI 12-7
Configure RF Group Mode
  Using GUI 12-6
Configuring ACLs - GUI 6-57
Configuring a Spectrum Expert 13-24
Configuring CCX Client Roaming (GUI) 4-60
Configuring Cisco CleanAir
  Using the GUI 13-5
Configuring Cisco CleanAir
  Using the CLI 13-8
Configuring Client Exclusion Policies (CLI) 6-73
Configuring Client Exclusion Policies (GUI) 6-73
configuring ClientLink (CLI) 9-16
Configuring Client Reporting (CLI) A-36
Configuring Client Reporting (GUI) A-33
Configuring Controller (GUI) 2-2
Configuring Country Codes (CLI) 8-90
Configuring Country Codes (GUI) 8-88
Configuring Coverage Hole Detection on a WLAN (GUI) 7-86
Configuring Debut Facility A-43
Configuring Dynamic Anchoring of Static IP Clients
   Using the GUI 14-30
Configuring Ethernet VLAN Tagging (GUI) 9-75
Configuring FlexConnect APs using the CLI. 15-14
Configuring Sniffing on an Access Point
   Using the GUI A-48
Configuring Web Redirect (GUI) 7-84
Console Log Level parameter A-11
Control and Provisioning of Wireless Access Points protocol (CAPWAP) 1-5
   debugging 8-7
   described 8-2
   guidelines 8-2
   viewing MTU information 8-6
controller failure detection time, reducing 8-77
controller network module
   baud rate 3-2
   versions 3-3
controllers
   configuration
      saving 10-34
   connections 1-11
   discovery process 8-7
   multiple-controller deployment 1-3 to 1-4
   overview 1-6 to 1-7
   platforms 1-7 to ??
   single-controller deployment 1-3
   synchronizing with location appliance 4-110
   types of memory 1-12
   upgrading software
      using the CLI 10-10
      using the GUI 10-7
Controller Spanning Tree Configuration page 3-29
Controller Time Source Valid parameter 6-70
Controlling backup controllers (cli) 8-79
Control Path parameter 14-21
core dump files
  described A-20
Core Dump page A-20
Core Dump TFTP Upload A-22
Country Code parameter 8-89
country codes
  described 8-87
  Japanese 8-93
  viewing using the CLI 8-91
Country page 8-88
Coverage Exception Level per AP parameter 12-15
coverage hole detection
  configuring per controller
    using the CLI 12-20
    using the GUI 12-14 to 12-16
  disabling on a WLAN
  described 7-86
coverage hole detection and correction 12-4
Coverage Hole Detection Enabled parameter 7-86
CPU Access Control Lists page 6-61
CPUs, 5500 series controllers A-6
crash files
  uploading
    using the CLI A-19 to A-20
Creating AP Groups- GUI 7-73
Creating Multiple AP-Manager Interfaces (GUI) 3-42
Creating Multiple AP Manager Interfaces - CLI 3-44
Current Channel parameter 12-35
Custom Signatures page 6-115

D
data encryption
  and OfficeExtend access points 8-66
  configuring
    using the CLI 8-6
  for OfficeExtend access points 8-63
data encryption (GUI) 8-5
Data Encryption parameter 8-5, 8-63
Data Path parameter 14-21
Data Rates parameter 4-25
date
    configuring through NTP server 2-30
DCA Channel Sensitivity parameter 9-62, 12-12
DCA Channels parameter 9-63, 12-13
debug commands, sending 8-43
default enable password 8-16
default-group access point group 7-72
Default Mobility Group parameter 14-12
Default Routers parameter 7-17
Delivery Traffic Indication Map (DTIM). See DTIM period
Deny Counters parameter 6-59
Description parameter 6-29, 9-20
Designated Root parameter 3-30
DES IPSec data encryption 6-9
Destination parameter 6-58, 15-18
Destination Port parameter 6-59, 15-18
Detect and Report Ad-Hoc Networks parameter 6-84
device certificates
    downloading
        using the GUI 10-19 to 10-21
        overview 10-19
        using with local EAP 6-38, 6-42
DHCP Addr. Assignment Required parameter 7-15
DHCP Allocated Lease page 7-18
DHCP option 43, in controller discovery process 8-8
DHCP option 82
    configuring
        using the GUI 6-55
        described 6-53
        example 6-54
DHCP Option 82 Remote ID Field Format parameter 6-54
DHCP Parameters page 4-35, 6-54
DHCP proxy
    configuring
        using the CLI 4-35
        using the GUI 4-34 to 4-87
DHCP Scope > Edit page  7-17
DHCP scopes
  described  7-16
DHCP Scopes page  7-16
DHCP server discovery  8-8
DHCP Server IP Addr parameter  7-14
DHCP Server Override parameter  7-14
DHCP servers
  internal  7-12
DHCP Timeout
  configure using GUI  4-35
diagnostic channel
  described  A-28
Diagnostic Channel parameter  A-29
directed roam request  4-59
Direction parameter  6-59
disabled clients, configuring a timeout  7-20
discovery request timer, configuring  8-80, 9-27
distribution system ports  3-3 to 3-4
Diversity parameter  12-36
DNS Domain Name parameter  7-17
DNS IP Address parameter  8-49
DNS Servers parameter  7-17
Domain Name parameter  8-50
domain name server (DNS) discovery  8-8
Download button
  downloading a CA certificate  10-24
  downloading a configuration file  10-32
  downloading a customized web authentication login page  11-23
  downloading a device certificate  10-21
  downloading a signature file  6-114
Download File to Controller page  10-17
  downloading a customized web authentication login page  11-23
  downloading CA certificates  10-23
  downloading configuration files  10-31
  downloading device certificates  10-20
  downloading IDS signatures  6-114
  downloading login banner file  10-16
Download SSL Certificate parameter 11-7
DSCP parameter 6-59, 15-18
DTIM 7-21
DTLS 4-2
DTLS data encryption. See data encryption
DTPC Support parameter 4-24
Dynamic Anchoring for Clients with Static IP Addresses
  Configuring 14-28
dynamic AP management
  for dynamic interface 3-20
  for the management interface 3-9
Dynamic AP Management parameter 3-21
  for dynamic interface 3-18
  for management interface 3-8
dynamic AP-manager interface 3-21
dynamic channel assignment (DCA)
  20-MHz channelization 12-4, 12-12
  40-MHz channelization 12-4, 12-12
  configuring
    using the CLI 12-19 to 12-20
    using the GUI 9-60 to 9-63, 12-10 to 12-14
  described 12-3
  sensitivity thresholds 9-62
dynamic frequency selection 8-96 to 8-97
dynamic interface
  described 3-17
dynamic interface example 3-45
dynamic transmit power control, configuring 4-24
dynamic WEP, configuring 7-28
Dynamic WEP Key Index parameter 6-39

