Cisco Wireless LAN Controller Configuration Guide

Software Release 5.2
November 2008

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

Text Part Number: OL-17037-01

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

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

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

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

CONTENTS

Preface xxiii

- Audience xxiv
- Purpose xxiv
- Organization xxiv
- Conventions xxv
- Related Publications xxvii
- Obtaining Documentation and Submitting a Service Request xxvii

CHAPTER 1 **Overview** 1-1

- Cisco Unified Wireless Network Solution Overview 1-2
  - Single-Controller Deployments 1-3
  - Multiple-Controller Deployments 1-4
- Operating System Software 1-4
- Operating System Security 1-5
  - Cisco WLAN Solution Wired Security 1-5
- Layer 2 and Layer 3 Operation 1-6
  - Operational Requirements 1-6
  - Configuration Requirements 1-6
- Cisco Wireless LAN Controllers 1-6
  - Client Location 1-7
- Controller Platforms 1-7
  - Cisco 2100 Series Controllers 1-8
    - Features Not Supported 1-8
  - Cisco 4400 Series Controllers 1-8
  - Catalyst 6500 Series Wireless Services Module 1-9
  - Cisco 7600 Series Router Wireless Services Module 1-10
  - Cisco 28/37/38xx Series Integrated Services Router 1-11
  - Catalyst 3750G Integrated Wireless LAN Controller Switch 1-11
- Cisco UWN Solution Wired Connections 1-12
- Cisco UWN Solution WLANs 1-12
- Identity Networking 1-13
  - Enhanced Integration with Cisco Secure ACS 1-13
- File Transfers 1-14

Power over Ethernet 1-14

Startup Wizard 1-15

Cisco Wireless LAN Controller Memory 1-15

Cisco Wireless LAN Controller Failover Protection 1-16

Network Connections to Cisco Wireless LAN Controllers 1-17

Cisco 2100 Series Wireless LAN Controllers 1-17

Cisco 4400 Series Wireless LAN Controllers 1-18

CHAPTER 2 **Using the Web-Browser and CLI Interfaces** 2-1

Using the Web-Browser Interface 2-2

Guidelines for Using the GUI 2-2

Opening the GUI 2-2

Enabling Web and Secure Web Modes 2-2

Using the GUI to Enable Web and Secure Web Modes 2-3

Using the CLI to Enable Web and Secure Web Modes 2-4

Loading an Externally Generated SSL Certificate 2-5

Using the CLI 2-7

Logging into the CLI 2-7

Using a Local Serial Connection 2-8

Using a Remote Ethernet Connection 2-8

Logging Out of the CLI 2-9

Navigating the CLI 2-9

Enabling Wireless Connections to the Web-Browser and CLI Interfaces 2-9

CHAPTER 3 **Configuring Ports and Interfaces** 3-1

Overview of Ports and Interfaces 3-2

Ports 3-2

Distribution System Ports 3-4

Service Port 3-5

Interfaces 3-6

Management Interface 3-6

AP-Manager Interface 3-6

Virtual Interface 3-7

Service-Port Interface 3-8

Dynamic Interface 3-8

WLANs 3-9

Configuring the Management, AP-Manager, Virtual, and Service-Port Interfaces 3-10

Using the GUI to Configure the Management, AP-Manager, Virtual, and Service-Port Interfaces 3-11

Using the CLI to Configure the Management, AP-Manager, Virtual, and Service-Port Interfaces **3-13**

Using the CLI to Configure the Management Interface **3-13**

Using the CLI to Configure the AP-Manager Interface **3-14**

Using the CLI to Configure the Virtual Interface **3-14**

Using the CLI to Configure the Service-Port Interface **3-15**

Configuring Dynamic Interfaces **3-16**

Using the GUI to Configure Dynamic Interfaces **3-16**

Using the CLI to Configure Dynamic Interfaces **3-18**

Configuring Ports **3-19**

Configuring Port Mirroring **3-22**

Configuring Spanning Tree Protocol **3-23**

Using the GUI to Configure Spanning Tree Protocol **3-24**

Using the CLI to Configure Spanning Tree Protocol **3-28**

Enabling Link Aggregation **3-29**

Link Aggregation Guidelines **3-32**

Using the GUI to Enable Link Aggregation **3-33**

Using the CLI to Enable Link Aggregation **3-34**

Using the CLI to Verify Link Aggregation Settings **3-34**

Configuring Neighbor Devices to Support LAG **3-34**

Configuring a 4400 Series Controller to Support More Than 48 Access Points **3-34**

Using Link Aggregation **3-35**

Using Multiple AP-Manager Interfaces **3-35**

CHAPTER 4 **Configuring Controller SettingsWireless Device Access** **4-1**

Using the Configuration Wizard **4-2**

Before You Start **4-2**

Resetting the Device to Default Settings **4-3**

Resetting to Default Settings Using the CLI **4-3**

Resetting to Default Settings Using the GUI **4-3**

Running the Configuration Wizard on the CLI **4-4**

Using the AutoInstall Feature for Controllers Without a Configuration **4-6**

Overview of AutoInstall **4-6**

Obtaining an IP Address Through DHCP and Downloading a Configuration File from a TFTP Server **4-7**

Selecting a Configuration File **4-8**

Example of AutoInstall Operation **4-9**

Managing the System Date and Time **4-10**

Configuring an NTP Server to Obtain the Date and Time **4-10**

Configuring the Date and Time Manually **4-10**

Using the GUI to Configure the Date and Time 4-10
Using the CLI to Configure the Date and Time 4-11
Configuring 802.11 Bands 4-14
Using the GUI to Configure 802.11 Bands 4-14
Using the CLI to Configure 802.11 Bands 4-15
Configuring 802.11n Parameters 4-17
Using the GUI to Configure 802.11n Parameters 4-17
Using the CLI to Configure 802.11n Parameters 4-19
Configuring DHCP Proxy 4-22
Using the GUI to Configure DHCP Proxy 4-22
Using the CLI to Configure DHCP Proxy 4-23
Configuring Administrator Usernames and Passwords 4-23
Configuring Usernames and Passwords 4-23
Restoring Passwords 4-24
Configuring SNMP 4-24
Changing the Default Values of SNMP Community Strings 4-25
Using the GUI to Change the SNMP Community String Default Values 4-25
Using the CLI to Change the SNMP Community String Default Values 4-27
Changing the Default Values for SNMP v3 Users 4-27
Using the GUI to Change the SNMP v3 User Default Values 4-27
Using the CLI to Change the SNMP v3 User Default Values 4-29
Configuring Aggressive Load Balancing 4-29
Using the GUI to Configure Aggressive Load Balancing 4-30
Using the CLI to Configure Aggressive Load Balancing 4-30
Configuring Fast SSID Changing 4-31
Using the GUI to Configure Fast SSID Changing 4-31
Using the CLI to Configure Fast SSID Changing 4-31
Enabling 802.3X Flow Control 4-31
Configuring 802.3 Bridging 4-32
Using the GUI to Configure 802.3 Bridging 4-32
Using the CLI to Configure 802.3 Bridging 4-33
Configuring Multicast Mode 4-34
Understanding Multicast Mode 4-34
Guidelines for Using Multicast Mode 4-35
Using the GUI to Enable Multicast Mode 4-36
Using the GUI to View Multicast Groups 4-37
Using the CLI to Enable Multicast Mode 4-38
Using the CLI to View Multicast Groups 4-39

Using the CLI to View an Access Point's Multicast Client Table 4-39

Configuring Client Roaming 4-40

Intra-Controller Roaming 4-40

Inter-Controller Roaming 4-40

Inter-Subnet Roaming 4-40

Voice-over-IP Telephone Roaming 4-40

CCX Layer 2 Client Roaming 4-41

Using the GUI to Configure CCX Client Roaming Parameters 4-42

Using the CLI to Configure CCX Client Roaming Parameters 4-43

Using the CLI to Obtain CCX Client Roaming Information 4-43

Using the CLI to Debug CCX Client Roaming Issues 4-44

Configuring IP-MAC Address Binding 4-44

Configuring Quality of Service 4-45

Configuring Quality of Service Profiles 4-45

Using the GUI to Configure QoS Profiles 4-45

Using the CLI to Configure QoS Profiles 4-47

Configuring Quality of Service Roles 4-48

Using the GUI to Configure QoS Roles 4-48

Using the CLI to Configure QoS Roles 4-50

Configuring Voice and Video Parameters 4-52

Call Admission Control 4-52

Bandwidth-Based CAC 4-52

Load-Based CAC 4-52

Expedited Bandwidth Requests 4-53

U-APSD 4-54

Traffic Stream Metrics 4-54

Using the GUI to Configure Voice Parameters 4-54

Using the GUI to Configure Video Parameters 4-56

Using the GUI to View Voice and Video Settings 4-57

Using the CLI to Configure Voice Parameters 4-62

Using the CLI to Configure Video Parameters 4-63

Using the CLI to View Voice and Video Settings 4-64

Configuring EDCA Parameters 4-67

Using the GUI to Configure EDCA Parameters 4-67

Using the CLI to Configure EDCA Parameters 4-68

Configuring Cisco Discovery Protocol 4-69

Using the GUI to Configure Cisco Discovery Protocol 4-72

Using the GUI to View Cisco Discovery Protocol Information 4-73

Using the CLI to Configure Cisco Discovery Protocol 4-77

Using the CLI to View Cisco Discovery Protocol Information 4-78

Configuring RFID Tag Tracking 4-79

Using the CLI to Configure RFID Tag Tracking 4-81

Using the CLI to View RFID Tag Tracking Information 4-82

Using the CLI to Debug RFID Tag Tracking Issues 4-83

Configuring and Viewing Location Settings 4-84

Installing the Location Appliance Certificate 4-84

Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues 4-85

Synchronizing the Controller and Location Appliance 4-86

Using the CLI to View Location Settings 4-86

Configuring the Supervisor 720 to Support the WiSM 4-89

General WiSM Guidelines 4-90

Configuring the Supervisor 4-90

Using the Wireless LAN Controller Network Module 4-91

CHAPTER 5 Configuring Security Solutions 5-1

Cisco UWN Solution Security 5-2

Security Overview 5-2

Layer 1 Solutions 5-2

Layer 2 Solutions 5-2

Layer 3 Solutions 5-3

Integrated Security Solutions 5-3

Configuring RADIUS 5-3

Configuring RADIUS on the ACS 5-4

Using the GUI to Configure RADIUS 5-6

Using the CLI to Configure RADIUS 5-11

RADIUS Authentication Attributes Sent by the Access Point 5-15

RADIUS Accounting Attributes 5-17

Configuring TACACS+ 5-18

Configuring TACACS+ on the ACS 5-19

Using the GUI to Configure TACACS+ 5-23

Using the CLI to Configure TACACS+ 5-25

Viewing the TACACS+ Administration Server Logs 5-27

Configuring Local Network Users 5-29

Using the GUI to Configure Local Network Users 5-30

Using the CLI to Configure Local Network Users 5-32

Configuring LDAP 5-33

Using the GUI to Configure LDAP 5-33

Using the CLI to Configure LDAP 5-36

Configuring Local EAP 5-38

Using the GUI to Configure Local EAP 5-40

Using the CLI to Configure Local EAP 5-45

Configuring the System for SpectraLink NetLink Telephones 5-50

Using the GUI to Enable Long Preambles 5-50

Using the CLI to Enable Long Preambles 5-51

Using the CLI to Configure Enhanced Distributed Channel Access 5-52

Using Management over Wireless 5-52

Using the GUI to Enable Management over Wireless 5-52

Using the CLI to Enable Management over Wireless 5-52

Configuring DHCP Option 82 5-53

Configuring and Applying Access Control Lists 5-54

Using the GUI to Configure Access Control Lists 5-55

Using the GUI to Apply Access Control Lists 5-59

Applying an Access Control List to an Interface 5-59

Applying an Access Control List to the Controller CPU 5-60

Applying an Access Control List to a WLAN 5-61

Applying a Preauthentication Access Control List to a WLAN 5-62

Using the CLI to Configure Access Control Lists 5-63

Using the CLI to Apply Access Control Lists 5-65

Configuring Management Frame Protection 5-66

Guidelines for Using MFP 5-67

Using the GUI to Configure MFP 5-68

Using the GUI to View MFP Settings 5-69

Using the CLI to Configure MFP 5-70

Using the CLI to View MFP Settings 5-71

Using the CLI to Debug MFP Issues 5-73

Configuring Client Exclusion Policies 5-73

Configuring Identity Networking 5-74

Identity Networking Overview 5-74

RADIUS Attributes Used in Identity Networking 5-75

QoS-Level 5-75

ACL-Name 5-75

Interface-Name 5-76

VLAN-Tag 5-76

Tunnel Attributes 5-77

Configuring AAA Override 5-78

Updating the RADIUS Server Dictionary File for Proper QoS Values 5-78

Using the GUI to Configure AAA Override 5-79

Using the CLI to Configure AAA Override 5-80

Managing Rogue Devices 5-80

Challenges 5-80

Detecting Rogue Devices 5-81

Classifying Rogue Access Points 5-81

WCS Interaction 5-84

Configuring RLDP 5-84

Using the GUI to Configure RLDP 5-84

Using the CLI to Configure RLDP 5-85

Configuring Rogue Classification Rules 5-87

Using the GUI to Configure Rogue Classification Rules 5-87

Using the CLI to Configure Rogue Classification Rules 5-90

Viewing and Classifying Rogue Devices 5-93

Using the GUI to View and Classify Rogue Devices 5-93

Using the CLI to View and Classify Rogue Devices 5-98

Configuring IDS 5-103

Configuring IDS Sensors 5-103

Using the GUI to Configure IDS Sensors 5-103

Using the CLI to Configure IDS Sensors 5-105

Viewing Shunned Clients 5-106

Configuring IDS Signatures 5-107

Using the GUI to Configure IDS Signatures 5-109

Using the CLI to Configure IDS Signatures 5-115

Using the CLI to View IDS Signature Events 5-117

Configuring wIPS 5-119

Configuring wIPS on an Access Point 5-119

Viewing wIPS Information 5-120

Detecting Active Exploits 5-122

Configuring Maximum Local Database Entries 5-122

Using the GUI to Configure Maximum Local Database Entries 5-122

Using the CLI to Specify the Maximum Number of Local Database Entries 5-122

CHAPTER 6 Configuring WLANsWireless Device Access 6-1

WLAN Overview 6-2

Configuring WLANs 6-2

Creating WLANs 6-3

Using the GUI to Create WLANs 6-3

Using the CLI to Create WLANs 6-5

Searching WLANs 6-7

Configuring DHCP 6-8

Internal DHCP Server 6-8

External DHCP Servers 6-8

DHCP Assignment 6-8

Security Considerations 6-9

Using the GUI to Configure DHCP 6-9

Using the CLI to Configure DHCP 6-10

Using the CLI to Debug DHCP 6-11

Configuring DHCP Scopes 6-11

Configuring MAC Filtering for WLANs 6-14

Enabling MAC Filtering 6-15

Creating a Local MAC Filter 6-15

Configuring a Timeout for Disabled Clients 6-15

Assigning WLANs to Interfaces 6-15

Configuring the DTIM Period 6-16

Using the GUI to Configure the DTIM Period 6-16

Using the CLI to Configure the DTIM Period 6-17

Configuring Peer-to-Peer Blocking 6-18

Guidelines for Using Peer-to-Peer Blocking 6-19

Using the GUI to Configure Peer-to-Peer Blocking 6-19

Using the CLI to Configure Peer-to-Peer Blocking 6-20

Configuring Layer 2 Security 6-20

Static WEP Keys 6-21

Dynamic 802.1X Keys and Authorization 6-21

Configuring a WLAN for Both Static and Dynamic WEP 6-22

WPA1 and WPA2 6-22

CKIP 6-25

Configuring a Session Timeout 6-27

Using the GUI to Configure a Session Timeout 6-27

Using the CLI to Configure a Session Timeout 6-28

Configuring Layer 3 Security 6-28

VPN Passthrough 6-29

Web Authentication 6-29

Assigning a QoS Profile to a WLAN 6-30

Using the GUI to Assign a QoS Profile to a WLAN 6-31

Using the CLI to Assign a QoS Profile to a WLAN 6-32

Configuring QoS Enhanced BSS 6-32

Guidelines for Configuring QBSS 6-34

Additional Guidelines for Using 7921 and 7920 Wireless IP Phones 6-34

Using the GUI to Configure QBSS 6-35

Using the CLI to Configure QBSS 6-36
Configuring IPv6 Bridging 6-36
Guidelines for Using IPv6 Bridging 6-37
Using the GUI to Configure IPv6 Bridging 6-38
Using the CLI to Configure IPv6 Bridging 6-39
Configuring Cisco Client Extensions 6-39
Using the GUI to Configure CCX Aironet IEs 6-40
Using the GUI to View a Client's CCX Version 6-40
Using the CLI to Configure CCX Aironet IEs 6-42
Using the CLI to View a Client's CCX Version 6-42
Configuring Access Point Groups 6-42
Creating Access Point Groups 6-44
Configuring Web Redirect with 802.1X Authentication 6-49
Conditional Web Redirect 6-49
Splash Page Web Redirect 6-50
Configuring the RADIUS Server 6-50
Using the GUI to Configure Web Redirect 6-51
Using the CLI to Configure Web Redirect 6-52
Disabling Accounting Servers per WLAN 6-53
Disabling Coverage Hole Detection per WLAN 6-54
Using the GUI to Disable Coverage Hole Detection on a WLAN 6-54
Using the CLI to Disable Coverage Hole Detection on a WLAN 6-55
Configuring NAC Out-of-Band Integration 6-55
Guidelines for Using NAC Out-of-Band Integration 6-56
Using the GUI to Configure NAC Out-of-Band Integration 6-57
Using the CLI to Configure NAC Out-of-Band Integration 6-60