E

EAP-FAST parameter 6-40
EAPOL-Key Max Retries parameter 6-40
EAPOL-Key Timeout parameter 6-39
EAP Profile Name parameter 6-42
EAP-TLS parameter 6-40
EDCA Profile parameter 4-89
Edit QoS Profile page  4-64  
Edit QoS Role Data Rates page  4-69  
Egress Interface parameter  11-32  
Email Input parameter  11-33  
Enable AP Local Authentication parameter  15-24  
Enable Authentication for Listener parameter  4-21  
Enable Check for All Standard and Custom Signatures parameter  6-115  
Enable Controller Management to be accessible from Wireless Clients parameter  6-52  
Enable Counters parameter  6-57  
Enable Coverage Hole Detection parameter  12-15  
Enable CPU ACL parameter  6-61  
Enable Default Authentication parameter  4-21  
Enable DHCP Proxy parameter  4-35  
Enable Dynamic AP Management parameter  3-43  
Enable EAP-FAST Authentication parameter  15-24  
Enable IGMP Snooping parameter  4-54  
Enable LEAP Authentication parameter  15-24  
Enable Least Latency Controller Join parameter  8-64  
Enable Link Latency parameter  8-64, 8-107  
Enable Listener parameter  4-21  
Enable Low Latency MAC parameter  4-89  
Enable LSC on Controller parameter  8-32  
Enable NAT Address parameter  3-7  
Enable Notification parameter  4-21  
Enable OfficeExtend AP parameter  8-63  
Enable passive client  7-96  
Enable Password parameter  8-18  
Enable Server Status parameter  6-33  
Enable Tracking Optimization parameter  8-98  
Encryption Key parameter  7-36  
end-user license agreement (EULA)  4-6, 4-7  
enhanced distributed channel access (EDCA) parameters configuring using the CLI  4-90  
enhanced neighbor list described  4-59, 9-89  
request (E2E)  4-59  
Enter Saved Permission Ticket File Name parameter  4-17  
EoIP port  14-21, 14-27  
epings  14-21, 14-28
error codes, for failed VoIP calls  7-53 to 7-55
Ethernet connection, using remotely  2-24 to 2-25
evaluation licenses
    installed on 5500 series controllers  4-3
event reporting for MFP  6-67
Excessive 802.11 Association Failures parameter  6-73
Excessive 802.11 Authentication Failures parameter  6-73
Excessive 802.1X Authentication Failures parameter  6-73
Excessive Web Authentication Failures parameter  6-73
Expedited Bandwidth parameter  4-75
expedited bandwidth requests
    described  4-72
    enabling
        using the GUI  4-75
Expiration Timeout for Rogue AP and Rogue Client Entries parameter  6-83
Extensible Authentication Protocol (EAP)
    configuring  7-28
    setting local timers  6-42 to 6-43
    timeout and failure counters
        per access point  6-46
        per client  6-46

F

factory default settings
    resetting using the GUI  4-115
failover priority for access points
    configuring
        using the CLI  8-83
        using the GUI  8-82 to 8-83
    described  8-81 to 8-82
    viewing using the CLI  8-84
failover protection  1-13
fake access point detection  6-130
Fallback Mode parameter  6-9
Fast Ethernet port  3-3
fast heartbeat timer
    configuring
        using the CLI  8-80
using the GUI 8-78

described 8-77

fast SSID changing

calculating using the GUI 4-49

fault tolerance 15-5

Federal Information Processing Standards (FIPS) 6-11

File Compression parameter 8-46

File Name to Save Credentials parameter 4-16

file transfers 1-12

File Type parameter

downloading a CA certificate 10-23

downloading a configuration file 10-31

downloading a customized web authentication login page 11-23

downloading a device certificate 10-20

Login Banner 10-17

upgrading controller software 10-6

uploading a configuration file 10-29

uploading packet capture files A-25

uploading PACs 10-26

filter, using to view clients 8-116 to 8-117

Fingerprint parameter 6-108

flashing LEDs, configuring 8-114

FlexConnect

authentication process 15-2 to 15-5

bandwidth restriction 15-3

debugging 15-11, 15-14

illustrated 15-2

FlexConnect groups

backup RADIUS server 15-21

CCKM 15-21

described 15-20

example 15-20

local authentication 15-22

FlexConnect Groups page 15-23

FlexConnect Group Support 15-22

FlexConnect Mode AP Fast Heartbeat Timeout parameter 8-78

FlexConnect parameter 8-62

Forward Delay parameter 3-30

forwarding plane architecture 4-50
G

General (controller) page
  configuring 802.3 bridging  4-51
  configuring an RF group  12-29
  enabling link aggregation  3-37

General (security) page  6-26

General page  6-39

Generate Rehost Ticket button  4-17

gigabit Ethernet port  3-4

Global AP Failover Priority parameter  8-83

Global Configuration page
  configuring backup controllers  8-78, 9-24
  configuring failover priority for access points  8-82
  configuring global credentials for access points  8-18, 8-23, 8-78

global credentials for access points
described  8-16

  overriding
    using the CLI  8-19
    using the GUI  8-18

Global multicast mode  7-95

Group Mode parameter  12-31, 14-17

Group Name parameter  14-12, 15-23

Guest LAN parameter  11-31

guest N+1 redundancy  14-20

guest user accounts
  viewing
    using the CLI  11-6
    using the GUI  11-5

Guest User parameter  6-29

Guest User Role parameter  6-29

guest WLAN, creating  11-5

GUI
  browsers supported  2-17
  enabling wireless connections  2-38
guidelines 2-17
using 2-16
Guidelines and Limitations for Predownloading 10-12

H
Headline parameter 11-13
Hello Time parameter 3-30
help, obtaining 2-17
hex2pcap sample output A-45
Holdtime parameter 3-30, 4-94
Honeypot access point detection 6-130
HTTP Access parameter 2-18
HTTP Configuration page 2-18
HTTPS Access parameter 2-18
Hysteresis parameter 4-61

I
Identity Request Max Retries parameter 6-39
Identity Request Timeout parameter 6-39
IDS sensors
described 6-106
IDS signatures
described 6-111
frequency 6-116
MAC frequency 6-116, 6-118
measurement interval 6-116
pattern 6-116
quiet time 6-116, 6-119
tracking method 6-116
IGMP Snooping 7-96
IGMP Timeout parameter 4-54
IKE Diffie Hellman Group parameter 6-9
IKE Phase 1 parameter 6-9
Index parameter for IDS 6-107
indoor access points
  converting to mesh access points 9-122
infrastructure MFP
  components  6-67
  described  6-66
Infrastructure Protection parameter  6-70
Ingress Interface parameter  11-32
Injector Switch MAC Address parameter  8-112
inline power  8-110
installing a license (GUI)  4-6
Install License button  4-6
inter-controller roaming
  described  4-58
  example  14-2
Interface groups  3-47
Interface Name parameter  7-74, 7-89, 7-92, 9-21
Interface parameter  7-14
interfaces
  overview  3-4 to 3-17
Interfaces > Edit page
  applying an ACL to an interface  6-60
  configuring NAC out-of-band integration  7-90
  creating multiple AP-manager interfaces  3-43
Interfaces > New page  3-17, 3-42
Interfaces page  3-7, 3-11, 3-14, 3-15
interference  12-3
Interferences  13-2
Interference threshold parameter  12-16
Internet Group Management Protocol (IGMP)
  configuring
    using the CLI  4-55
    using the GUI  4-54
  snooping  4-52
inter-release mobility  14-10
inter-subnet mobility  14-7
inter-subnet roaming
  described  4-58
  illustrated  14-3 to 14-4
Interval parameter  9-61, 12-11, 12-46
intra-controller roaming
  described  4-58
illustrated 14-1
Inventory page 8-101
Invoke Channel Update Now button 9-61, 12-11
Invoke Power Update Now button 12-8
IP address-to-MAC address binding
   configuring 4-62 to 4-63
   described 4-63
IP Mask parameter 4-39
IPSec parameter 6-9
IP Theft or IP Reuse parameter 6-73

J
Japanese country codes 8-93
Japanese regulations for migrating access points from the -J to the -U regulatory domain 8-93 to 8-95

K
Keep Alive Count parameter 14-21
Keep Alive Interval parameter 14-21
Key Encryption Key (KEK) parameter 6-8
Key Format parameter 7-36
Key Index parameter 7-36
key permutation
   configuring 7-36, 7-37
   described 7-35
Key Permutation parameter 7-36
Key Size parameter 7-36
Key Wrap Format parameter 6-8
Key Wrap parameter 6-8

L
LAG. See link aggregation (LAG)
LAG Mode on Next Reboot parameter 3-38
Last Auto Channel Assignment parameter 9-62, 12-13
Last Power Level Assignment parameter 12-8
Layer 2
Layer 2 Security parameter 7-31, 7-36, 7-84
Layer 3 operation 1-5
Layer 3 security described 6-3
Layer 3 Security parameter
for web authentication 7-40
for web redirect 7-84
for wired guest access 11-32
LDAP
choosing server priority order 6-33
configuring
using the GUI 6-31 to 6-34
LDAP server
assigning to WLANs 6-34
choosing local authentication bind method
using the CLI 6-34
using the GUI 6-33
LDAP Servers > New page 6-33
LDAP Servers page 6-32
LDAP Servers parameter 6-42
LEAP parameter 6-40
Lease Time parameter 7-17
LEDs
configuring 8-114
interpreting A-2
license agent
described 4-20
License Agent Configuration page 4-21
License Commands (Rehost) page 4-16
License Commands page 4-6
License Detail page 4-8, 4-13
licenses
activating ap-count evaluation licenses
using the CLI 4-14 to 4-15
installing
using the CLI 4-7
obtaining 4-4 to 4-6
rehosting
  described 4-15
  using the GUI 4-15 to 4-17
removing
  using the CLI 4-7
  using the GUI 4-8
required for OfficeExtend access points 8-62
saving
  using the CLI 4-7
  using the GUI 4-6
transferring to a replacement controller after an RMA 4-19 to ??
viewing
  using the CLI 4-9 to 4-12
Licenses page 4-8, 4-12
licensing portal, using to register PAKs 4-5
Lifetime parameter 6-29, 11-4
Lightweight Access Point Protocol (LWAPP) 1-5
lightweight mode, reverting to autonomous mode 8-29
link aggregation (LAG)
  described 3-34 to 3-35
  example 3-34
  illustrated 3-36
link latency
  and OfficeExtend access points 8-64, 8-66
  described 8-106
Link Status parameter 3-24
Link Test
  button 8-104
  option 8-104, 9-119
  page 8-104
  window 9-119
link test
  described 8-103
  performing
    using the CLI 8-105
    using the GUI 8-104 to 8-105, 9-119 to 9-120
types of packets 8-103
Link Trap parameter 3-24, 3-25
Listener Message Processing URL parameter 4-21
Load-based AC parameter 4-75
load-based CAC
   described 4-72
   enabling
      using the GUI 4-75
Lobby Ambassador Guest Management > Guest Users List page 11-3
Local Auth Active Timeout parameter 6-39
local authentication, local switching 15-3
Local Authentication on a WLAN
   using the GUI 15-14
local EAP
   debugging 6-46
      example 6-38
      viewing information using the CLI 6-45
Local EAP Authentication parameter 6-42
Local Management Users > New page 11-2
Local Management Users page 11-2
Local Mode AP Fast Heartbeat Timeout parameter 8-78
Local Mode AP Fast Heartbeat Timer parameter 8-78
Local Net Users > New page 6-28
Local Net Users page 6-28, 11-5
local significant certificate (LSC)
   configuring
      using the CLI 8-33 to 8-35
      using the GUI 8-31 to 8-33
   described 8-31
Local Significant Certificates (LSC) - AP Provisioning page 8-32
Local Significant Certificates (LSC) - General page 8-31
local user database, capacity 11-2
location
   calibration 12-45
   configuring settings using the CLI 4-110 to 4-112
   viewing settings using the CLI 4-112 to 4-114
location appliance
   installing certificate 4-109 to 4-110
   synchronizing with controller 4-110
location-based services 12-45
location presence 4-113
login banner file
clearing 10-18 to 10-19