CHAPTER 7 Controlling Lightweight Access Points 7-1
Access Point Communication Protocols 7-2
Guidelines for Using CAPWAP 7-2
The Controller Discovery Process 7-2
Verifying that Access Points Join the Controller 7-4
Using the GUI to Verify that Access Points Join the Controller 7-4
Using the CLI to Verify that Access Points Join the Controller 7-4
Viewing CAPWAP MTU Information 7-5
Debugging CAPWAP 7-5
Configuring Global Credentials for Access Points 7-5
Using the GUI to Configure Global Credentials for Access Points 7-6
Using the CLI to Configure Global Credentials for Access Points 7-8

Configuring Authentication for Access Points 7-9
  - Using the GUI to Configure Authentication for Access Points 7-10
  - Using the CLI to Configure Authentication for Access Points 7-12
  - Configuring the Switch for Authentication 7-14

Embedded Access Points 7-14

Autonomous Access Points Converted to Lightweight Mode 7-16
  - Guidelines for Using Access Points Converted to Lightweight Mode 7-16
  - Reverting from Lightweight Mode to Autonomous Mode 7-17
    - Using a Controller to Return to a Previous Release 7-17
    - Using the MODE Button and a TFTP Server to Return to a Previous Release 7-17
  - Authorizing Access Points 7-18
    - Authorizing Access Points Using SSCs 7-18
    - Authorizing Access Points Using MICs 7-18
    - Authorizing Access Points Using LSCs 7-19
    - Using the GUI to Authorize Access Points 7-22
    - Using the CLI to Authorize Access Points 7-23
  - Using DHCP Option 43 and DHCP Option 60 7-24
  - Troubleshooting the Access Point Join Process 7-24
    - Configuring the Syslog Server for Access Points 7-26
    - Viewing Access Point Join Information 7-26
  - Using a Controller to Send Debug Commands to Access Points Converted to Lightweight Mode 7-28
  - Converted Access Points Send Crash Information to Controller 7-28
  - Converted Access Points Send Radio Core Dumps to Controller 7-28
    - Using the CLI to Retrieve Radio Core Dumps 7-29
    - Using the GUI to Upload Radio Core Dumps 7-29
    - Using the CLI to Upload Radio Core Dumps 7-30
  - Uploading Memory Core Dumps from Converted Access Points 7-31
    - Using the GUI to Upload Access Point Core Dumps 7-31
    - Using the CLI to Upload Access Point Core Dumps 7-32
  - Display of MAC Addresses for Converted Access Points 7-32
  - Disabling the Reset Button on Access Points Converted to Lightweight Mode 7-33
  - Configuring a Static IP Address on an Access Point Converted to Lightweight Mode 7-33
  - Supporting Oversized Access Point Images 7-33

Cisco Workgroup Bridges 7-34
  - Guidelines for Using WGBs 7-35
  - Sample WGB Configuration 7-37
  - Using the GUI to View the Status of Workgroup Bridges 7-37
  - Using the CLI to View the Status of Workgroup Bridges 7-40
  - Using the CLI to Debug WGB Issues 7-40

Configuring Backup Controllers 7-41
- Using the GUI to Configure Backup Controllers 7-42
- Using the CLI to Configure Backup Controllers 7-44

Configuring Failover Priority for Access Points 7-46
- Using the GUI to Configure Failover Priority for Access Points 7-46
- Using the CLI to Configure Failover Priority for Access Points 7-48
- Using the CLI to View Failover Priority Settings 7-48

Configuring Country Codes 7-49
- Guidelines for Configuring Multiple Country Codes 7-49
- Using the GUI to Configure Country Codes 7-50
- Using the CLI to Configure Country Codes 7-52

Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain 7-55
- Guidelines for Migration 7-56
- Migrating Access Points to the -U Regulatory Domain 7-56

Using the W56 Band in Japan 7-58

Dynamic Frequency Selection 7-58

Optimizing RFID Tracking on Access Points 7-59
- Using the GUI to Optimize RFID Tracking on Access Points 7-59
- Using the CLI to Optimize RFID Tracking on Access Points 7-61

Configuring Probe Request Forwarding 7-62

Retrieving the Unique Device Identifier on Controllers and Access Points 7-63
- Using the GUI to Retrieve the Unique Device Identifier on Controllers and Access Points 7-63
- Using the CLI to Retrieve the Unique Device Identifier on Controllers and Access Points 7-64

Performing a Link Test 7-64
- Using the GUI to Perform a Link Test 7-65
- Using the CLI to Perform a Link Test 7-67

Configuring Link Latency 7-67
- Using the GUI to Configure Link Latency 7-68
- Using the CLI to Configure Link Latency 7-69

Configuring Power over Ethernet 7-70
- Using the GUI to Configure Power over Ethernet 7-71
- Using the CLI to Configure Power over Ethernet 7-73

Configuring Flashing LEDs 7-74

Viewing Clients 7-74
- Using the GUI to View Clients 7-74
- Using the CLI to View Clients 7-78

CHAPTER 8

Controlling Mesh Access Points 8-1

Cisco Aironet Mesh Access Points 8-2
Access Point Roles 8-2
Network Access 8-3
Deployment Modes 8-4
Cisco Wireless Mesh Network 8-4
Wireless Backhaul 8-4
Point-to-Point Wireless Bridging 8-5
Point-to-Multipoint Wireless Bridging 8-5

Architecture Overview 8-6
CAPWAP 8-6
Cisco Adaptive Wireless Path Protocol Wireless Mesh Routing 8-6
Mesh Neighbors, Parents, and Children 8-7
Wireless Mesh Constraints 8-7

Adding Mesh Access Points to the Mesh Network 8-10
Adding MAC Addresses of Mesh Access Points to the Controller Filter List 8-10
Configuring External Authentication and Authorization Using a RADIUS Server 8-13
Defining the Mesh Access Point Role 8-16
Configuring Global Mesh Parameters 8-16
Configuring Local Mesh Parameters 8-22
Client Roaming 8-24
Configuring Ethernet Bridging and Ethernet VLAN Tagging 8-25

Configuring Advanced Features 8-32
Configuring Voice Parameters in Mesh Networks 8-32
CAC 8-32
QoS and DSCP Marking 8-32
Guidelines for Using Voice on the Mesh Network 8-33
Voice Call Support in a Mesh Network 8-34
Using the CLI to View Voice Details for Mesh Networks 8-34
Enabling Mesh Multicast Containment **for Video** 8-37
Backhaul Client Access (Universal Access) for Indoor and Outdoor Mesh Access Points 8-39

Viewing Mesh Statistics and Reports 8-39
Viewing Mesh Statistics for an Access Point 8-39
Using the GUI to View Mesh Statistics for an Access Point 8-39
Using the CLI to View Mesh Statistics for an Access Point 8-43
Viewing Neighbor Statistics for an Access Point 8-44
Using the GUI to View Neighbor Statistics for an Access Point 8-44
Using the CLI to View Neighbor Statistics for an Access Point 8-47

Converting Indoor Access Points to Mesh Access Points (1130AG, 1240AG) 8-48

Changing MAP and RAP Roles for Indoor Mesh Access Points (1130AG, 1240AG) 8-49
Using the GUI to Change MAP and RAP Roles for Indoor Mesh Access Points 8-49
Using the CLI to Change MAP and RAP Roles for Indoor Mesh Access Points 8-49
Converting Indoor Mesh Access Points to Non-Mesh Lightweight Access Points (1130AG, 1240AG) 8-50
Configuring Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers 8-51
Configuration Guidelines 8-51
Using the GUI to Enable Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers 8-52
Using the CLI to Enable Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers 8-53

CHAPTER 9

Managing Controller Software and Configurations 9-1
Upgrading Controller Software 9-2
Guidelines for Upgrading Controller Software 9-2
Guidelines for Upgrading to Controller Software 5.2 in Mesh Networks 9-3
Mandatory Boot Variable Update for Networks with 1522 Access Points 9-4
Upgrade Compatibility Matrix 9-6
Using the GUI to Upgrade Controller Software 9-8
Using the CLI to Upgrade Controller Software 9-10
Transferring Files to and from a Controller 9-13
Downloading Device Certificates 9-13
Using the GUI to Download Device Certificates 9-14
Using the CLI to Download Device Certificates 9-15
Downloading CA Certificates 9-16
Using the GUI to Download CA Certificates 9-16
Using the CLI to Download CA Certificates 9-17
Uploading PACs 9-19
Using the GUI to Upload PACs 9-19
Using the CLI to Upload PACs 9-20
Uploading and Downloading Configuration Files 9-21
Uploading Configuration Files 9-21
Downloading Configuration Files 9-23
Saving Configurations 9-26
Editing Configuration Files 9-27
Clearing the Controller Configuration 9-28
Erasing the Controller Configuration 9-28
Resetting the Controller 9-28

CHAPTER 10 **Managing User Accounts** 10-1

Creating Guest User Accounts 10-2

Creating a Lobby Ambassador Account 10-2

Using the GUI to Create a Lobby Ambassador Account 10-2

Using the CLI to Create a Lobby Ambassador Account 10-3

Creating Guest User Accounts as a Lobby Ambassador 10-4

Viewing Guest User Accounts 10-6

Using the GUI to View Guest Accounts 10-6

Using the CLI to View Guest Accounts 10-7

Web Authentication Process 10-7

Choosing the Web Authentication Login Page 10-9

Choosing the Default Web Authentication Login Page 10-10

Using the GUI to Choose the Default Web Authentication Login Page 10-10

Using the CLI to Choose the Default Web Authentication Login Page 10-11

Modified Default Web Authentication Login Page Example 10-13

Creating a Customized Web Authentication Login Page 10-14

Using a Customized Web Authentication Login Page from an External Web Server 10-16

Using the GUI to Choose a Customized Web Authentication Login Page from an External Web Server 10-16

Using the CLI to Choose a Customized Web Authentication Login Page from an External Web Server 10-17

Downloading a Customized Web Authentication Login Page 10-17

Using the GUI to Download a Customized Web Authentication Login Page 10-18

Using the CLI to Download a Customized Web Authentication Login Page 10-19

Customized Web Authentication Login Page Example 10-20

Using the CLI to Verify the Web Authentication Login Page Settings 10-20

Assigning Login, Login Failure, and Logout Pages per WLAN 10-21

Using the GUI to Assign Login, Login Failure, and Logout Pages per WLAN 10-21

Using the CLI to Assign Login, Login Failure, and Logout Pages per WLAN 10-22

Configuring Wired Guest Access 10-23

Configuration Overview 10-25

Configuration Guidelines 10-25

Using the GUI to Configure Wired Guest Access 10-25

Using the CLI to Configure Wired Guest Access 10-29

CHAPTER 11 **Configuring Radio Resource ManagementWireless Device Access** 11-1

Overview of Radio Resource Management 11-2

Radio Resource Monitoring 11-2

Transmit Power Control 11-2

Dynamic Channel Assignment 11-3

Coverage Hole Detection and Correction 11-4

RRM Benefits 11-5

Overview of RF Groups 11-5

RF Group Leader 11-6

RF Group Name 11-6

Configuring an RF Group 11-6

Using the GUI to Configure an RF Group 11-7

Using the CLI to Configure RF Groups 11-7

Viewing RF Group Status 11-8

Using the GUI to View RF Group Status 11-8

Using the CLI to View RF Group Status 11-9

Configuring RRM 11-9

Using the GUI to Configure RRM 11-9

Using the GUI to Configure RF Group Mode 11-10

Using the GUI to Configure Transmit Power Control 11-10

Using the GUI to Configure Dynamic Channel Assignment 11-12

Using the GUI to Configure Coverage Hole Detection 11-15

Using the GUI to Configure RRM Profile Thresholds, Monitoring Channels, and Monitor Intervals 11-17

Using the CLI to Configure RRM 11-19

Using the CLI to View RRM Settings 11-23

Using the CLI to Debug RRM Issues 11-25

Overriding RRM 11-25

Statically Assigning Channel and Transmit Power Settings to Access Point Radios 11-26

Using the GUI to Statically Assign Channel and Transmit Power Settings 11-26

Using the CLI to Statically Assign Channel and Transmit Power Settings 11-30

Disabling Dynamic Channel and Power Assignment Globally for a Controller 11-33

Using the GUI to Disable Dynamic Channel and Power Assignment 11-33

Using the CLI to Disable Dynamic Channel and Power Assignment 11-33

Enabling Rogue Access Point Detection in RF Groups 11-34

Using the GUI to Enable Rogue Access Point Detection in RF Groups 11-34

Using the CLI to Enable Rogue Access Point Detection in RF Groups 11-36

Configuring CCX Radio Management Features 11-36

Radio Measurement Requests 11-37

Location Calibration 11-37

Using the GUI to Configure CCX Radio Management 11-37

Using the CLI to Configure CCX Radio Management 11-39

Using the CLI to Obtain CCX Radio Management Information 11-39

Using the CLI to Debug CCX Radio Management Issues 11-41
Configuring Pico Cell Mode 11-41
Guidelines for Using Pico Cell Mode 11-42
Using the GUI to Configure Pico Cell Mode 11-42
Using the CLI to Configure Pico Cell Mode 11-44
Using the CLI to Debug Pico Cell Mode Issues 11-45

CHAPTER 12 Configuring Mobility GroupsWireless Device Access 12-1
Overview of Mobility 12-2
Overview of Mobility Groups 12-5
Determining When to Include Controllers in a Mobility Group 12-7
Messaging among Mobility Groups 12-7
Using Mobility Groups with NAT Devices 12-8
Configuring Mobility Groups 12-9
Prerequisites 12-9
Using the GUI to Configure Mobility Groups 12-11
Using the CLI to Configure Mobility Groups 12-14
Viewing Mobility Group Statistics 12-16
Using the GUI to View Mobility Group Statistics 12-16
Using the CLI to View Mobility Group Statistics 12-19
Configuring Auto-Anchor Mobility 12-20
Guidelines for Using Auto-Anchor Mobility 12-21
Using the GUI to Configure Auto-Anchor Mobility 12-21
Using the CLI to Configure Auto-Anchor Mobility 12-23
WLAN Mobility Security Values 12-25
Using Symmetric Mobility Tunneling 12-26
Running Mobility Ping Tests 12-28

CHAPTER 13 Configuring Hybrid REAPWireless Device Access 13-1
Overview of Hybrid REAP 13-2
Hybrid-REAP Authentication Process 13-2
Hybrid REAP Guidelines 13-4
Configuring Hybrid REAP 13-5
Configuring the Switch at the Remote Site 13-5
Configuring the Controller for Hybrid REAP 13-6
Using the GUI to Configure the Controller for Hybrid REAP 13-7
Using the CLI to Configure the Controller for Hybrid REAP 13-11
Configuring an Access Point for Hybrid REAP 13-11

Using the GUI to Configure an Access Point for Hybrid REAP **13-11**

Using the CLI to Configure an Access Point for Hybrid REAP **13-14**

Connecting Client Devices to the WLANs **13-15**

Configuring Hybrid-REAP Groups **13-15**

Hybrid-REAP Groups and Backup RADIUS Servers **13-16**

Hybrid-REAP Groups and CCKM **13-16**

Hybrid-REAP Groups and Local Authentication **13-17**

Using the GUI to Configure Hybrid-REAP Groups **13-17**

Using the CLI to Configure Hybrid-REAP Groups **13-22**

APPENDIX A **Safety Considerations and Translated Safety Warnings** **A-1**

Safety Considerations **A-2**

Warning Definition **A-2**

Class 1 Laser Product Warning **A-5**

Ground Conductor Warning **A-7**

Chassis Warning for Rack-Mounting and Servicing **A-9**

Battery Handling Warning for 4400 Series Controllers **A-18**

Equipment Installation Warning **A-20**

More Than One Power Supply Warning for 4400 Series Controllers **A-23**

APPENDIX B **Declarations of Conformity and Regulatory Information** **B-1**

Regulatory Information for Lightweight Access Points **B-2**

Manufacturers Federal Communication Commission Declaration of Conformity Statement **B-2**