described 10-16
downloading
  using the CLI 10-17 to 10-18
  using the GUI 10-16 to 10-17
Login Banner page 10-19
logs
  roaming A-39, A-40
  RSNA A-39, A-40 to A-41
  syslog A-39, A-40 to A-41
uploading
  using the GUI A-18 to A-19
long preambles
described 6-47
LWAPP-enabled access points
debug commands 8-43
disabling the reset button 8-48
MAC addresses displayed on controller GUI 8-48
radio core dumps
described 8-43
receiving debug commands from controller 8-43
retrieving radio core dumps 8-43
reverting to autonomous mode 8-29 to 8-30
sending crash information to controller 8-43
uploading
  access point core dumps 8-45 to 8-47
  radio core dumps 8-44 to 8-45

M

MAC address of access point
displayed on controller GUI 8-48
MAC Address parameter 9-20
MAC filtering
  configuring on WLANs 7-19 to 7-20
MAC Filtering page 9-20
MAC Filters > New page 9-20
management frame protection (MFP)
types 6-66
Management Frame Protection parameter 6-70
Management Frame Protection Settings page 6-70
management frame validation 6-67
management interface described 3-6
Management IP Address parameter 8-62
management over wireless described 6-52
Master Controller Configuration page 8-8
Master Controller Mode parameter 8-9
Max Age parameter 3-30
Max HTTP Message Size parameter 4-21
Maximum Age parameter 3-30
maximum local database entries configuring using the GUI 6-26
Maximum Local Database Entries parameter 6-27
Maximum Number of Sessions parameter 4-21
Max-Login Ignore Identity Response parameter 6-39
Max RF Bandwidth parameter 4-75, 4-78
MCS data rates 4-28
Member MAC Address parameter 14-12
memory types 1-12
memory leaks, monitoring A-26 to A-27
mesh network example 9-98
parameters configuring using the CLI 9-55
configuring using the GUI 9-31 to 9-36
statistics viewing for an access point using the CLI 9-117 to 9-118
viewing for an access point using the GUI 9-113 to 9-117
Mesh > LinkTest Results page 9-119
mesh access points and CAPWAP 9-11
converting to non-mesh access points 9-123
models 9-1
network access 9-3
operating with Cisco 3200 Series Mobile Access Routers
configuration guidelines 9-125

described 9-124 to 9-125

using the CLI to configure 9-126

roles 9-2

mesh neighbors, parents, and children 9-11

mesh network hierarchy 9-3

mesh node security statistics 9-116 to 9-117

mesh node statistics 9-115

mesh routing 9-11

Message Authentication Code Key (MACK) parameter 6-8, 6-11

message logs

configuring

using the CLI A-12 to A-15

using the GUI A-9

viewing

using the CLI A-15

using the GUI A-12

See also system logging

Message Logs page A-12

Message parameter for web authentication 11-14

Metrics Collection parameter 4-76

MFP Client Protection parameter 6-69

MIC 7-29, 7-35

migrating access points from the -J to the -U regulatory domain 8-93 to 8-95

Min Failed Client Count per AP parameter 12-15

Minimum RSSI parameter 4-61

mirror mode. See port mirroring, configuring

MMH MIC

configuring 7-36, 7-37

described 7-35

MMH Mode parameter 7-36

Mobile Announce messages 14-7

mobility

failover 14-20

overview 14-1

Mobility Anchor Config page 14-26

Mobility Anchor Create button 14-21

mobility anchors. See auto-anchor mobility

Mobility Anchors option 14-21
Mobility Group Members > Edit All page 14-13

mobility groups
configuring
with one NAT device 14-8
with two NAT devices 14-9
determining when to include controllers 14-7
difference from RF groups 12-26
examples 14-7
illustrated 14-5
messaging among 14-7
number of access points supported 14-5
number of controllers supported 14-5
using with NAT devices 14-7 to 14-9

mobility group statistics
  types 14-16

mobility list
  detecting failed members 14-20
  number of controllers supported 14-7
  ping requests to members 14-20

Mobility Multicast Messaging > Edit page 14-14
Mobility Multicast Messaging page 14-14
mobility ping tests, running 14-27
Mobility Statistics page 14-17
MODE access point button 8-48
Mode parameter 4-60, 12-46
Monitoring 13-19
monitor intervals, configuring using the GUI 12-17
mpings 14-21, 14-28
multicast 4-54
Multicast Appliance Mode parameter 3-25
Multicast Groups page 4-56
multicast mode
described 4-52 to 4-53
Multicast-Multicast mode 7-94
Multicast Optimization 3-49
Multicast page 4-54
Multicast VLAN
  using the GUI 3-50
multiple country codes
configuring
  using the CLI  8-90
  using the GUI  8-89 to 8-90