Department of Communications—Canada **B-3**

Canadian Compliance Statement **B-3**

European Community, Switzerland, Norway, Iceland, and Liechtenstein **B-4**

Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC **B-4**

Declaration of Conformity for RF Exposure **B-5**

Guidelines for Operating Controllers in Japan **B-6**

VCCI Class A Warning for 4400 Series Controllers in Japan **B-6**

VCCI Class B Warning for 2100 Series Controllers in Japan **B-6**

Power Cable and AC Adapter Warning for Japan **B-7**

Guidelines for Operating Controllers and Access Points in Japan **B-7**

Administrative Rules for Cisco Aironet Access Points in Taiwan **B-8**

Access Points with IEEE 802.11a Radios **B-8**

All Access Points **B-9**

Declaration of Conformity Statements **B-10**

FCC Statement for Cisco 2100 Series Wireless LAN Controllers B-10

FCC Statement for 4400 Series Wireless LAN Controllers B-10

APPENDIX C **End User License and Warranty** C-1

End User License Agreement C-2

Limited Warranty C-4

Disclaimer of Warranty C-5

General Terms Applicable to the Limited Warranty Statement and End User License Agreement C-6

Notices C-6

OpenSSL/Open SSL Project C-6

License Issues C-7

APPENDIX D **Troubleshooting** D-1

Interpreting LEDs D-2

Interpreting Controller LEDs D-2

Interpreting Lightweight Access Point LEDs D-2

System Messages D-2

Using the CLI to Troubleshoot Problems D-5

Configuring System and Message Logging D-6

Using the GUI to Configure System and Message Logging D-7

Using the GUI to View Message Logs D-9

Using the CLI to Configure System and Message Logging D-10

Using the CLI to View System and Message Logs D-12

Viewing Access Point Event Logs D-13

Uploading Logs and Crash Files D-14

Using the GUI to Upload Logs and Crash Files D-14

Using the CLI to Upload Logs and Crash Files D-15

Uploading Core Dumps from the Controller D-17

Using the CLI to Upload Controller Core Dumps D-17

Monitoring Memory Leaks D-17

Troubleshooting CCXv5 Client Devices D-19

Diagnostic Channel D-19

Client Reporting D-19

Roaming and Real-Time Diagnostics D-20

Using the GUI to Configure the Diagnostic Channel D-20

Using the CLI to Configure the Diagnostic Channel D-21

Using the GUI to Configure Client Reporting D-25

Using the CLI to Configure Client Reporting D-28

Using the CLI to Configure Roaming and Real-Time Diagnostics D-31

Using the Debug Facility D-34

Configuring Wireless Sniffing D-39

Prerequisites for Wireless Sniffing D-39

Using the GUI to Configure Sniffing on an Access Point D-39

Using the CLI to Configure Sniffing on an Access Point D-41

Troubleshooting Access Points Using Telnet or SSH D-42

Debugging the Access Point Monitor Service D-43

Using the CLI to Debug Access Point Monitor Service Issues D-43

APPENDIX E

Logical Connectivity Diagrams E-1

Cisco WiSM E-2

Cisco 28/37/38xx Integrated Services Router E-3

Catalyst 3750G Integrated Wireless LAN Controller Switch E-4

INDEX

Preface

This preface provides an overview of the *Cisco Wireless LAN Controller Configuration Guide*, *Release 5.2*, references related publications, and explains how to obtain other documentation and technical assistance, if necessary. It contains these sections:

- Audience, page xxiv
- Purpose, page xxiv
- Organization, page xxiv
- Conventions, page xxv
- Related Publications, page xxvii
- Obtaining Documentation and Submitting a Service Request, page xxvii

Audience

This guide describes Cisco Wireless LAN Controllers and Cisco Lightweight Access Points. This guide is for the networking professional who installs and manages these devices. To use this guide, you should be familiar with the concepts and terminology of wireless LANs.

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 5.2. 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:

Chapter 1, "Overview," provides an overview of the network roles and features of wireless LAN controllers.

Chapter 2, "Using the Web-Browser and CLI Interfaces," describes how to use the controller GUI and CLI.

Chapter 3, "Configuring Ports and Interfaces," describes the controller's physical ports and interfaces and provides instructions for configuring them.

Chapter 4, "Configuring Controller SettingsWireless Device Access," describes how to configure settings on the controllers.

Chapter 5, "Configuring Security Solutions," describes application-specific solutions for wireless LANs.

Chapter 6, "Configuring WLANsWireless Device Access," describes how to configure wireless LANs and SSIDs on your system.

Chapter 7, "Controlling Lightweight Access Points," explains how to connect lightweight access points to the controller and manage access point settings.

Chapter 8, "Controlling Mesh Access Points," explains how to connect mesh access points to the controller and manage access point settings.

Chapter 9, "Managing Controller Software and Configurations," describes how to upgrade and manage controller software and configurations.

Chapter 10, "Managing User Accounts," explains how to create and manage guest user accounts, describes the web authentication process, and provides instructions for customizing the web authentication login.

Chapter 11, "Configuring Radio Resource ManagementWireless Device Access," describes radio resource management (RRM) and explains how to configure it on the controllers.

Chapter 12, "Configuring Mobility GroupsWireless Device Access," describes mobility groups and explains how to configure them on the controllers.

Chapter 13, "Configuring Hybrid REAPWireless Device Access," describes hybrid REAP and explains how to configure this feature on controllers and access points.

Appendix A, "Safety Considerations and Translated Safety Warnings," lists safety considerations and translations of the safety warnings that apply to the Cisco Unified Wireless Network Solution products.

Appendix B, "Declarations of Conformity and Regulatory Information," provides declarations of conformity and regulatory information for the products in the Cisco Unified Wireless Network Solution.

Appendix C, "End User License and Warranty," describes the end user license and warranty that apply to the Cisco Unified Wireless Network Solution products.

Appendix D, "Troubleshooting," describes the LED patterns on controllers and lightweight access points, lists system messages that can appear on the Cisco Unified Wireless Network Solution interfaces, and provides CLI commands that can be used to troubleshoot problems on the controller.

Appendix E, "Logical Connectivity Diagrams,"provides logical connectivity diagrams and related software commands for controllers that are integrated into other Cisco products.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in boldface text.
- Arguments for which you supply values are in italic.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **boldface**.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and timesavers use these conventions and symbols:

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

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

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

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

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

Attention **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)**

Related Publications

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

- *Quick Start Guide*: *Cisco 2100 Series Wireless LAN Controllers*
- *Quick Start Guide*: *Cisco 4400 Series Wireless LAN Controllers*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless Control System Configuration Guide*
- *Quick Start Guide: Cisco Wireless Control System*
- Quick start guide and hardware installation guide for your specific lightweight access point

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

http://www.cisco.com/cisco/web/psa/default.html

Obtaining Documentation and Submitting a Service Request

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

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

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

CHAPTER 1

Overview

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

- Cisco Unified Wireless Network Solution Overview, page 1-2
- Operating System Software, page 1-5
- Operating System Security, page 1-5
- Layer 2 and Layer 3 Operation, page 1-6
- Cisco Wireless LAN Controllers, page 1-7
- Controller Platforms, page 1-8
- Cisco UWN Solution Wired Connections, page 1-12
- Cisco UWN Solution WLANs, page 1-13
- Identity Networking, page 1-13
- File Transfers, page 1-14
- Power over Ethernet, page 1-14
- Startup Wizard, page 1-15
- Cisco Wireless LAN Controller Memory, page 1-16
- Cisco Wireless LAN Controller Failover Protection, page 1-16
- Network Connections to Cisco Wireless LAN Controllers, page 1-17

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 2.
- A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco Wireless LAN Controllers. See Chapter 2.
- The Cisco Wireless Control System (WCS), which you use to configure and monitor one or more Cisco Wireless LAN Controllers and associated access points. WCS has tools to facilitate large-system monitoring and control. WCS runs on Windows 2000, Windows 2003, and Red Hat Enterprise Linux ES servers.

  Note WCS software release 5.2 must be used with controllers running controller software release 5.2. Do not attempt to use older versions of WCS software with controllers running controller software release 5.2.

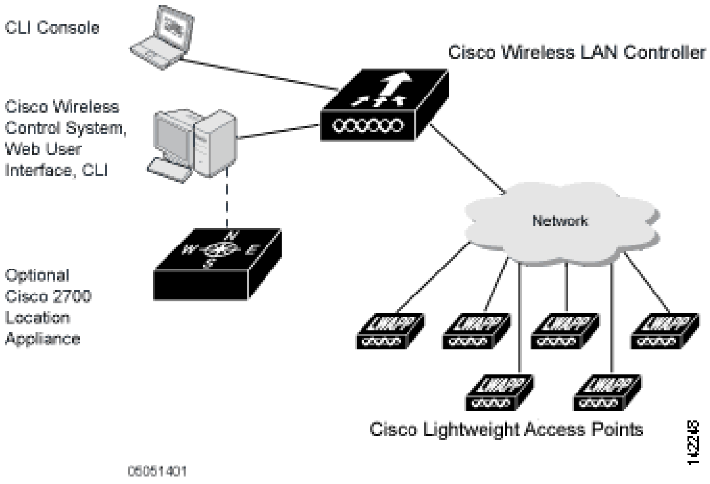
- An industry-standard SNMP V1, V2c, and V3 interface can be used with any SNMP-compliant third-party network management system.

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, all of the Cisco wireless LAN controllers are hereafter referred to as *controllers*, and all of the Cisco lightweight access points are hereafter referred to as *access points*.

Figure 1-1 shows the Cisco Wireless LAN Solution components, which can be simultaneously deployed across multiple floors and buildings.

Figure 1-1 Cisco UWN Solution Components


CLI Console
Cisco Wireless LAN Controller
Cisco Wireless Control System, Web User Interface, CLI
Network
Optional Cisco 2700 Location Appliance
LWAPP
Cisco Lightweight Access Points
142248
05051401

Single-Controller Deployments

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

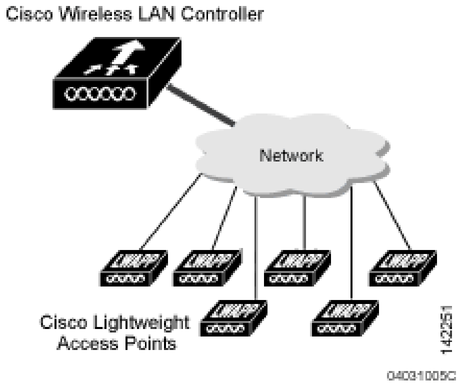
- Autodetecting and autoconfiguring lightweight access points as they are added to the network.
- Full control of lightweight access points.
- Lightweight access points connect to controllers through the network. The network equipment may or may not provide Power over Ethernet to the access points.

Note that 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 operators want to confine multiple VLANs to separate subnets.

Figure 1-2 shows a typical single-controller deployment.

Figure 1-2 Single-Controller Deployment


Cisco Wireless LAN Controller
Network
LWAPP
Cisco Lightweight Access Points
142251
04031005C

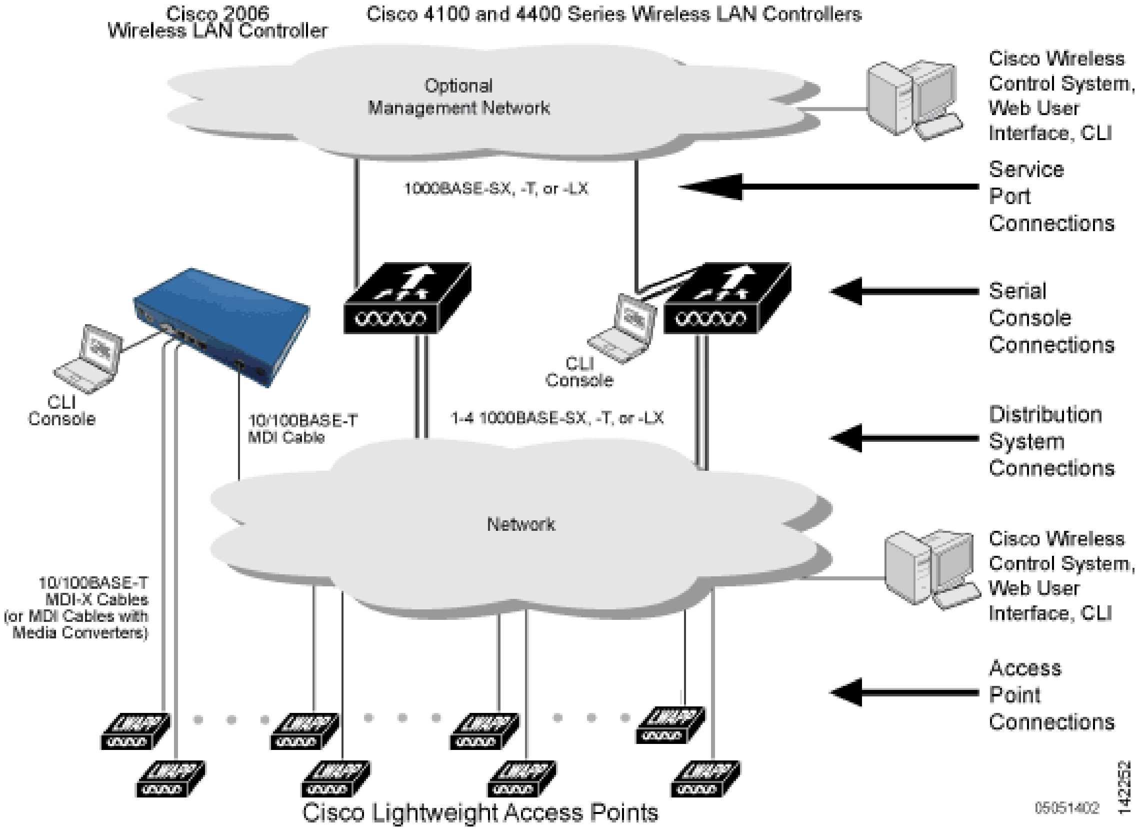
Multiple-Controller Deployments

Each controller can support lightweight access points across multiple floors and buildings simultaneously. However, full functionality of the Cisco Wireless LAN Solution is realized 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 (refer to the "Cisco Wireless LAN Controller Failover Protection" section on page 1-16).

Figure 1-3 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.

Figure 1-3 Typical Multi-Controller Deployment



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. (Refer to the "Cisco UWN Solution WLANs" section on page 1-13.)

The 802.11 Static WEP weaknesses can be overcome using robust industry-standard security solutions, such as:

- 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) + message integrity code checksum (Michael) dynamic keys, or
  - WEP keys, with or without Pre-Shared key Passphrase.
- RSN with or without Pre-Shared key.
- Optional MAC filtering.

The WEP problem can be further solved using industry-standard Layer 3 security solutions, such as:

- Passthrough VPNs
- The Cisco Wireless LAN Solution supports local and RADIUS MAC address filtering.
- The Cisco Wireless LAN Solution supports local and RADIUS user/password authentication.
- The Cisco Wireless LAN Solution also uses manual and automated disabling to block access to network services. In manual disabling, the operator blocks access using client MAC addresses. In automated disabling, which is always active, the operating system software automatically blocks access to network services for an operator-defined period of time when a client fails to authenticate for a fixed number of consecutive attempts. This 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

Many traditional access point vendors concentrate on security for the Wireless interface similar to that described in the "Operating System Security" section on page 1-5. However, for secure Cisco Wireless LAN Controller Service Interfaces, Cisco Wireless LAN Controller to access point, and inter-Cisco Wireless LAN Controller communications during device servicing and client roaming, the operating system includes built-in security.

Each Cisco Wireless LAN 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 Cisco Wireless LAN Controller or lightweight access point.

Cisco Wireless LAN Controllers and lightweight access points also use the signed certificates to verify downloaded code before it is loaded, ensuring that hackers do not download malicious code into any Cisco Wireless LAN 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 ISO Data Link Layer 2 or Network Layer 3. Control and Provisioning of Wireless Access Points protocol (CAPWAP) communications between the controller and lightweight access points are conducted at Network Layer 3. Layer 2 mode does not support CAPWAP.

Note Controller software release 5.2 or later supports 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 4400 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 Cisco Wireless LAN Controller deployments network, it is convenient to have all lightweight access points associate with one master controller on the same subnet. That way, the operator does not have to log into multiple controllers to find out which controller newly-added lightweight access points 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 Cisco Wireless LAN Controller. This process is described in the "Cisco Wireless LAN Controller Failover Protection" section on page 1-16.

The operator can monitor the master controller using the WCS Web User Interface and watch as access points associate with the master controller. The operator can then verify 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, assign primary, secondary, and tertiary controllers to each access point. Cisco recommends 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 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, refer to the *Cisco Wireless Control System Configuration Guide* and the *Cisco Location Appliance Configuration Guide* at these URLs:

Cisco Wireless Control System Configuration Guide:

http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

Cisco Location Appliance Configuration Guide:

http://www.cisco.com/en/US/products/ps6386/products_installation_and_configuration_guides_list.html

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. The 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 for use with software release 5.2:

- Cisco 2100 series controllers
- Cisco 4400 series controllers
- Catalyst 6500 Series Wireless Services Module (WiSM)
- Cisco 7600 Series Router Wireless Services Module (WiSM)
- Cisco 28/37/38xx Series Integrated Services Router with Controller Network Module
- Catalyst 3750G Integrated Wireless LAN Controller Switch

The first three controllers are stand-alone platforms. The remaining four controllers are integrated into Cisco switch and router products.