N

NAC in-band mode  7-88
NAC out-of-band integration
  and FlexConnect  15-6
  guidelines  7-89
NAC out-of-band support
  configuring for a specific access point group
    using the CLI  7-93
    using the GUI  7-91
NAC State parameter  7-74, 7-91, 7-92
NAT address
  for dynamic interface  3-18, 3-20
  for management interface  3-7, 3-9
NAT devices in mobility groups  14-7 to 14-9
Native VLAN ID parameter  15-12
Neighor Discovery Packet  12-25
neighbor information
  viewing for an access point using the CLI  9-121
  viewing for an access point using the GUI  9-118 to 9-121
Neighbor Information option  9-118
Neighbor Packet Frequency parameter  12-17
neighbor statistics
  viewing for an access point using the CLI  9-121
  viewing for an access point using the GUI  9-118 to 9-121
Netbios Name Servers parameter  7-17
Netmask parameter  7-17
Network Mobility Services Protocol (NMSP)  4-101
  debugging  4-108
    modifying the notification interval for clients, RFID tags, and rogues  4-105
    viewing settings  4-105 to 4-108
Network parameter  7-17
NTP server
  configuring to obtain time and date  2-30
Number of Attempts to LSC parameter  8-32
Number of Hits parameter  6-59

O

OfficeExtend Access Point Configuration page  8-68
OfficeExtend Access Point Home page  8-67
OfficeExtend Access Points
   LEDs  A-53
   positioning  A-53
OfficeExtend access points
   and NAT  8-52
configuring
   using the GUI  8-62 to 8-65
described  8-52
firewall requirements  8-61
licensing requirements  8-62
supported access point models  8-52
trap logs  8-62
typical setup  8-52
viewing statistics  8-69 to 8-70
OfficeExtend AP parameter  8-64
online help, using  2-17
operating system
   security  1-4 to 1-5
   software  1-4
Order Used for Authentication parameter  6-10, 6-23
Override Global Config parameter  11-26, 11-33
Over-ride Global Credentials parameter  8-19, 8-24, 8-64
Override Interface ACL parameter  6-62
oversized access point images  8-51
Overview of CleanAir  13-1

P

P2P Blocking parameter  7-26
packet capture files
   described  A-23
   sample output in Wireshark  A-24
uploading
  using the CLI  A-25 to A-26
Params parameter  8-32
Passive clients  7-93
password guidelines  8-23
Password parameter
  for access point authentication  8-23
  for access points  8-18
  for local net users  6-29
  for PACs  10-26
passwords
  viewing in clear text  A-9
path loss measurement (S60), CLI command  4-110
PEAP parameter  6-40
peer-to-peer blocking
  described  7-24
  examples  7-25
permanent licenses, installed on 5500 series controllers  4-3
Personal SSID parameter  8-68
Physical Mode parameter  3-24, 3-25
Physical Status parameter  3-24
ping link test  8-103
ping tests  14-27
pinning  12-27
PMK cache lifetime timer  7-32
PMKID caching  7-32
PoE Status parameter  8-112
Pool End Address parameter  7-17
Pool Start Address parameter  7-17
port mirroring, configuring  3-25 to 3-26
Port Number parameter
  for controller  3-24
  for LDAP server  6-33
  for RADIUS server  6-8
  for TACACS+ server  6-22
  for wired guest access  11-31
Port parameter for IDS  6-107
ports
  configuring  3-23 to 3-31
on 5500 series controllers 3-2, 3-3
on Catalyst 3750G Integrated Wireless LAN Controller Switch 3-2, 3-4
on Cisco 28/37/38xx Series Integrated Services Router 3-2 to 3-3, 4-114, 8-38
on Cisco WiSM 3-3

Ports page 3-23
Power Assignment Leader parameter 12-8
Power Injector Selection parameter 8-112
Power Injector State parameter 8-112
Power Neighbor Count parameter 12-8
Power over Ethernet (PoE)
 configuring using the CLI 8-113
 using the GUI 8-111 to 8-113
described 1-12, 8-110
Power Over Ethernet (PoE) parameter 3-24
Power Threshold parameter 12-8
preauthentication access control list (ACL)
 applying to a WLAN
 using the CLI 6-65
 for external web server 11-20, 15-11
Preauthentication ACL parameter 6-63, 7-84
Predownloading an image 10-10
Primary Controller Name parameter 8-62
Primary Controller parameters 8-62, 8-79, 9-26
Primary RADIUS Server parameter 15-23
priming access points 8-8
Priority Order > Local-Auth page 6-39
Priority Order > Management User page 6-10, 6-23
Priority parameter 3-30
Privacy Protocol parameter 4-41
probe request forwarding, configuring 8-100
probe requests, described 8-100
product authorization key (PAK)
 obtaining for license upgrade 4-4
 registering 4-5
product ID for controller, finding 4-18
product ID of controller, finding 4-16
Profile Details page A-36
Profile Name parameter 7-5, 7-102, 9-20, 11-31
protected access credentials (PACs)
  overview 10-25
  uploading
    using the CLI 10-27 to 10-28
    using the GUI 10-26
    using with local EAP 6-38, 15-24
Protection Type parameter 6-68, 12-42
Protocol parameter 6-58, 15-18
Protocol Type parameter 4-66
PSK
  configuring 7-31
  described 7-29
PSK Format parameter 7-31
public key cryptography (PKC), with mobility 14-7

QB
QBSS 7-46
QoS
  levels 4-64, 7-44
  translation values 7-44
  with CAC 4-72
QoS profiles
  configuring
    using the CLI 4-66 to 4-67
    using the GUI 4-64 to 4-66
QoS roles
  configuring
    using the CLI 4-69 to 4-71
    using the GUI 4-67 to 4-69
QoS Roles for Guest Users page 4-68
Quality of Service (QoS) parameter 7-45
quarantined VLAN
  configuring 3-7, 3-18
  using 15-9
  with FlexConnect 15-5
  with NAC out-of-band integration 7-90
Quarantine parameter
  for dynamic interface 3-18
for management interface 3-7
NAC out-of-band integration 7-90
Query Interval parameter 6-107
queue statistics 9-115