Cisco 2100 Series Controllers

The Cisco 2100 Series Wireless LAN Controllers work in conjunction with Cisco lightweight access points and the Cisco Wireless Control System (WCS) to provide system-wide wireless LAN functions. Each 2100 series controller controls up to 6, 12, or 25 lightweight access points for multi-controller architectures typical of enterprise branch deployments. It may also be used for single controller deployments for small and medium-sized environments.

Caution Do not connect a power-over-Ethernet (PoE) cable to the controller's console port. Doing so may damage the controller.

Note Wait at least 20 seconds before reconnecting an access point to the controller. Otherwise, the controller may fail to detect the device.

Features Not Supported

This hardware feature is not supported on 2100 series controllers:

- Service port (separate out-of-band management 10/100-Mbps Ethernet interface)

These software features are not supported on 2100 series controllers:

- VPN termination (such as IPSec and L2TP)
- Termination of guest controller tunnels (origination of guest controller tunnels is supported)
- External web authentication web server list
- Spanning tree
- Port mirroring
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)
- Multicast-unicast mode

Cisco 4400 Series Controllers

The Cisco 4400 Series Wireless LAN Controller is available in two models: 4402 and 4404. The 4402 supports up to 50 lightweight access points while the 4404 supports up to 100, making it ideal for large-sized enterprises and large-density applications.

Figure - Cisco 4400 Series Wireless LAN Controller

The Cisco 4400 Series Wireless LAN Controller can be factory-ordered with a VPN/Enhanced Security Module (Crypto Card) to support VPN, IPSec and other processor-intensive tasks. The VPN/Enhanced Security Module can also be installed in the field.
The 4400 series controller can be equipped with one or two Cisco 4400 series power supplies. When the controller is equipped with two Cisco 4400 series power supplies, the power supplies are redundant, and either power supply can continue to power the controller if the other power supply fails.

Catalyst 6500 Series Wireless Services Module

The Catalyst 6500 Series Wireless Services Module (WiSM) is an integrated Catalyst 6500 switch and two Cisco 4404 controllers that supports up to 300 lightweight access points. The switch has eight internal Gigabit Ethernet ports that connect the switch and the controller. The switch and the internal controller run separate software versions, which must be upgraded separately.

Note Without any other service module installed, the Catalyst 6509 switch chassis can support up to seven Cisco WiSMs, and the Catalyst 6506 with a Supervisor 720 can support up to four Cisco WiSMs. If one or more service modules are installed, the chassis can support up to a maximum of four service modules (WiSMs included). Redundant supervisors cannot be used with these maximum configurations.

Refer to the following documents for additional information:

- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Wireless Services Module Installation and Configuration Note*
- *Release Notes for Catalyst 6500 Series Switch Wireless LAN Services Module*
- *Configuring a Cisco Wireless Services Module and Wireless Control System*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Wireless Services Module Installation and Verification Note*

You can find these documents at these URLs:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

http://www.cisco.com/en/US/docs/wireless/technology/wism/technical/reference/appnote.html

http://www.cisco.com/en/US/docs/wireless/technology/wism/installation/note/78_17121.html

Cisco 7600 Series Router Wireless Services Module

The Cisco 7600 Series Router Wireless Services Module (WiSM) is an integrated Cisco 7600 router and two Cisco 4404 controllers that supports up to 300 lightweight access points. The router has eight internal Gigabit Ethernet ports that connect the router and the controller. The router and the internal controller run separate software versions, which must be upgraded separately.

Note The WiSM is supported on Cisco 7600 series routers running only Cisco IOS Release 12.2(18)SXF5 or later.

Note Without any other service module installed, the Cisco 7609 router chassis can support up to seven Cisco WiSMs, and any other Cisco 7600 series router chassis can support up to six Cisco WiSMs. If one or more service modules are installed, the chassis can support up to a maximum of four service modules (WiSMs included). Redundant supervisors cannot be used with these maximum configurations.

Refer to the following documents for additional information:

- *Cisco 7600 Series Router Installation Guide*
- *Cisco 7600 Series Router Software Configuration Guide*
- *Cisco 7600 Series Router Command Reference*
- *Configuring a Cisco Wireless Services Module and Wireless Control System*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Wireless Services Module Installation and Verification Note*

You can find these documents at these URLs:

http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html

http://www.cisco.com/en/US/docs/wireless/technology/wism/technical/reference/appnote.html

http://www.cisco.com/en/US/docs/wireless/technology/wism/installation/note/78_17121.html

Cisco 28/37/38xx Series Integrated Services Router

The Cisco 28/37/38xx Series Integrated Services Router is an integrated 28/37/38xx router and Cisco controller network module that supports up to 6, 8, 12, or 25 lightweight access points, depending on the version of the network module. The versions that support 8, 12, or 25 access points and the NME-AIR-WLC6-K9 6-access-point version feature a high-speed processor and more on-board memory than the NM-AIR-WLC6-K9 6-access-point version. An internal Fast Ethernet port (on the NM-AIR-WLC6-K9 6-access-point version) or an internal Gigabit Ethernet port (on the 8-, 12-, and 25-access-point versions and on the NME-AIR-WLC6-K9 6-access-point version) connects the router and the integrated controller. The router and the internal controller run separate software versions, which must be upgraded separately. Refer to the following documents for additional information:

- *Cisco Wireless LAN Controller Network Module Feature Guide*
- *Cisco 28/37/38xx Series Hardware Installation Guide*

You can find these documents at this URL:

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

Note The Cisco 2801 Integrated Services Router does not support the controller network module.

Catalyst 3750G Integrated Wireless LAN Controller Switch

The Catalyst 3750G Integrated Wireless LAN Controller Switch is an integrated Catalyst 3750 switch and Cisco 4400 series controller that supports up to 25 or 50 lightweight access points. The switch has two internal Gigabit Ethernet ports that connect the switch and the controller. The switch and the internal controller run separate software versions, which must be upgraded separately. Refer to the following documents for additional information:

- *Catalyst 3750G Integrated Wireless LAN Controller Switch Getting Started Guide*
- *Catalyst 3750 Switch Hardware Installation Guide*
- *Release Notes for the Catalyst 3750 Integrated Wireless LAN Controller Switch, Cisco IOS Release 12.2(25)FZ*

You can find these documents at this URL:

http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html

Cisco UWN Solution Wired Connections

The Cisco UWN Solution components communicate with each other using industry-standard Ethernet cables and connectors. The following paragraphs contain details of the wired connections.

- The 2100 series controller connects to the network using from one to six 10/100BASE-T Ethernet cables.
- The 4402 controller connects to the network using one or two fiber-optic Gigabit Ethernet cables, and the 4404 controller connects to the network using up to four fiber-optic Gigabit Ethernet cables: two redundant Gigabit Ethernet connections to bypass single network failures.
- The controllers in the Wireless Services Module (WiSM), installed in a Cisco Catalyst 6500 Series Switch or a Cisco 7600 Series Router, connect to the network through ports on the switch or router.
- The Wireless LAN Controller Network Module, installed in a Cisco Integrated Services Router, connects to the network through the ports on the router.
- The controller in the Catalyst 3750G Integrated Wireless LAN Controller Switch connects to the network through the ports on the switch.
- Cisco lightweight access points connects 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 16 WLANs for lightweight access points. Each WLAN has a separate WLAN ID (1 through 16), a separate WLAN SSID (WLAN name), and can be assigned unique security policies. Using software release 3.2 and later, you can configure both static and dynamic WEP on the same WLAN.

The lightweight access points broadcast all active Cisco UWN Solution WLAN SSIDs and enforce the policies defined for each WLAN.

Note Cisco recommends 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, the operator can manage the system across the enabled WLAN using CLI and Telnet, http/https, and SNMP.

To configure WLANs, refer to Chapter 6.

Identity Networking

Controllers can have the following parameters applied to all clients associating with a particular wireless LAN: QoS, global or Interface-specific DHCP server, Layer 2 and Layer 3 Security Policies, and default Interface (which includes physical port, VLAN and ACL assignments).

However, the controllers can also have individual clients (MAC addresses) override the preset wireless LAN parameters by using MAC Filtering or by Allowing AAA Override parameters. This configuration can be used, for example, to have all company clients log into the corporate wireless LAN, and then have clients connect using different QoS, DHCP server, Layer 2 and Layer 3 Security Policies, and Interface (which includes physical port, VLAN and ACL assignments) settings on a per-MAC Address basis.

When Cisco UWN Solution operators configure MAC Filtering for a client, they can assign a different VLAN to the MAC Address, which can be used to have operating system automatically reroute the client to the management interface or any of the operator-defined interfaces, each of which have their own VLAN, access control list (ACL), DHCP server, and physical port assignments. This MAC Filtering can be used as a coarse version of AAA Override, and normally takes precedence over any AAA (RADIUS or other) Override.

However, when Allow AAA Override is enabled, the RADIUS (or other AAA) server can alternatively be configured to return QoS, DSCP, 802.1p priority tag values and ACL on a per-MAC Address basis. Allow AAA Override gives the AAA Override precedence over the MAC Filtering parameters set in the controller; if there are no AAA Overrides available for a given MAC Address, the operating system uses the MAC Filtering parameters already in the controller. This AAA (RADIUS or other) Override can be used as a finer version of AAA Override, but only takes precedence over MAC Filtering when Allow AAA Override is enabled.

Note that in all cases, the Override parameters (Operator-Defined Interface and QoS, for example) must already be defined in the controller configuration.

In all cases, the operating system will use QoS, DSCP, 802.1p priority tag values and ACL provided by the AAA server or MAC Filtering regardless of the Layer 2 and/or Layer 3 authentication used.

Also note that the operating system only moves clients from the default Cisco UWN Solution WLAN VLAN to a different VLAN when configured for MAC filtering, 802.1X, and/or WPA Layer 2 authentication. To configure WLANs, refer to Chapter 6.

Enhanced Integration with Cisco Secure ACS

The identity-based networking feature uses authentication, authorization, and accounting (AAA) override. When the following vendor-specific attributes are present in the RADIUS access accept message, the values override those present in the wireless LAN profile:

- QoS level
- 802.1p value
- VLAN interface name
- Access control list (ACL) name

In this release, support is being added for the AAA server to return the VLAN number or name using the standard "RADIUS assigned VLAN name/number" feature defined in IETF RFC 2868 (RADIUS Attributes for Tunnel Protocol Support). To assign a wireless client to a particular VLAN, the AAA server sends the following attributes to the controller in the access accept message:

- IETF 64 (Tunnel Type): VLAN
- IETF 65 (Tunnel Medium Type): 802
- IETF 81 (Tunnel Private Group ID): VLAN # or VLAN Name String

This enables Cisco Secure ACS to communicate a VLAN change that may be a result of a posture analysis. Benefits of this new feature include:

- Integration with Cisco Secure ACS reduces installation and setup time
- Cisco Secure ACS operates smoothly across both wired and wireless networks

This feature supports 2100 and 4400 series controllers and 1130 and 1200 series lightweight access points.

File Transfers

The Cisco UWN Solution operator can upload and download operating system code, configuration, and certificate files to and from controller using the GUI, CLI commands, or Cisco WCS.

- To use CLI commands, refer to the "Transferring Files to and from a Controller" section on page 8-7.
- To use Cisco WCS to upgrade software, refer to the *Cisco Wireless Control System Configuration Guide*. Click this URL to browse to this document:

  http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

Power over Ethernet

Lightweight access points can receive power via 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 installer time. PoE also frees installers from having to mount Cisco 1000 series lightweight access points or other powered equipment near AC outlets, providing greater flexibility in positioning Cisco 1000 series lightweight access points for maximum coverage.

When you are using PoE, the installer runs 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 lightweight 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.

Startup Wizard

When a controller is powered up with a new factory operating system software load or after being reset to factory defaults, the bootup script runs the Startup Wizard, which prompts the installer for initial configuration. The Startup Wizard:

- Ensures that the controller has a System Name, up to 32 characters.
- Adds an Administrative username and password, each up to 24 characters.
- Ensures that the controller can communicate with the GUI, CLI, or Cisco WCS (either directly or indirectly) through the service port by accepting a valid IP configuration protocol (none or DHCP), and if none, IP Address and netmask. If you do not want to use the service port, enter 0.0.0.0 for the IP Address and netmask.
- Ensures that the controller can communicate with the network (802.11 Distribution System) through the management interface by collecting a valid static IP Address, netmask, default router IP address, VLAN identifier, and physical port assignment.
- Prompts for the IP address of the DHCP server used to supply IP addresses to clients, the controller management interface, and optionally to the service port interface.
- Collects the Virtual Gateway IP Address; any fictitious, unassigned IP address (such as 1.1.1.1) to be used by Layer 3 Security and Mobility managers.
- Allows you to enter the Mobility Group (RF Group) Name.
- Collects the wireless LAN 1 802.11 SSID, or Network Name.
- Asks you to define whether or not clients can use static IP addresses. Yes = more convenient, but lower security (session can be hijacked), clients can supply their own IP Address, better for devices that cannot use DHCP. No = less convenient, higher security, clients must DHCP for an IP Address, works well for s XP devices.
- If you want to configure a RADIUS server from the Startup Wizard, the RADIUS server IP address, communication port, and Secret.
- Collects the Country Code.
- Enables or disables the 802.11a/n and 802.11b/g/n lightweight access point networks.
- Enables or disables radio resource management (RRM).

To use the Startup Wizard, refer to the "Using the Configuration Wizard" section on page 4-2.

Cisco Wireless LAN Controller Memory

The controller contains two kinds of memory: volatile RAM, which holds the current, active controller configuration, and NVRAM (non-volatile 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:

- Using the Configuration Wizard
- Clearing the Controller Configuration
- Saving Configurations
- Resetting the Controller
- Logging Out of the CLI

Cisco Wireless LAN Controller Failover Protection

Each controller has a defined number of communication ports for lightweight access points. This means that when multiple controllers with unused access point ports are deployed on the same network, if one controller fails, the dropped access points automatically poll for unused controller ports and associate with them.

During installation, Cisco recommends 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 configured lightweight access points obtain an IP address from the local DHCP server (only in Layer 3 operation), attempt to contact their primary, secondary, and tertiary controllers, and then attempt to contact the IP addresses of the other controllers in the Mobility group. This prevents the access points from spending time sending out blind polling messages, resulting in a faster recovery period.

In multiple-controller deployments, this means that if one controller fails, its dropped access points reboot and do the following under direction of the radio resource management (RRM):

- Obtain an IP address from a local DHCP server (one on the local subnet).
- 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 on the same subnet.
- If the access point finds no master controller on the same subnet, it attempts to contact stored mobility group members by IP address.
- Should none of the mobility group members be 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 on the same subnet to respond to its discovery messages with unused ports.

This means that when sufficient controllers are deployed, should one controller fail, active access point client sessions are momentarily dropped while the dropped access point associates with an unused port on another controller, allowing the client device to immediately reassociate and reauthenticate.

Network Connections to Cisco Wireless LAN Controllers

Regardless of operating mode, all controllers use the network as an 802.11 distribution system. Regardless of the Ethernet port type or speed, each controller monitors and communicates with its related controllers across the network. The following sections give details of these network connections:

- Cisco 2100 Series Wireless LAN Controllers, page 1-17
- Cisco 4400 Series Wireless LAN Controllers, page 1-18

Note Chapter 3 provides information on configuring the controller's ports and assigning interfaces to them.