R

Radio > Statistics page 7-52
radio core dumps
described 8-43
uploading
using the GUI 8-45
radio measurement requests
configuring
on the CLI 12-47
on the GUI 12-46
overview 12-44
viewing status using the CLI 12-47
radio preamble 6-47
radio resource management (RRM)
CCX features. See CCX radio management
configuring
monitor intervals using the GUI 12-17
coverage hole detection
configuring per controller using the CLI 12-20
configuring per controller using the GUI 12-16
described 12-4
debugging 12-25
disabling dynamic channel and power assignment
using the CLI 12-40
overriding RRM 12-32 to 12-40
overview 12-1
specifying channels 9-60 to 9-63, 12-10 to 12-13
statically assigning channel and transmit power settings
using the CLI 12-37
using the GUI 12-33 to 12-37
update interval 12-28, 12-32
Wireless > 802.11a/n (or 802.11b/g/n) > RRM > TPC parameter 12-7
radio resource management (RRM) settings
viewing using the CLI 12-22 to 12-24
radio resource monitoring 12-2

RADIUS
accounting 6-4
authentication 6-3
choosing authentication priority order 6-10
configuring on ACS 6-4, 6-5
FIPS standard 6-11
KEK parameter 6-11
MACK parameter 6-11
server fallback behavior 6-9, 6-12
using FlexConnect 15-21
RADIUS > Fallback Parameters page 6-9
RADIUS authentication attributes 6-13 to 6-16
Range (RootAP to MeshAP) parameter 9-32
Redirect URL After Login parameter 11-13
Refresh-time Interval parameter 4-94
Regenerate Certificate button 11-7
rehosting a license. See licenses
Rehost Ticket File Name parameter 4-17
Remote Authentication Dial-In User Service. See RADIUS
Request Max Retries parameter 6-39
Request Timeout parameter 6-39
Reserved Roaming Bandwidth parameter 4-75
Reset Link Latency button 8-107
Reset Personal SSID parameter 8-63
resetting the controller 10-36
Re-sync button 6-108
reverse path filtering (RPF) 14-25
RF Channel Assignment parameter 12-40
RF Group Leader
Auto mode, Static Mode 12-27
RF group leader
described 12-27
RF group name
described 12-28
entering 12-29
RF groups
cascading 12-27
configuring
  using the GUI 12-29
difference from mobility groups 12-26
overview 12-26 to 12-28
pinning 12-27
viewing status
  using the CLI 12-31
  using the GUI 12-30 to 12-31
RF Group support 12-28
RFID tags
  described 4-101
  number supported per controller 4-102
tracking
  debugging using the CLI 4-104
RFID tracking on access points, optimizing
  using the GUI 8-97 to 8-99
RF-Network Name parameter 12-29
RLDP. See Rogue Location Discovery Protocol (RLDP)
roaming and real-time diagnostics
  configuring using the CLI A-42
  described A-39
logs
  described A-39
  viewing A-40
roam reason report 4-59
roam reason report, described 9-89
rogue access points
  alarm 12-42
  automatically containing
    using the CLI 6-86
    using the GUI 6-84
  classification mapping table 6-89
rogue detection 6-83, 6-85
  and OfficeExtend access points 8-63, 8-66
Rogue Detection parameter 6-83, 8-63
Rogue Location Discovery Protocol (RLDP)
  defined 6-82
Rogue Location Discovery Protocol parameter 6-83
Rogue on Wire parameter 6-84
Rogue Policies page 6-83
rogue states 6-89
Role Name parameter 4-69
Role of the Controller 13-2
Role parameter 6-29
root bridge 3-27
Root Cost parameter 3-30
Root Port parameter 3-30
RRM. See radio resource management (RRM)
RSNA logs
    configuring A-40 to A-41
    described A-39