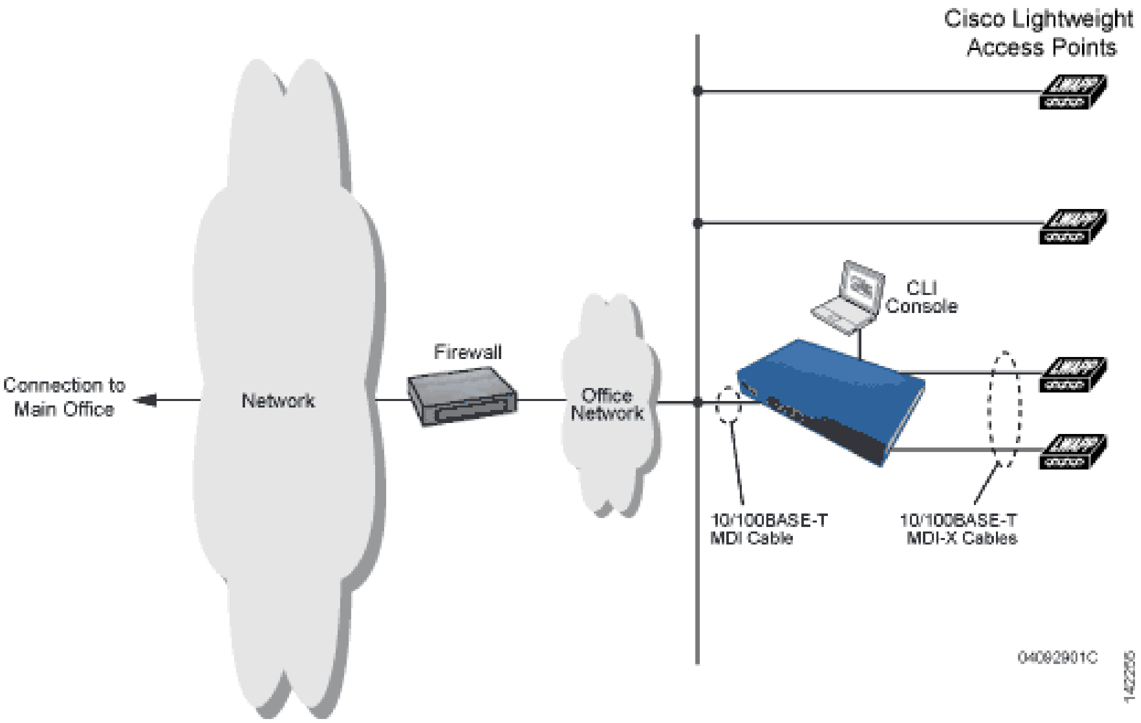
Cisco 2100 Series Wireless LAN Controllers

Cisco 2100 series controllers can communicate with the network through any one of their physical data ports, as the logical management interface can be assigned to one of the ports. The physical port description is as follows:

- Up to six 10/100BASE-T cables can plug into the six back-panel data ports on the 2100 series controller chassis. The 2100 series also has two PoE ports (ports 7 and 8).

Figure 1-4 shows connections to the 2100 series controllers.

Figure 1-4 Physical Network Connections to the 2100 Series Controller


Cisco Lightweight Access Points
CLI Console
Connection to Main Office
Network
Firewall
Office Network
10/100BASE-T MDI Cable
10/100BASE-T MDI-X Cables
04092901C
142255

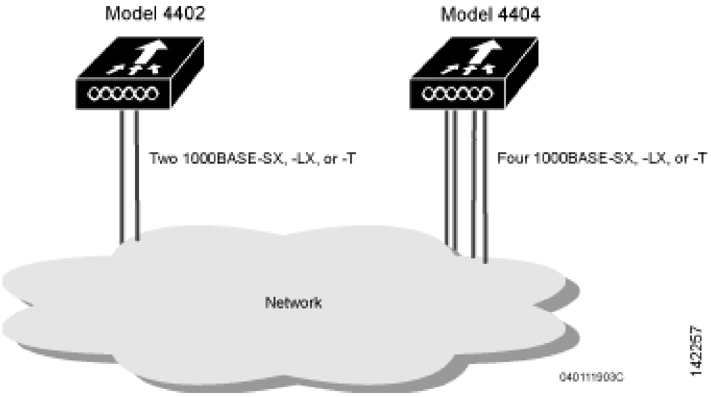
Cisco 4400 Series Wireless LAN Controllers

Cisco 4400 series controllers can communicate with the network through one or two pairs of physical data ports, and the logical management interface can be assigned to the ports. The physical port descriptions follows:

- For the 4402 controller, up to two of the following connections are supported in any combination:
  - 1000BASE-T (Gigabit Ethernet, front panel, RJ-45 physical port, UTP cable).
  - 1000BASE-SX (Gigabit Ethernet, front panel, LC physical port, multi-mode 850nM (SX) fiber-optic links using LC physical connectors).
  - 1000BASE-LX (Gigabit Ethernet, front panel, LC physical port, multi-mode 1300nM (LX/LH) fiber-optic links using LC physical connectors).
- For the 4404 controller, up to four of the following connections are supported in any combination:
  - 1000BASE-T (Gigabit Ethernet, front panel, RJ-45 physical port, UTP cable).
  - 1000BASE-SX (Gigabit Ethernet, front panel, LC physical port, multi-mode 850nM (SX) fiber-optic links using LC physical connectors).
  - 1000BASE-LX (Gigabit Ethernet, front panel, LX physical port, multi-mode 1300nM (LX/LH) fiber-optic links using LC physical connectors).

Figure 1-5 shows connections to the 4400 series controller.

Figure 1-5 Physical Network Connections to 4402 and 4404 Series Controllers



CHAPTER 2

Using the Web-Browser and CLI Interfaces

This chapter describes the web-browser and CLI interfaces that you use to configure the controller. It contains these sections:

- Using the Web-Browser Interface, page 2-2
- Using the CLI, page 2-7
- Enabling Wireless Connections to the Web-Browser and CLI Interfaces, page 2-9

Using the Web-Browser Interface

The web-browser interface (hereafter called the 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 operational status for the controller and its associated access points.

Note Cisco recommends that you enable the HTTPS interface and disable the HTTP interface to ensure more robust security for your Cisco UWN Solution.

Guidelines for Using the GUI

Keep these guidelines in mind when using the 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).

  Note Opera and Netscape are not supported.

  Note 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.

- You can use either the service port interface or the management interface to access the GUI. Cisco recommends that you use the service-port interface. Refer to Chapter 3 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.

Opening the GUI

To open the GUI, enter the controller IP address in the browser's address line. For a secure connection, enter **https://*ip-address***. For a less secure connection, enter **http://*ip-address***. See the "Using the GUI to Enable Web and Secure Web Modes" section on page 2-3 for instructions on setting up HTTPS.

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.

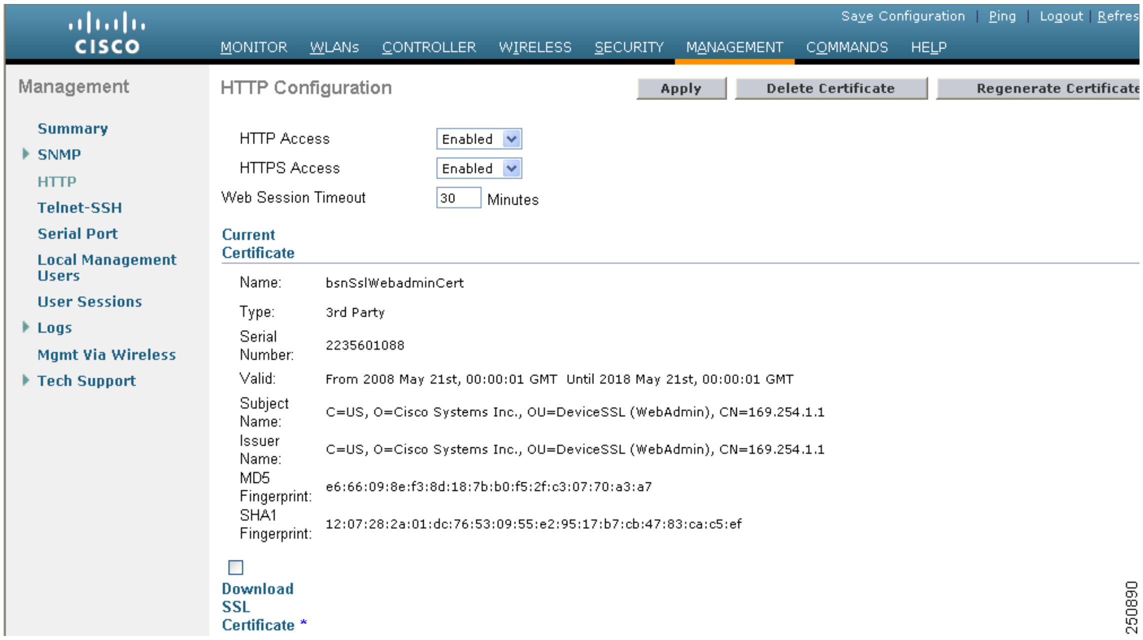
You can configure web and secure web mode using the controller GUI or CLI.

Using the GUI to Enable Web and Secure Web Modes

Follow these steps to enable web mode, secure web mode, or both using the controller GUI.

Step 1 Click **Management** > **HTTP** to open the HTTP Configuration page (see Figure 2-1).

Figure 2-1 HTTP Configuration Page



HTTP Configuration

HTTP Access: Enabled

HTTPS Access: Enabled

Web Session Timeout: 30 Minutes

Current Certificate

Name:	bsnSslWebadminCert
Type:	3rd Party
Serial Number:	2235601088
Valid:	From 2008 May 21st, 00:00:01 GMT Until 2018 May 21st, 00:00:01 GMT
Subject Name:	C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAdmin), CN=169.254.1.1
Issuer Name:	C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAdmin), CN=169.254.1.1
MD5 Fingerprint:	e6:66:09:8e:f3:8d:18:7b:b0:f5:2f:c3:07:70:a3:a7
SHA1 Fingerprint:	12:07:28:2a:01:dc:76:53:09:55:e2:95:17:b7:cb:47:83:ca:c5:ef

☐ Download SSL Certificate *

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 box. 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 box. Otherwise, choose **Disabled**. The default value is Enabled. Secure web mode is a secure connection.

Step 4 In the Web Session Timeout field, 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 (see Figure 2-1).

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 2-5.

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.

Using the CLI to Enable Web and Secure Web Modes

Follow these steps to enable web mode, secure web mode, or both using the controller 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 2-5.

Step 6 (Optional) If you need to generate a new certificate, enter this command:

config certificate generate webadmin

After a few seconds, the controller verifies that the certificate has been generated.

Step 7 To save the SSL certificate, key, and secure web password to non-volatile RAM (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

Loading an Externally Generated SSL Certificate

You can use a TFTP server to download an externally generated SSL certificate to the controller. Follow these guidelines for using TFTP:

- 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 computer as the Cisco WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.

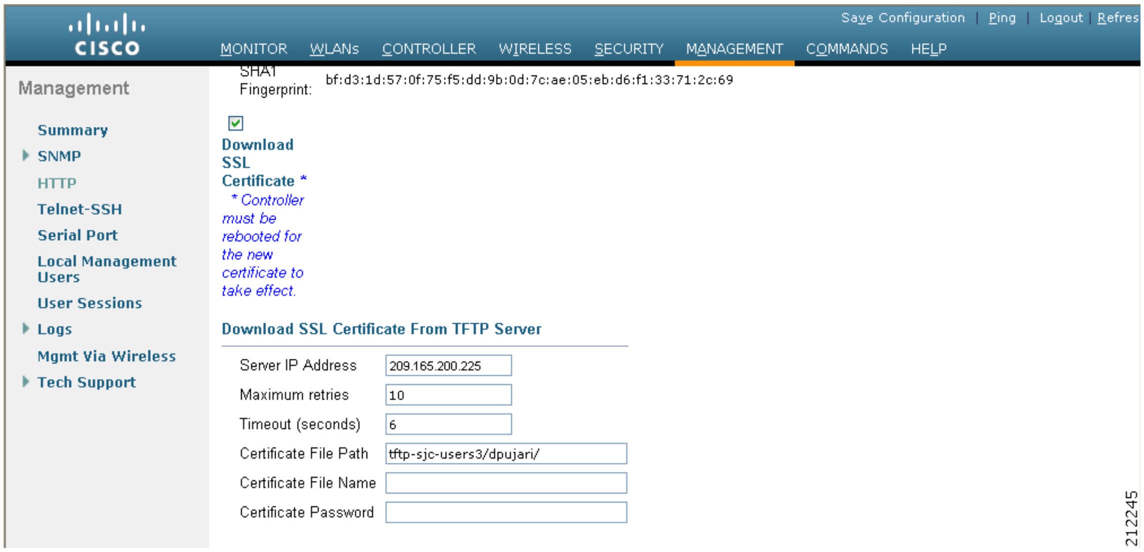
Note Every HTTPS certificate contains an embedded RSA key. The length of the key can vary from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you obtain a new certificate from a Certificate Authority, make sure that the RSA key embedded in the certificate is at least 768 bits long.

Using the GUI to Load an SSL Certificate

Follow these steps to load an externally generated SSL certificate using the controller GUI.

Step 1 On the HTTP Configuration page, check the **Download SSL Certificate** check box (see Figure 2-2).

Figure 2-2 HTTP Configuration Page



SHA1 Fingerprint: bf:d3:1d:57:0f:75:f5:dd:9b:0d:7c:ae:05:eb:d6:f1:33:71:2c:69

☑ Download SSL Certificate *

* Controller must be rebooted for the new certificate to take effect.

Download SSL Certificate From TFTP Server

Server IP Address	209.165.200.225
Maximum retries	10
Timeout (seconds)	6
Certificate File Path	tftp-sjc-users3/dpujari/
Certificate File Name	
Certificate Password	

Step 2 In the Server IP Address field, enter the IP address of the TFTP server.

Step 3 In the Maximum Retries field, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 4 In the Timeout field, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 5 In the Certificate File Path field, enter the directory path of the certificate.

Step 6 In the Certificate File Name field, enter the name of the certificate (*webadmincert_name*.pem).

Step 7 (Optional) In the Certificate Password field, 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, click **Commands** > **Reboot** > **Reboot** > **Save and Reboot**.