S
Save and Reboot button 10-21, 10-24
Save Licenses button 4-7
saving configuration settings 10-33
Scan Threshold parameter 4-61
Scope Name parameter 7-16
Search AP window 8-15, 8-41
Search Clients page 8-116
Search WLANs window 7-8, 8-10, 8-15
Secondary Controller parameters 8-79, 9-26
Secondary RADIUS Server parameter 15-23
SE-Connect 13-4, 13-25
secure web mode
    described 2-18
security
    overview 6-2
Security Mode parameter 9-34
security settings
    local and external authentication 9-31
Select APs from Current Controller parameter 15-23
self-signed certificate (SSC)
    used to authorize access points 8-30
Sequence parameter 6-58, 15-17
serial number for controller, finding 4-18
serial number of controller, finding 4-16
serial port
  - baud rate setting 2-24
  - timeout 2-24
Server Address parameter 6-107
Server Index (Priority) parameter 6-7, 6-22, 6-33
Server IP Address parameter
  - for LDAP server 6-33
  - for RADIUS server 6-7
  - for TACACS+ server 6-22
  - for wireless sniffer A-48
Server Key parameter 6-41, 15-24
Server Status parameter 6-8, 6-22
Server Timeout parameter 6-8, 6-22, 6-33
service port 3-4
service-port interface
  - configuring using the GUI 3-6 to 3-8, 3-10 to 3-14
Set Priority button 4-13
Set reboot time 10-14
Set to Factory Default button 12-18
Severity Level Filtering parameter A-10
Shared Secret Format parameter 6-7, 6-22
Shared Secret parameter 6-8, 6-22
Short Preamble Enabled parameter 6-47
short preambles 6-47
Show Wired Clients option 8-74
shunned clients
  - described 6-106
Signature Events Summary page 6-116
Signature Events Track Detail page 6-117
Simple Bind parameter 6-33
sniffing. See wireless sniffing A-47
Sniff parameter A-48
SNMP, configuring 4-37 to 4-38
SNMP engine Id 4-38
SNMP v1 / v2c Community page 4-39
SNMP v3 users
  - changing default values using the GUI 4-40 to 4-41
SNMP V3 Users page 4-41
software, upgrading
  guidelines  10-1 to 10-3
  using the CLI  10-7 to 10-10
  using the GUI  10-5 to 10-7
software, upgrading in mesh networks
  guidelines  10-5
Source parameter for ACLs  6-58, 15-18
Source Port parameter  6-59, 15-18
Spanning Tree Algorithm parameter  3-30
spanning tree protocol  3-31
spanning tree protocol (GUI)  3-28
Spanning Tree Protocol (STP)
  described  3-27
  spanning-tree root  3-27
Spanning Tree Specification parameter  3-29
SpectraLink NetLink phones
  overview  6-47
Spectralink Voice Priority parameter  4-89
Spectrum Expert  13-24
splash page web redirect  7-82
Splash Page Web Redirect parameter  7-84
SRE  1-10
SSC key-hash on Cisco WiSM  8-29
SSH
  and OfficeExtend access points  8-64, 8-66
    configuring
      using the CLI  2-37 to 2-38
    troubleshooting access points
      using the CLI  A-51 to A-52
      using the GUI  A-49 to A-51
SSH parameter  A-51
SSID
  configuring
    using the CLI  7-6
    using the GUI  7-5
  described  7-1
SSL certificate
  generating
    using the CLI  2-19
loading
  using the CLI 2-21 to 2-22
  using the GUI 2-20 to 2-21
SSLv2, configuring for web administration 2-19
SSLv2 for web authentication, disabling 11-13
Standard Signatures page 6-115
stateful DHCPv6 IP addressing 7-61
State parameter 6-108, 6-116
static IP address
  configuring
    using the CLI 8-51
    using the GUI 8-50
  described 8-48
Static IP parameter 8-49
Static Mobility Group Members page 14-12
Statistics option 9-114
Status parameter
  for DHCP scopes 7-17
  for guest LANs 11-32
  for SNMP community 4-39
  for WLANs 7-5, 7-102
Sticky PMKID Caching 7-33
STP Mode parameter 3-28
STP Port Designated Bridge parameter 3-28
STP Port Designated Cost parameter 3-28
STP Port Designated Port parameter 3-28
STP Port Designated Root parameter 3-28
STP Port Forward Transitions Count parameter 3-28
STP Port Path Cost Mode parameter 3-28
STP Port Path Cost parameter 3-29
STP Port Priority parameter 3-28
STP State parameter 3-28
strong passwords 8-23
Summary page 2-36
switch, configuring at the remote site 15-8
Switch IP Address (Anchor) parameter 14-21
SX/LC/T small form-factor plug-in (SFP) modules 3-3
symmetric mobility tunneling
  illustrated 14-25
verifying status
  using the CLI  14-26
Symmetric Mobility Tunneling Mode parameter  14-26
syslog
  described  A-39
  levels  A-11
  logs  A-40 to A-41
Syslog Configuration page  A-10
syslog server
  number supported by controller  A-10
  removing from controller  A-10
  severity level filtering  A-10
Syslog Server IP Address parameter  A-10
system logging
  configuring
    using the CLI  A-12 to A-15
    using the GUI  A-9 to A-12
  setting severity level  A-11
system logs, viewing using the CLI  A-15
system messages  A-3
System Resource Information page  A-7
system resources
  viewing using the CLI  A-7
  viewing using the GUI  A-6

T

TACACS+
  accounting  6-18
  authentication  6-17
  authorization  6-18
  choosing authentication priority order  6-23
  configuring
    using the CLI  6-24
    using the GUI  6-23
  described  6-17
  roles  6-18, 6-21
TACACS+ (Authentication, Authorization, or Accounting) Servers > New page  6-22
TACACS+ (Authentication, Authorization, or Accounting) Servers page  6-22
TACACS+ Administration .csv page (on CiscoSecure ACS) 6-24, 6-26
TCP MSS
  configuring 8-110
  described 8-108
Telnet
  and OfficeExtend access points 8-64, 8-66
  troubleshooting access points
    using the CLI A-51 to A-52
    using the GUI A-50 to A-51
Telnet parameter  A-51
Telnet sessions
  configuring
    using the CLI 2-37 to 2-38
    using the GUI 2-35 to 2-37
Telnet-SSH Configuration page  2-35
Tertiary Controller parameters 8-79, 9-26
text2pcap sample output A-45
TFTP server guidelines 10-2
time, configuring
  using the NTP server 2-30
time-length-values (TLVs), supported for CDP 4-91 to 4-92
Time Since Topology Changed parameter 3-29
timestamps, enabling or disabling in log and debug messages A-15
Time to Live for the PAC parameter 6-41, 15-25
time zone
  configuring using the CLI 2-33
  configuring using the GUI 2-32
TKIP
  configuring 7-31, 7-32
  described 7-29
  parameter 7-31
Topology Change Count parameter 3-29
traffic specifications (TSPEC) request
  described 4-72
  examples 4-72
traffic stream metrics (TSM)
  configuring
    using the GUI 4-76
  described 4-73
viewing statistics
  using the CLI  4-81 to 4-83
  using the GUI  4-80 to 4-81
Transfer Mode parameter
  downloading a CA certificate  10-23
  downloading a configuration file  10-31
  downloading a customized web authentication login page  11-23
  downloading a device certificate  10-20
  upgrading controller software  10-6
  uploading a configuration file  10-29
  uploading a PAC  10-26
  uploading packet capture files  A-25
Transition Time parameter  4-61
transmit power
  statically assigning using the CLI  12-37
  statically assigning using the GUI  12-37
transmit power levels  12-36
transmit power threshold, decreasing  12-18
trap logs
  for OfficeExtend access points  8-62
Trap Logs page  4-3, 7-52
troubleshooting
  access point join process  8-38 to 8-43
  CCXv5 clients  A-28 to A-42
  problems  A-8 to A-9
Troubleshooting OEAPs  A-53
tunnel attributes and identity networking  6-78
Tx Power Level Assignment parameter  12-40
Type parameter  7-4, 7-102, 11-31

U

U-APSD
  described  4-73
  viewing status
    using the CLI  4-81
    using the GUI  4-80
UDP, use in RADIUS  6-4
UDP port  14-21, 14-27
unicast mode  4-52
unique device identifier (UDI)
described  8-101
retrieving
using the CLI  8-102
using the GUI  8-101 to 8-102
Upload button  6-114, 8-45, 10-27, A-19, A-25
Upload CSV File parameter  15-24
Upload File from Controller page  8-44, 10-26, 10-29, A-18, A-24
URL parameter  11-21
URL to Send the Notifications parameter  4-21
USB console port, using on a 5500 series controller 3-32 to 3-33
Use AES Key Wrap parameter  6-7
User Access Mode parameter  11-3
user accounts, managing  11-1 to 11-25
User Attribute parameter  6-33
User Base DN parameter  6-33
User Credentials parameter  6-33
User Name parameter  6-29
Username parameter  8-18, 8-23, 8-24
User Object Type parameter  6-33
User parameter  10-26
User Profile Name parameter  4-41
Using CLI to monitor the Air quality  13-20
Using GUI to monitor air quality  13-19
Using Our SSID parameter  6-85
using the GUI  6-60

V
Validate Rogue Clients Against AAA parameter  6-83
Valid Client on Rogue AP parameter  6-85
Validity parameter  10-26
VCI strings  8-37
Verify Certificate CN Identity parameter  6-41
video information, viewing for mesh networks using the CLI  9-98 to 9-100
virtual interface
configuring
using the GUI  3-6 to 3-8, 3-10 to 3-14
described 3-13
VLAN Identifier parameter
  for AP-manager interface 3-11
  for dynamic interface 3-18, 3-19
VLAN ID parameter 7-89, 15-13
VLAN interface. See dynamic interface
VLAN Mappings
  button 15-13
  page 15-13
VLANs
  described 3-17
  guidelines 3-23
VLAN Select 3-46
VLAN Support parameter 15-12
Voice & Video Optimized parameter 4-89
voice information, viewing for mesh networks using the CLI 9-98 to 9-100
Voice Optimized parameter 4-89
voice-over-IP (VoIP) telephone roaming 4-58
Voice RSSI parameter 12-15
voice settings
  configuring
    using the GUI 4-76
  viewing
    using the GUI 4-81
VoIP calls, error codes 7-53 to 7-55
VoIP snooping
  described 7-50
VoIP Snooping and Reporting parameter 7-51
VPN passthrough
  configuring using the GUI 7-43

W
webauth.tar files 11-26
webauth bundle 11-22
web authentication
  certificate
    obtaining using the CLI 11-9
    obtaining using the GUI 11-6 to 11-8
configuring a WLAN for
  using the GUI  7-39
  described  11-9
  process  11-9 to 11-12
  successful login page  11-12
Web Authentication Certificate page  11-7
web authentication login page
  choosing the default
    using the CLI  11-14 to 11-16
  customizing from an external web server
    using the GUI  11-19 to 11-21
  default  11-11
  modified default example  11-16
  previewing  11-14, 11-24
Web Authentication option  11-32
Web Authentication Type parameter  11-13, 11-20, 11-23
Web Auth Type parameter  11-26, 11-33
web-browser security alert  11-10
Web Login page  11-13, 11-20
web mode
  described  2-18
Web Passthrough option  11-32
Web Policy parameter  6-63, 7-40, 7-84
Web Server IP Address parameter  11-21
Web Session Timeout parameter  2-18
WEP keys, configuring  7-28
WGB parameter  8-74
WGB Wired Clients page  8-74
wired guest access
  configuration overview  11-30
  described  11-28 to 11-30
  one-controller example  11-29
  two-controller example  11-30
wireless intrusion prevention system (wIPS)
  described  6-121
  viewing information  6-127
wireless sniffing
  configuring
    using the GUI  A-48
prerequisites A-47
WLAN ID parameter 7-5, 7-102
WLAN mobility security values 14-23
WLAN override 10-2
WLAN Profile parameter 6-29
WLANs
  checking security settings 7-28
  configuring
    conditional web redirect 7-84 to 7-85
  connecting clients to 15-15
  creating
    using the GUI 7-102
  deleting
    using the CLI 7-7
    using the GUI 7-4
  enabling or disabling
    using the CLI 7-7
    using the GUI 7-6
  session timeout
    described 7-37
  splash page web redirect 7-82
  wired security solution 1-5
WLANs > Edit (Advanced) page 7-51, 7-59, 7-86
  applying an ACL to a WLAN 6-62
  configuring infrastructure MFP for a WLAN 6-69
  configuring NAC out-of-band integration 7-91
  configuring the diagnostic channel A-29
WLANs > Edit (QoS) page 7-48
WLANs > Edit (Security > AAA Servers) page
  choosing RADIUS or LDAP servers for external authentication 11-26
  disabling accounting servers on a WLAN 7-85
WLANs > Edit (Security > Layer 2) page 7-31, 7-36
WLANs > Edit (Security > Layer 3) page
  applying a preauthentication ACL to a WLAN 6-63
  configuring a WLAN for VPN Passthrough 7-43
  configuring web redirect 7-84
  configuring wired guest access 11-32
WLANs > Edit page 7-5, 7-102, 11-32
WLANs > New page 11-31, 15-9
WLANs page 7-3, 7-6, 7-9, 7-10, 7-102, 14-21

WLAN SSID parameter
- configuring for guest user 11-4
- creating WLANs 7-5
- mapping an access point group to a WLAN 7-74, 7-92

WMM
- configuring 4-29, 7-48, 7-49
- described 7-46
- with CAC 4-72

WMM parameter 4-89, 4-90

WMM Policy parameter 7-48

workgroup bridges (WGBs)
- debugging 8-75
- described 8-70
- illustrated 8-52, 8-63, 8-68, 8-71
- sample configuration 8-73
- viewing status
  - using the CLI 8-74
  - using the GUI 8-73 to 8-74

world mode 4-25, 4-26

WPA2 Policy parameter 7-31

WPA Policy parameter 7-31

wplus license. See licenses