Using the CLI to Load an SSL Certificate

Follow these steps to load an externally generated SSL certificate using the controller 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>
TFTP Filename...............................
Are you sure you want to start? (y/n) n
Transfer Canceled
```

Step 4 Use these commands to change the download settings:

transfer download mode tftp

transfer download datatype webauthcert

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 CLI

The Cisco UWN Solution command line interface (CLI) is built into each controller. The CLI allows you to use a VT-100 emulator 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 emulators to access the controller.

Note Refer to the C*isco Wireless LAN Controller Command Reference* for information on specific commands.

Note If you want to input any strings from the XML configuration into CLI commands, you must enclose the strings in quotation marks.

Logging into the CLI

You access the CLI using one of two methods:

- A direct ASCII serial connection to the controller console port
- A remote console session over Ethernet through the pre-configured service port or the distribution system ports

Before you log into 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 computer that has a DB-9 serial port and is running a terminal emulation program
- A DB-9 male-to-female null-modem serial cable

Follow these steps to log into the CLI through the serial port.

Step 1 Connect your computer to the controller using the DB-9 null-modem serial cable.

Step 2 Open a terminal emulator session using these settings:

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

Step 3 At the prompt, log into the CLI. The default username is *admin*, and the default password is *admin*.

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.

Using a Remote Ethernet Connection

You need these items to connect to a controller remotely:

- A computer with access to the controller over the Ethernet network
- The IP address of the controller
- A 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.

Follow these steps to log into the CLI through a remote Ethernet connection.

Step 1 Verify that your terminal emulator 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 At the prompt, log into the CLI. The default username is *admin*, and the default password is *admin*.

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.

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 2-1 lists commands you use to navigate the CLI and to perform common tasks.

Table 2-1 Commands for CLI Navigation and Common Tasks

Command	Action
help	At the root level, view systemwide navigation commands
?	View commands available at the current level
command **?**	View parameters for a specific command
exit	Move down one level
Ctrl-Z	Return from any level to the root level
save config	At the root level, save configuration changes from active working RAM to non-volatile RAM (NVRAM) so they are retained after reboot
reset system	At the root level, reset the controller without logging out

Enabling Wireless Connections to the Web-Browser and CLI Interfaces

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. Follow these steps to enable wireless connections to the GUI or CLI.

Step 1 Log into the CLI.

Step 2 Enter **config network mgmt-via-wireless enable**.

Step 3 Use a wireless client to associate to a lightweight access point connected to the controller.

Step 4 On the wireless client, open a Telnet session to the controller, or browse to the controller GUI.

Tip To use the controller GUI to enable wireless connections, click **Management** > **Mgmt Via Wireless** page and check the **Enable Controller Management to be accessible from Wireless Clients** check box.

CHAPTER 3

Configuring Ports and Interfaces

This chapter describes the controller's physical ports and interfaces and provides instructions for configuring them. It contains these sections:

- Overview of Ports and Interfaces, page 3-2
- Configuring the Management, AP-Manager, Virtual, and Service-Port Interfaces, page 3-10
- Configuring Dynamic Interfaces, page 3-16
- Configuring Ports, page 3-19
- Enabling Link Aggregation, page 3-29
- Configuring a 4400 Series Controller to Support More Than 48 Access Points, page 3-34

Overview of Ports and Interfaces

Three concepts are key to understanding how controllers connect to a wireless network: ports, interfaces, and WLANs.

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. The following figures show the ports available on each controller.

Note The controller in a Cisco Integrated Services Router and the controllers on the Cisco WiSM do not have external physical ports. They connect to the network through ports on the router or switch.

Figure 3-1 Ports on the Cisco 2100 Series Wireless LAN Controllers

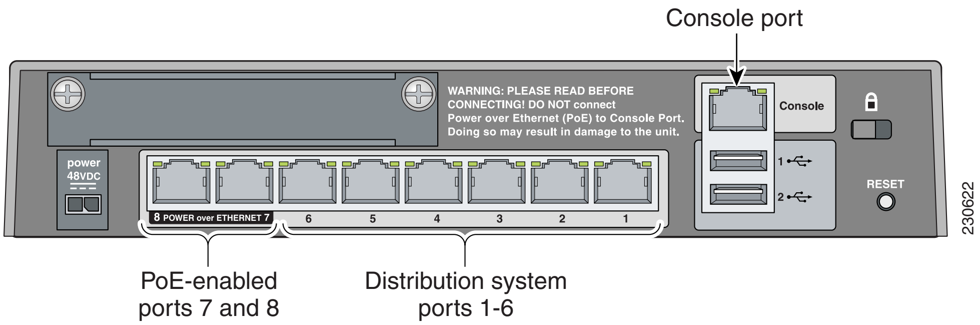
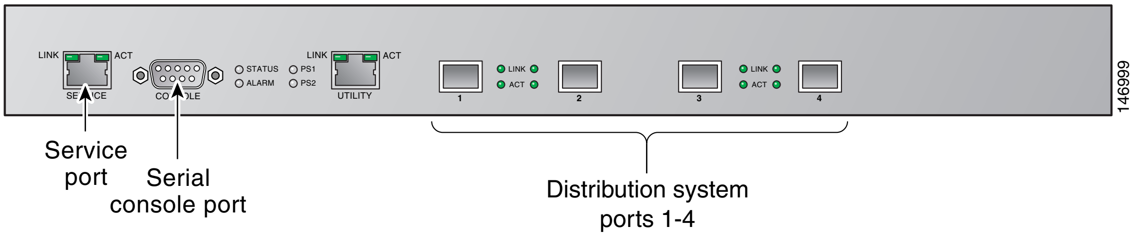

Console port
WARNING: PLEASE READ BEFORE CONNECTING! DO NOT connect Power over Ethernet (PoE) to Console Port. Doing so may result in damage to the unit.
Console
power 48VDC
8 POWER over ETHERNET 7
6
5
4
3
2
1
RESET
230622
PoE-enabled ports 7 and 8
Distribution system ports 1-6

Figure 3-2 Ports on the Cisco 4400 Series Wireless LAN Controllers



Note Figure 3-2 shows a Cisco 4404 controller. The Cisco 4402 controller is similar but has only two distribution system ports. The utility port, which is the unlabeled port in Figure 3-2, is currently not operational.

Figure 3-3 Ports on the Catalyst 3750G Integrated Wireless LAN Controller Switch

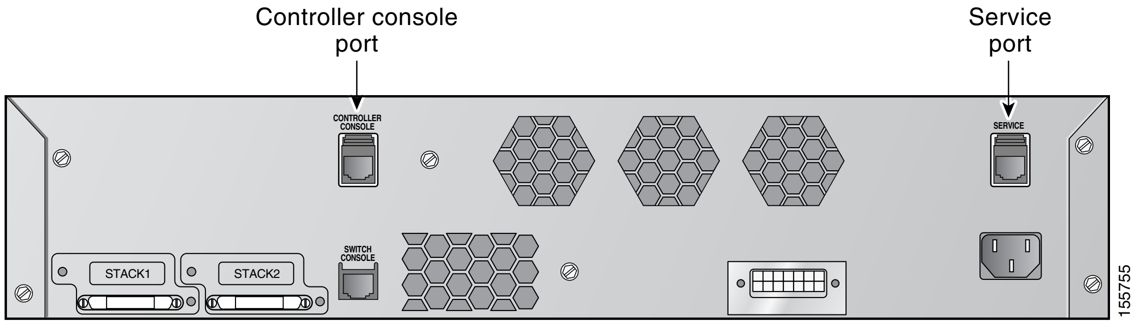


Table 3-1 provides a list of ports per controller.

Table 3-1 Controller Ports

Controller	Service Ports	Distribution System Ethernet Ports	Serial Console Port
2100 series	None	8 (6 + 2 PoE ports)	1
4402	1	2	1
4404	1	4	1
Cisco WiSM	2 (ports 9 and 10)	8 (ports 1-8)	2
Controller Network Module within the Cisco 28/37/38xx Series Integrated Services Routers	None	1	1[1]
Catalyst 3750G Integrated Wireless LAN Controller Switch	1	2 (ports 27 and 28)	1

[1] The baud rate for the Gigabit Ethernet version of the controller network module is limited to 9600 bps while the baud rate for the Fast Ethernet version supports up to 57600 bps.

Note Appendix E provides logical connectivity diagrams and related software commands for the integrated controllers.

Distribution System Ports

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

- Cisco 2100 series controllers have eight 10/100 copper Ethernet distribution system ports through which the controller can support up to 6, 12, or 25 access points. Two of these ports (7 and 8) are power-over-Ethernet (PoE) enabled and can be used to provide power directly to access points that are connected to these ports.

  Note All client connections to the 2100 series controllers are limited to the 10/100 Ethernet uplink port connection between the switch and the controller, even though their connection speeds might be higher. The exception is for access points running in local hybrid-REAP mode because this traffic is switched at the access point level and not forwarded back to the controller.

- Cisco 4402 controllers have two Gigabit Ethernet distribution system ports, each of which is capable of managing up to 48 access points. However, Cisco recommends no more than 25 access points per port due to bandwidth constraints. The 4402-25 and 4402-50 models allow a total of 25 or 50 access points to join the controller.
- Cisco 4404 controllers have four Gigabit Ethernet distribution system ports, each of which is capable of managing up to 48 access points. However, Cisco recommends no more than 25 access points per port due to bandwidth constraints. The 4404-25, 4404-50, and 4404-100 models allow a total of 25, 50, or 100 access points to join the controller.

Note The Gigabit Ethernet ports on the 4402 and 4404 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

- The Cisco Catalyst 6500 Series Switch Wireless Services Module (WiSM) and the Cisco 7600 Series Router Wireless Services Module (WiSM) have eight internal Gigabit Ethernet distribution system ports (ports 1 through 8) that connect the switch or router and the integrated controller. These internal ports are located on the backplane of the switch or router and are not visible on the front panel. Through these ports, the controller can support up to 300 access points.
- The controller network module within the Cisco 28/37/38xx Series Integrated Services Router can support up to 6, 8, 12, or 25 access points (and up to 256, 256, 350, or 350 clients, respectively), depending on the version of the network module. The network module supports these access points through a Fast Ethernet distribution system port (on the NM-AIR-WLC6-K9 6-access-point version) or a Gigabit Ethernet distribution system port (on the 8-, 12-, and 25-access-point versions and on the NME-AIR-WLC6-K9 6-access-point version) that connects the router and the integrated controller. This port is located on the router backplane and is not visible on the front panel. The Fast Ethernet port operates at speeds up to 100 Mbps, and the Gigabit Ethernet port operates at speeds up to 1 Gbps.

- The Catalyst 3750G Integrated Wireless LAN Controller Switch has two internal Gigabit Ethernet distribution system ports (ports 27 and 28) that connect the switch and the integrated controller. These internal ports are located on the switch backplane and are not visible on the front panel. Each port is capable of managing up to 48 access points. However, Cisco recommends no more than 25 access points per port due to bandwidth constraints. The -S25 and -S50 models allow a total of 25 or 50 access points to join the controller.

Note Refer to the "Configuring a 4400 Series Controller to Support More Than 48 Access Points" section on page 3-34 if you want to configure your Cisco 4400 series controller to support more than 48 access points.

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

Note Some controllers support link aggregation (LAG), which bundles all of the controller's distribution system ports into a single 802.3ad port channel. Cisco 4400 series controllers support LAG in software release 3.2 and higher, and LAG is enabled automatically on the Cisco WiSM controllers. Refer to the "Enabling Link Aggregation" section on page 3-29 for more information.

Service Port

Cisco 4400 series controllers also have a 10/100 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.

Note The Cisco WiSM's controllers use the service port for internal protocol communication between the controllers and the Supervisor 720.

Note The Cisco 2100 series controllers and the controller in the Cisco Integrated Services Router do not have a service port.

Note The service port is not auto-sensing. You must use the correct straight-through or crossover Ethernet cable to communicate with the service port.

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)
- 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.

Note Refer to the "Enabling Link Aggregation" section on page 3-29 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.

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. 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 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.

Note If the service port is in use, the management interface must be on a different supernet from the service-port interface.

AP-Manager Interface

A controller has one or more AP-manager interfaces, which are used for all Layer 3 communications between the controller and lightweight access points after the access points have joined the controller. The AP-manager IP address is used as the tunnel source for CAPWAP packets from the controller to the access point and as the destination for CAPWAP packets from the access point to the controller.

For Cisco 4404 and WiSM controllers, configure the AP-manager interface on all distribution system ports (1, 2, 3, and 4). For Cisco 4402 controllers, configure the AP-manager interface on distribution system ports 1 and 2. In both cases, the static (or permanent) AP-manager interface is always assigned to distribution system port 1 and given a unique IP address. Configuring the AP-manager interface on the same VLAN or IP subnet as the management interface results in optimum access point association, but this is not a requirement.

Note If LAG is enabled, there can be only one AP-manager interface. But when LAG is disabled, you must assign an AP-manager interface to each port on the controller.

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

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.

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

Note Refer to the "Using Multiple AP-Manager Interfaces" section on page 3-35 for information on creating and using multiple AP-manager interfaces.

Virtual Interface

The virtual interface is used to support mobility management, Dynamic Host Configuration Protocol (DHCP) relay, and embedded Layer 3 security such as guest web authentication. 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, the 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.

  Note See Chapter 5 for additional information on web authentication.

The 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, the 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. Therefore, the virtual interface must be configured with an unassigned and unused gateway IP address, such as 1.1.1.1. The virtual interface IP address is not pingable and should not exist in any routing table in your network. In addition, the virtual interface cannot be mapped to a backup port.

Note 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 hand-off does not complete, and the client loses connectivity for a period of time.

Service-Port Interface

The service-port interface controls communications through and is statically mapped by the system to the service port. It must have an IP address on a different supernet from the management, AP-manager, and any dynamic interfaces, and it cannot be mapped to a backup port. This configuration enables you to manage the controller directly or through a dedicated operating system network, such as 10.1.2.x, which can ensure service access during network downtime.

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.

Note Only Cisco 4400 series controllers have a service-port interface.

Note 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.

Dynamic Interface

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 VLAN 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.

Note Configuring a dynamic interface with a secondary subnet is not supported.

Note Cisco recommends using tagged VLANs for dynamic interfaces.

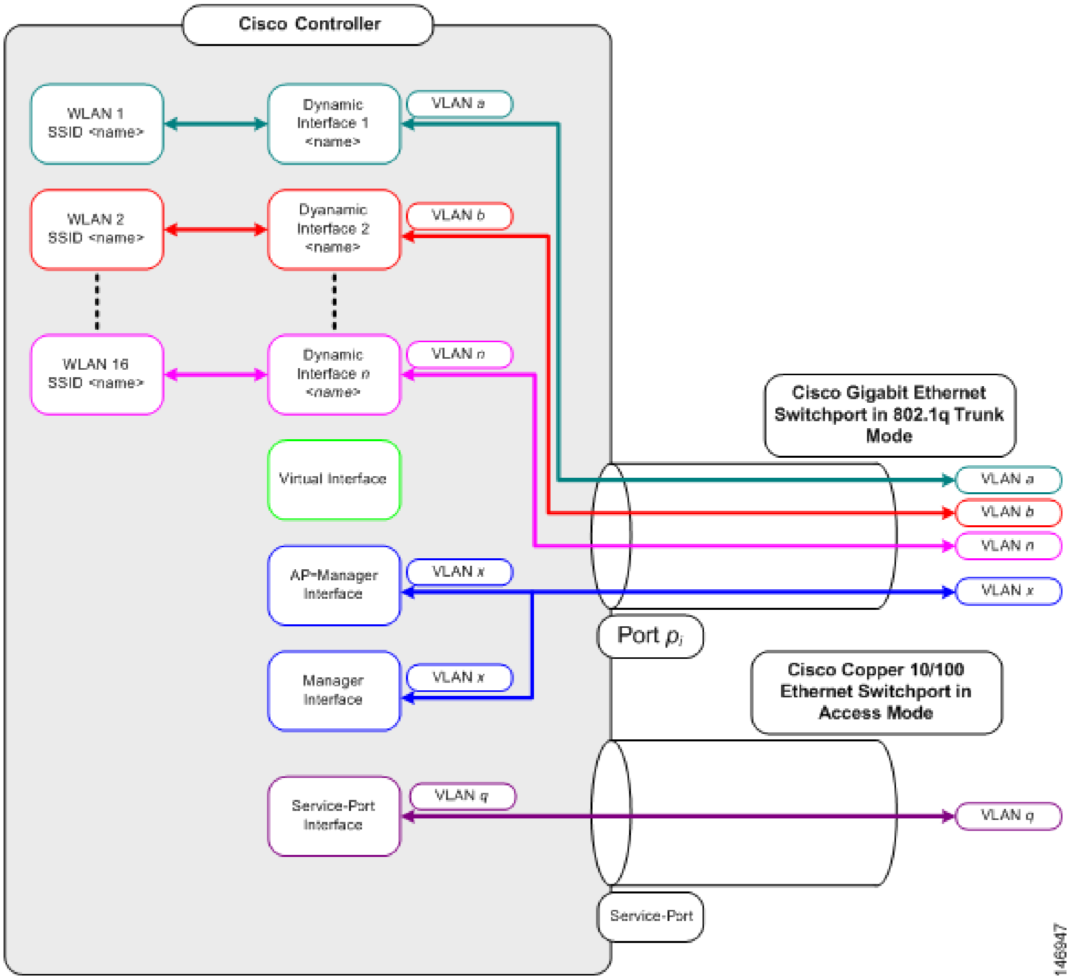
WLANs

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 16 access point WLANs can be configured per controller.

Note Chapter 6 provides instructions for configuring WLANs.

Figure 3-4 illustrates the relationship between ports, interfaces, and WLANs.

Figure 3-4 Ports, Interfaces, and WLANs



As shown in Figure 3-4, 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. Therefore, 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 non-zero value), the VLAN must be allowed on the 802.1Q trunk configuration on the neighbor switch and not be the native untagged VLAN.

Cisco recommends 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 Cisco recommends 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.

Follow the instructions on the pages indicated to configure your controller's interfaces and ports:

- Configuring the Management, AP-Manager, Virtual, and Service-Port Interfaces, page 3-10
- Configuring Dynamic Interfaces, page 3-16
- Configuring Ports, page 3-19
- Enabling Link Aggregation, page 3-29
- Configuring a 4400 Series Controller to Support More Than 48 Access Points, page 3-34

Configuring the Management, AP-Manager, Virtual, and Service-Port Interfaces

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.

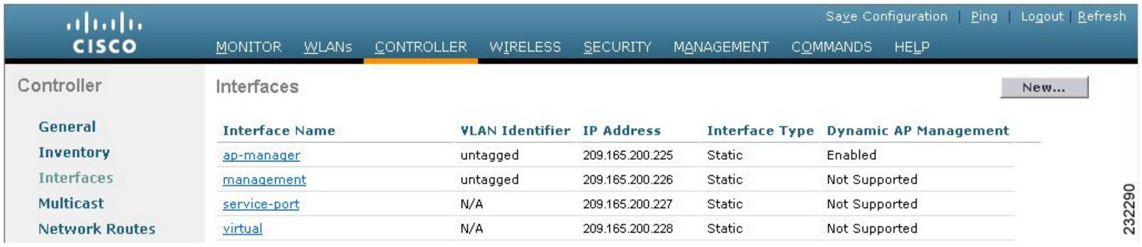
Note When assigning a WLAN to a DHCP server, both should be on the same subnet. Otherwise, you need to use a router to route traffic between the WLAN and the DHCP server.

Using the GUI to Configure the Management, AP-Manager, Virtual, and Service-Port Interfaces

Follow these steps to display and configure the management, AP-manager, virtual, and service-port interface parameters using the GUI.

Step 1 Click **Controller** > **Interfaces** to open the Interfaces page (see Figure 3-5).

Figure 3-5 Interfaces Page



Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	209.165.200.225	Static	Enabled
management	untagged	209.165.200.226	Static	Not Supported
service-port	N/A	209.165.200.227	Static	Not Supported
virtual	N/A	209.165.200.228	Static	Not Supported

This page shows the current controller interface settings.

Step 2 If you want to modify the settings of a particular interface, click the name of the interface. The Interfaces > Edit page for that interface appears.

Step 3 Configure the following parameters for each interface type:

Management Interface

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

- Quarantine and quarantine VLAN ID, if applicable

  Note Check 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 6 for more information about NAC out-of-band integration.

- VLAN identifier

  Note Enter **0** for an untagged VLAN or a non-zero value for a tagged VLAN. Cisco recommends using tagged VLANs for the management interface.

- Fixed IP address, IP netmask, and default gateway
- Physical port assignment
- Primary and secondary DHCP servers
- Access control list (ACL) setting, if required

  Note To create ACLs, follow the instructions in Chapter 5.

AP-Manager Interface

- VLAN identifier

Note Enter **0** for an untagged VLAN or a non-zero value for a tagged VLAN. Cisco recommends 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, Cisco recommends that both interfaces be on the same subnet for optimum access point association.

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

Note To create ACLs, follow the instructions in Chapter 5.

Virtual Interface

- Any fictitious, unassigned, and unused gateway IP address, such as 1.1.1.1
- DNS gateway host name

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 server(s) used by the client.

Service-Port Interface

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

- DHCP protocol (enabled) or
- 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 virtual interface, reboot the controller so your changes take effect.

Using the CLI to Configure the Management, AP-Manager, Virtual, and Service-Port Interfaces

This section provides instructions for displaying and configuring the management, AP-manager, virtual, and service-port interfaces using the CLI.

Using the CLI to Configure the Management Interface

Follow these steps to display and configure the management interface parameters using the CLI.

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

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

Step 2 Enter **config wlan disable** *wlan-number* 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 this command to configure a quarantine VLAN on the management interface.

- **config interface vlan management** {*vlan-id* | **0**}

  > **Note** Enter **0** for an untagged VLAN or a non-zero value for a tagged VLAN. Cisco recommends using tagged VLANs for the management interface.

- **config interface port management** *physical-ds-port-number*
- **config interface dhcp management** *ip-address-of-primary-dhcp-server* [*ip-address-of-secondary-dhcp-server*]
- **config interface acl management** *access-control-list-name*

  > **Note** See Chapter 5 for more information on ACLs.

Step 4 Enter **save config** to save your changes.

Step 5 Enter **show interface detailed management** to verify that your changes have been saved.

Using the CLI to Configure the AP-Manager Interface

Follow these steps to display and configure the AP-manager interface parameters using the CLI.

Step 1 Enter **show interface summary** 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 **show interface detailed ap-manager** to view the current AP-manager interface settings.

Step 3 Enter **config wlan disable** *wlan-number* 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 non-zero value for a tagged VLAN. Cisco recommends using tagged VLANs for the AP-manager interface.

- **config interface port ap-manager** *physical-ds-port-number*
- **config interface dhcp ap-manager** *ip-address-of-primary-dhcp-server* [*ip-address-of-secondary-dhcp-server*]
- **config interface acl ap-manager** *access-control-list-name*

  Note See Chapter 5 for more information on ACLs.

Step 5 Enter **save config** to save your changes.

Step 6 Enter **show interface detailed ap-manager** to verify that your changes have been saved.

Using the CLI to Configure the Virtual Interface

Follow these steps to display and configure the virtual interface parameters using the CLI.

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

Step 2 Enter **config wlan disable** *wlan-number* 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, such as 1.1.1.1.

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

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

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

Using the CLI to Configure the Service-Port Interface

Follow these steps to display and configure the service-port interface parameters using the CLI.

Step 1 Enter **show interface detailed service-port** 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*

Step 3 The service port is used for out-of-band management of the controller. If the management workstation is in a remote subnet, you may need to add a route on the controller in order to manage the controller from that remote workstation. To do so, enter this command:

config route add *network-ip-addr ip-netmask gateway*

Step 4 Enter **save config** to save your changes.

Step 5 Enter **show interface detailed service-port** to verify that your changes have been saved.

Configuring Dynamic Interfaces

This section provides instructions for configuring dynamic interfaces using either the GUI or CLI.

Using the GUI to Configure Dynamic Interfaces

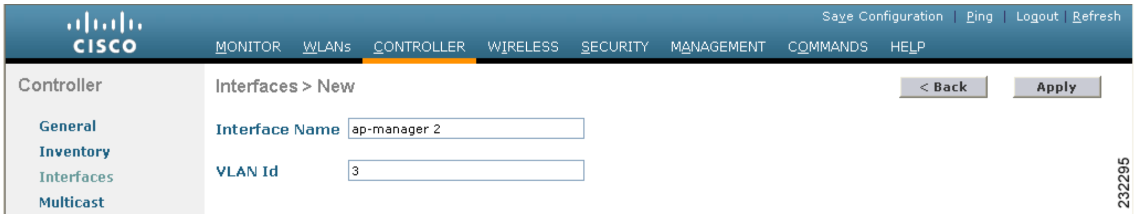
Follow these steps to create new or edit existing dynamic interfaces using the GUI.

Step 1 Click **Controller** > **Interfaces** to open the Interfaces page (see Figure 3-5).

Step 2 Perform one of the following:

- To create a new dynamic interface, click **New**. The Interfaces > New page appears (see Figure 3-6). 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 (see Figure 3-7). 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**.

Figure 3-6 Interfaces > New Page



Interfaces > New

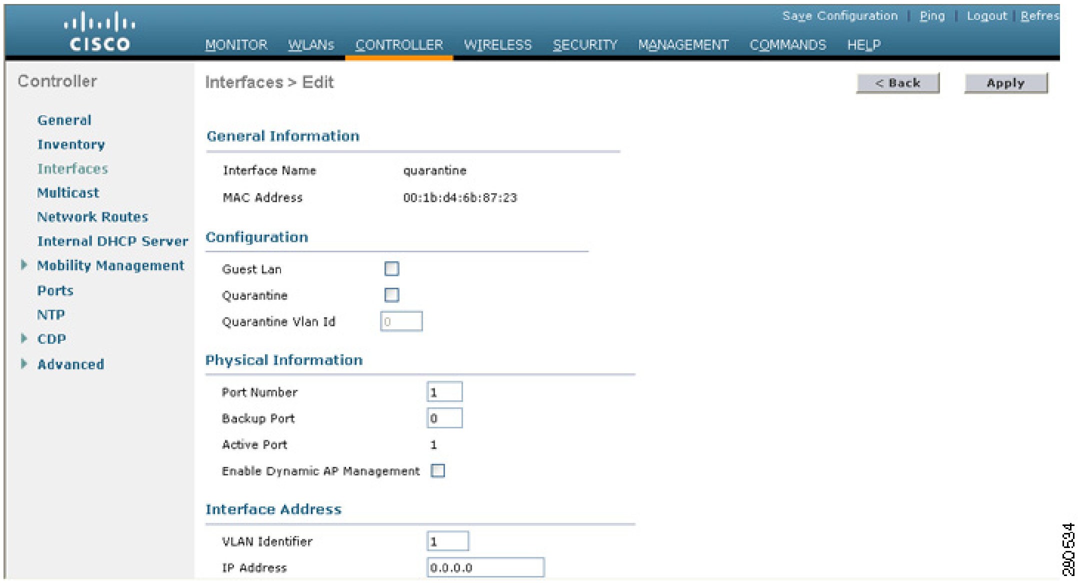
Interface Name: ap-manager 2

VLAN Id: 3

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

Step 4 Click **Apply** to commit your changes. The Interfaces > Edit page appears (see Figure 3-7).

Figure 3-7 Interfaces > Edit Page



Interfaces > Edit

General Information

Interface Name	quarantine
MAC Address	00:1b:d4:6b:87:23

Configuration

Guest Lan	□
Quarantine	□
Quarantine Vlan Id	0

Physical Information

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	□

Interface Address

VLAN Identifier	1
IP Address	0.0.0.0

Step 5 Configure the following parameters:

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

Note Check 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 6 for more information about NAC out-of-band integration.

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

Note See Chapter 5 for more information on ACLs.

Note 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.

Using the CLI to Configure Dynamic Interfaces

Follow these steps to configure dynamic interfaces using the CLI.

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

Step 2 To view the details of a specific dynamic interface, enter **show interface detailed** *operator_defined_interface_name*.

Step 3 Enter **config wlan disable** *wlan_id* 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 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 5 for more information on ACLs.

Step 5 Enter **config wlan enable** *wlan_id* to re-enable each WLAN that uses the dynamic interface for distribution system communication.

Step 6 Enter **save config** to save your changes.

Step 7 Enter **show interface detailed** *operator_defined_interface_name* and **show interface summary** to verify that your changes have been saved.

Note If desired, you can enter **config interface delete** *operator_defined_interface_name* to delete a dynamic interface.

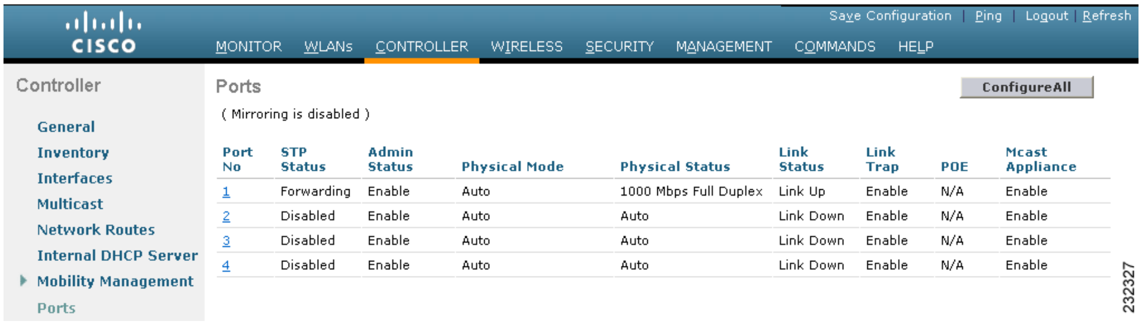
Configuring Ports

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

Follow these steps to use the GUI to view the status of the controller's ports and make any configuration changes if necessary.

Step 1 Click **Controller** > **Ports** to open the Ports page (see Figure 3-8).

Figure 3-8 Ports Page



Ports

(Mirroring is disabled)

Port No	STP Status	Admin Status	Physical Mode	Physical Status	Link Status	Link Trap	POE	Mcast Appliance
1	Forwarding	Enable	Auto	1000 Mbps Full Duplex	Link Up	Enable	N/A	Enable
2	Disabled	Enable	Auto	Auto	Link Down	Enable	N/A	Enable
3	Disabled	Enable	Auto	Auto	Link Down	Enable	N/A	Enable
4	Disabled	Enable	Auto	Auto	Link Down	Enable	N/A	Enable

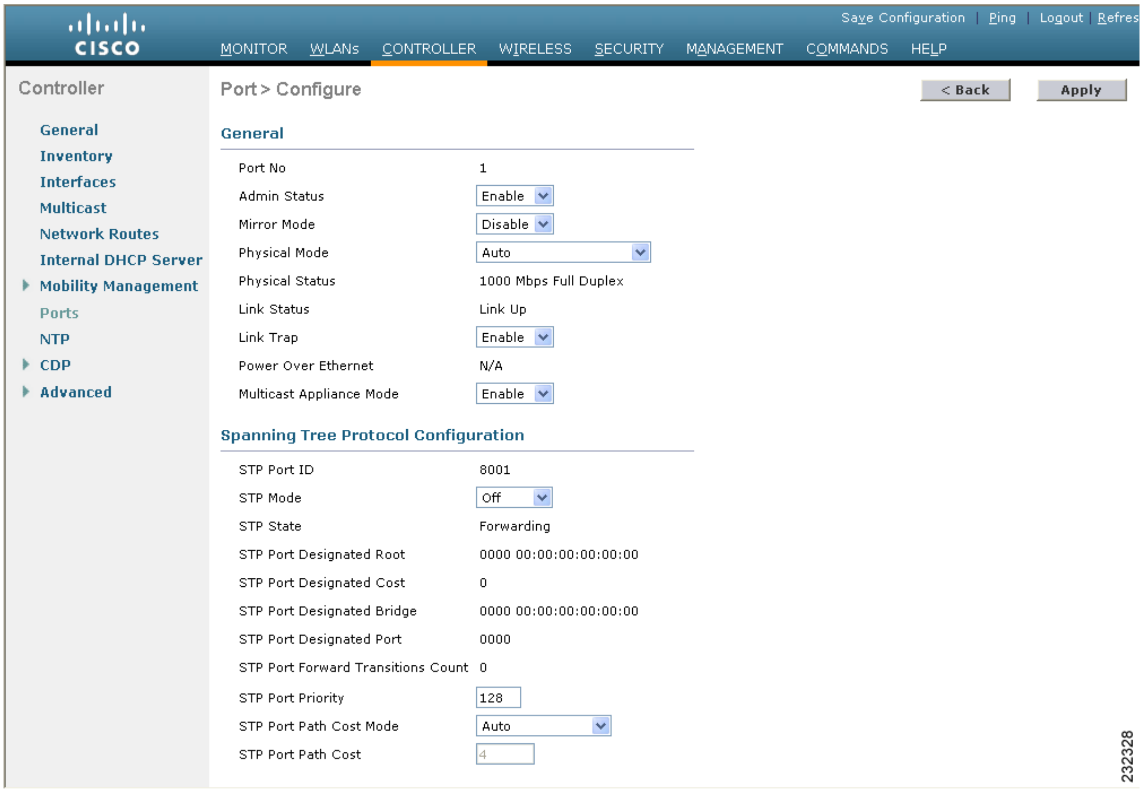
This page shows the current configuration for each of the controller's ports.

Step 2 If you want to change the settings of any port, click the number for that specific port. The Port > Configure page appears (see Figure 3-9).

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. For instance, 2100 series controllers and the controller in a Cisco Integrated Services Router have fewer configurable parameters than a 4400 series controller, which is shown in Figure 3-9.

Figure 3-9 Port > Configure Page



Port > Configure

General

Port No	1
Admin Status	Enable
Mirror Mode	Disable
Physical Mode	Auto
Physical Status	1000 Mbps Full Duplex
Link Status	Link Up
Link Trap	Enable
Power Over Ethernet	N/A
Multicast Appliance Mode	Enable

Spanning Tree Protocol Configuration

STP Port ID	8001
STP Mode	Off
STP State	Forwarding
STP Port Designated Root	0000 00:00:00:00:00:00
STP Port Designated Cost	0
STP Port Designated Bridge	0000 00:00:00:00:00:00
STP Port Designated Port	0000
STP Port Forward Transitions Count	0
STP Port Priority	128
STP Port Path Cost Mode	Auto
STP Port Path Cost	4

Table 3-2 interprets the current status of the port.

Table 3-2 Port Status

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>Port Number</td><td colspan="2">The number of the current port.</td></tr>
<tr><td rowspan="7">Physical Status</td><td colspan="2">The data rate being used by the port. The available data rates vary based on controller type.</td></tr>
<tr><td><b>Controller</b></td><td><b>Available Data Rates</b></td></tr>
<tr><td>4400 series</td><td>1000 Mbps full duplex</td></tr>
<tr><td>2100 series</td><td>10 or 100 Mbps, half or full duplex</td></tr>
<tr><td>WiSM</td><td>1000 Mbps full duplex</td></tr>
<tr><td>Controller network module</td><td>100 Mbps full duplex</td></tr>
<tr><td>Catalyst 3750G Integrated Wireless LAN Controller Switch</td><td>1000 Mbps full duplex</td></tr>
<tr><td>Link Status</td><td colspan="2">The port’s link status.
<b>Values:</b> Link Up or Link Down</td></tr>
</table>

Table 3-2 Port Status (continued)

Parameter	Description
Power over Ethernet (PoE)	Determines 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 3 Table 3-3 lists and describes the port's configurable parameters. Follow the instructions in the table to make any desired changes.

Table 3-3 Port Parameters

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>Admin Status</td><td colspan="2">Enables or disables the flow of traffic through the port.
<b>Options:</b> Enable or Disable
<b>Default:</b> Enable
<b>Note</b> 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.</td></tr>
<tr><td rowspan="8">Physical Mode</td><td colspan="2">Determines whether the port's data rate is set automatically or specified by the user. The supported data rates vary based on controller type.
<b>Default:</b> Auto</td></tr>
<tr><td><b>Controller</b></td><td><b>Supported Data Rates</b></td></tr>
<tr><td>4400 series</td><td>Auto or 1000 Mbps full duplex</td></tr>
<tr><td>2100 series</td><td>Auto or 10 or 100 Mbps, half or full duplex</td></tr>
<tr><td>WiSM</td><td>Auto or 1000 Mbps full duplex</td></tr>
<tr><td>Controller network module</td><td>Auto or 100 Mbps full duplex</td></tr>
<tr><td>Catalyst 3750G Integrated Wireless LAN Controller Switch</td><td>Auto or 1000 Mbps full duplex</td></tr>
<tr><td colspan="2"><b>Note</b> Make sure that a duplex mismatch does not exist between a 2100 series controller and the Catalyst switch. A duplex mismatch is a situation where the switch operates at full duplex and the connected device operates at half duplex or vice versa. The results of a duplex mismatch are extremely slow performance, intermittent connectivity, and loss of connection. Other possible causes of data link errors at full duplex are bad cables, faulty switch ports, or client software or hardware issues.</td></tr>
</table>

Table 3-3 Port Parameters (continued)

Parameter	Description
Link Trap	Causes the port to send a trap when the port's link status changes. **Options:** Enable or Disable **Default:** Enable
Multicast Appliance Mode	Enables or disables the multicast appliance service for this port. **Options:** Enable or Disable **Default:** Enable

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 Ports page and review your changes.

Step 7 Repeat this procedure for each additional port that you want to configure.

Step 8 Go to the following sections if you want to configure the controller's ports for these advanced features:

- Port mirroring, see below
- Spanning Tree Protocol (STP), page 3-23

Configuring Port Mirroring

Mirror mode enables you to duplicate to another port all of the traffic originating from or terminating at a single client device or access point. It is useful in diagnosing specific network problems. Mirror mode should be enabled only on an unused port as any connections to this port become unresponsive.

Note The 2100 series controllers, controller network modules, and Cisco WiSM controllers do not support mirror mode. Also, a controller's service port cannot be used as a mirrored port.

Note Port mirroring is not supported when link aggregation (LAG) is enabled on the controller.

Note Cisco recommends that you do not mirror traffic from one controller port to another as this setup could cause network problems.

Follow these steps to enable port mirroring.

Step 1 Click **Controller** > **Ports** to open the Ports page (see Figure 3-8).

Step 2 Click the number of the unused port for which you want to enable mirror mode. The Port > Configure page appears (see Figure 3-9).

Step 3 Set the Mirror Mode parameter to **Enable**.

Step 4 Click **Apply** to commit your changes.

Step 5 Perform one of the following:

- Follow these steps if you want to choose a specific client device that will mirror its traffic to the port you selected on the controller:

  a. Click **Wireless** > **Clients** to open the Clients page.

  b. Click the MAC address of the client for which you want to enable mirror mode. The Clients > Detail page appears.

  c. Under Client Details, set the Mirror Mode parameter to **Enable**.

- Follow these steps if you want to choose an access point that will mirror its traffic to the port you selected on the controller:

  a. Click **Wireless** > **Access Points** > **All APs** to open the All APs page.

  b. Click the name of the access point for which you want to enable mirror mode. The All APs > Details page appears.

  c. Click the **Advanced** tab.

  d. Set the Mirror Mode parameter to **Enable**.

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

Configuring Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two network devices. STP allows only one active path at a time between network devices but establishes redundant links as a backup if the initial link should fail.

The spanning-tree algorithm calculates the best loop-free path throughout a Layer 2 network. Infrastructure devices such as controllers and switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The devices do not forward these frames but use them to construct a loop-free path.

Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Infrastructure devices might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network.

STP defines a tree with a root bridge and a loop-free path from the root to all infrastructure devices in the Layer 2 network.

Note STP discussions use the term *root* to describe two concepts: the controller on the network that serves as a central point in the spanning tree is called the *root bridge*, and the port on each controller that provides the most efficient path to the root bridge is called the *root port*. The root bridge in the spanning tree is called the *spanning-tree root*.

STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path.

When two ports on a controller are part of a loop, the spanning-tree port priority and path cost settings determine which port is put in the forwarding state and which is put in the blocking state. The port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents media speed.

The controller maintains a separate spanning-tree instance for each active VLAN configured on it. A bridge ID, consisting of the bridge priority and the controller's MAC address, is associated with each instance. For each VLAN, the controller with the lowest controller ID becomes the spanning-tree root for that VLAN.

STP is disabled for the controller's distribution system ports by default. The following sections provide instructions for configuring STP for your controller using either the GUI or CLI.

Note STP cannot be configured for the controller in the Catalyst 3750G Integrated Wireless LAN Controller Switch.

Using the GUI to Configure Spanning Tree Protocol

Follow these steps to configure STP using the GUI.

Step 1 Click **Controller** > **Ports** to open the Ports page (see Figure 3-8).

Step 2 Click the number of the port for which you want to configure STP. The Port > Configure page appears (see Figure 3-9). This page shows the STP status of the port and enables you to configure STP parameters.

Table 3-4 interprets the current STP status of the port.

Table 3-4 Port Spanning Tree Status

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>STP Port ID</td><td colspan="2">The number of the port for which STP is enabled or disabled.</td></tr>
<tr><td rowspan="8">STP State</td><td colspan="2">The port's current STP state. It controls the action that a port takes upon receiving a frame.
<b>Values:</b> Disabled, Blocking, Listening, Learning, Forwarding, and Broken</td></tr>
<tr><td><b>STP State</b></td><td><b>Description</b></td></tr>
<tr><td>Disabled</td><td>The port is not participating in spanning tree because the port is shut down, the link is down, or STP is not enabled for this port.</td></tr>
<tr><td>Blocking</td><td>The port does not participate in frame forwarding.</td></tr>
<tr><td>Listening</td><td>The first transitional state after the blocking state when STP determines that the port should participate in frame forwarding.</td></tr>
<tr><td>Learning</td><td>The port prepares to participate in frame forwarding.</td></tr>
<tr><td>Forwarding</td><td>The port forwards frames.</td></tr>
<tr><td>Broken</td><td>The port is malfunctioning.</td></tr>
<tr><td>STP Port Designated Root</td><td colspan="2">The unique identifier of the root bridge in the configuration BPDUs.</td></tr>
</table>

Table 3-4 Port Spanning Tree Status (continued)

Parameter	Description
STP Port Designated Cost	The path cost of the designated port.
STP Port Designated Bridge	The identifier of the bridge that the port considers to be the designated bridge for this port.
STP Port Designated Port	The port identifier on the designated bridge for this port.
STP Port Forward Transitions Count	The number of times that the port has transitioned from the learning state to the forwarding state.

Step 3 Table 3-5 lists and describes the port's configurable STP parameters. Follow the instructions in the table to make any desired changes.

Table 3-5 Port Spanning Tree Parameters

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td rowspan="5">STP Mode</td><td colspan="2">The STP administrative mode associated with this port.
<b>Options:</b> Off, 802.1D, or Fast
<b>Default:</b> Off</td></tr>
<tr><th>STP Mode</th><th>Description</th></tr>
<tr><td>Off</td><td>Disables STP for this port.</td></tr>
<tr><td>802.1D</td><td>Enables this port to participate in the spanning tree and go through all of the spanning tree states when the link state transitions from down to up.</td></tr>
<tr><td>Fast</td><td>Enables this port to participate in the spanning tree and puts it in the forwarding state when the link state transitions from down to up more quickly than when the STP mode is set to 802.1D.
<b>Note</b> In this state, the forwarding delay timer is ignored on link up.</td></tr>
<tr><td>STP Port Priority</td><td colspan="2">The location of the port in the network topology and how well the port is located to pass traffic.
<b>Range:</b> 0 to 255
<b>Default:</b> 128</td></tr>
<tr><td>STP Port Path Cost Mode</td><td colspan="2">Determines whether the STP port path cost is set automatically or specified by the user. If you choose User Configured, you also need to set a value for the STP Port Path Cost parameter.
<b>Range:</b> Auto or User Configured
<b>Default:</b> Auto</td></tr>
</table>

Table 3-5 Port Spanning Tree Parameters (continued)

Parameter	Description
STP Port Path Cost	The speed at which traffic is passed through the port. This parameter must be set if the STP Port Path Cost Mode parameter is set to User Configured. **Options:** 0 to 65535 **Default:** 0, which causes the cost to be adjusted for the speed of the port when the link comes up. **Note** Typically, a value of 100 is used for 10-Mbps ports and 19 for 100-Mbps ports.

Step 4 Click **Apply** to commit your changes.

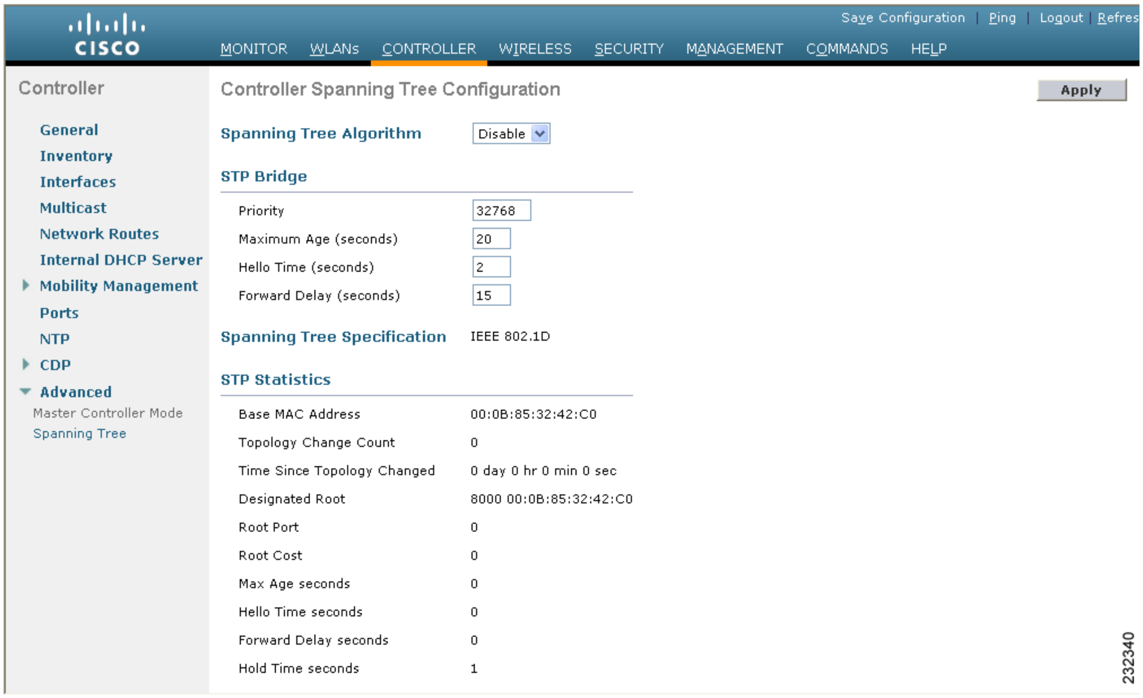
Step 5 Click **Save Configuration** to save your changes.

Step 6 Click **Back** to return to the Ports page.

Step 7 Repeat Step 2 through Step 6 for each port for which you want to enable STP.

Step 8 Click **Controller** > **Advanced** > **Spanning Tree** to open the Controller Spanning Tree Configuration page (see Figure 3-10).

Figure 3-10 Controller Spanning Tree Configuration Page



Controller Spanning Tree Configuration

Spanning Tree Algorithm: Disable

STP Bridge

Priority	32768
Maximum Age (seconds)	20
Hello Time (seconds)	2
Forward Delay (seconds)	15

Spanning Tree Specification: IEEE 802.1D

STP Statistics

Base MAC Address	00:0B:85:32:42:C0
Topology Change Count	0
Time Since Topology Changed	0 day 0 hr 0 min 0 sec
Designated Root	8000 00:0B:85:32:42:C0
Root Port	0
Root Cost	0
Max Age seconds	0
Hello Time seconds	0
Forward Delay seconds	0
Hold Time seconds	1

This page allows you to enable or disable the spanning tree algorithm for the controller, modify its characteristics, and view the STP status.Table 3-6 interprets the current STP status for the controller.

Table 3-6 Controller Spanning Tree Status

Parameter	Description
Spanning Tree Specification	The STP version being used by the controller. Currently, only an IEEE 802.1D implementation is available.
Base MAC Address	The MAC address used by this bridge when it must be referred to in a unique fashion. When it is concatenated with dot1dStpPriority, a unique bridge identifier is formed that is used in STP.
Topology Change Count	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
Time Since Topology Changed	The time (in days, hours, minutes, and seconds) since a topology change was detected by the bridge.
Designated Root	The bridge identifier of the spanning tree root. This value is used as the Root Identifier parameter in all configuration BPDUs originated by this node.
Root Port	The number of the port that offers the lowest cost path from this bridge to the root bridge.
Root Cost	The cost of the path to the root as seen from this bridge.
Max Age (seconds)	The maximum age of STP information learned from the network on any port before it is discarded.
Hello Time (seconds)	The amount of time between the transmission of configuration BPDUs by this node on any port when it is the root of the spanning tree or trying to become so. This is the actual value that this bridge is currently using.
Forward Delay (seconds)	This value controls how fast a port changes its spanning tree state when moving toward the forwarding state. It determines how long the port stays in each of the listening and learning states that precede the forwarding state. This value is also used, when a topology change has been detected and is underway, to age all dynamic entries in the forwarding database. **Note** This is the actual value that this bridge is currently using, in contrast to *Stp Bridge Forward Delay*, which is the value that this bridge and all others would start using if this bridge were to become the root.
Hold Time (seconds)	The minimum time period to elapse between the transmission of configuration BPDUs through a given LAN port. **Note** At most, one configuration BPDU can be transmitted in any hold time period.

Step 9 Table 3-7 lists and describes the controller's configurable STP parameters. Follow the instructions in the table to make any desired changes.

Table 3-7 Controller Spanning Tree Parameters

Parameter	Description
Spanning Tree Algorithm	Enables or disables STP for the controller. **Options:** Enable or Disable **Default:** Disable
Priority	The location of the controller in the network topology and how well the controller is located to pass traffic. **Range:** 0 to 65535 **Default:** 32768
Maximum Age (seconds)	The length of time that the controller stores protocol information received on a port. **Range:** 6 to 40 seconds **Default:** 20 seconds
Hello Time (seconds)	The length of time that the controller broadcasts hello messages to other controllers. **Options:** 1 to 10 seconds **Default:** 2 seconds
Forward Delay (seconds)	The length of time that each of the listening and learning states lasts before the port begins forwarding. **Options:** 4 to 30 seconds **Default:** 15 seconds

Step 10 Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Using the CLI to Configure Spanning Tree Protocol

Follow these steps to configure STP using the CLI.

Step 1 Enter **show spanningtree port** and **show spanningtree switch** to view the current STP status.

Step 2 If STP is enabled, you must disable it before you can change STP settings. Enter **config spanningtree switch mode disable** to disable STP on all ports.

Step 3 Enter one of these commands to configure the STP port administrative mode:

- **config spanningtree port mode 802.1d** {*port-number* | **all**}
- **config spanningtree port mode fast** {*port-number* | **all**}
- **config spanningtree port mode off** {*port-number* | **all**}

Step 4 Enter one of these commands to configure the STP port path cost on the STP ports:

- **config spanningtree port pathcost** *1-65535* {*port-number* | **all**}—Specifies a path cost from 1 to 65535 to the port.
- **config spanningtree port mode pathcost auto** {*port-number* | **all**}—Enables the STP algorithm to automatically assign the path cost. This is the default setting.

Step 5 Enter **config spanningtree port priority** *0-255 port-number* to configure the port priority on STP ports. The default priority is 128.

Step 6 If necessary, enter **config spanningtree switch bridgepriority** *0-65535* to configure the controller's STP bridge priority. The default bridge priority is 32768.

Step 7 If necessary, enter **config spanningtree switch forwarddelay** *4-30* to configure the controller's STP forward delay in seconds. The default forward delay is 15 seconds.

Step 8 If necessary, enter **config spanningtree switch hellotime** *1-10* to configure the controller's STP hello time in seconds. The default hello time is 2 seconds.

Step 9 If necessary, enter **config spanningtree switch maxage** *6-40* to configure the controller's STP maximum age. The default maximum age is 20 seconds.

Step 10 After you configure STP settings for the ports, enter **config spanningtree switch mode enable** to enable STP for the controller. The controller automatically detects logical network loops, places redundant ports on standby, and builds a network with the most efficient pathways.

Step 11 Enter **save config** to save your settings.

Step 12 Enter **show spanningtree port** and **show spanningtree switch** to verify that your changes have been saved.

Enabling Link Aggregation

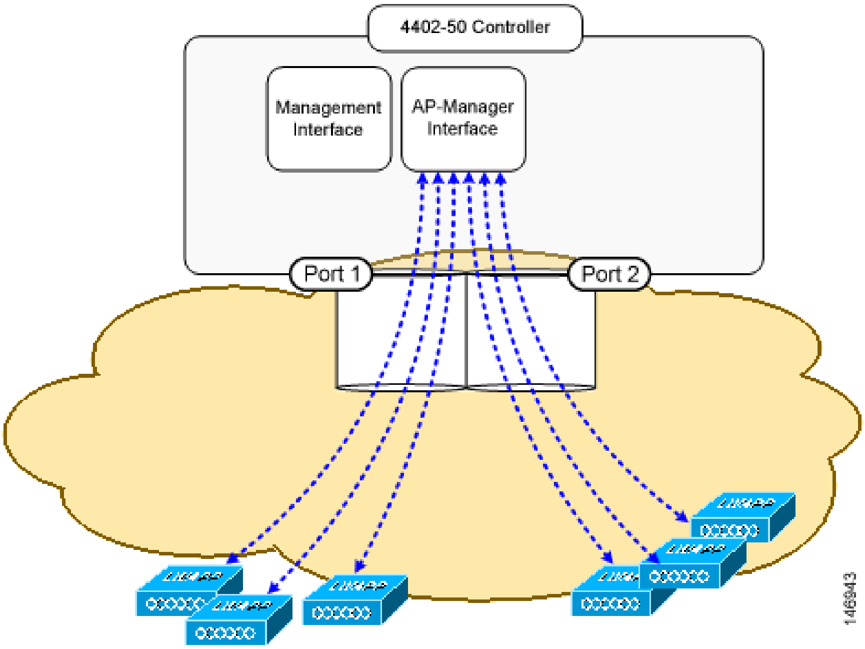
Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller's distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to configure the ports on your controller. When LAG is enabled,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

Cisco 4400 series controllers support LAG in software release 3.2 and higher, and LAG is enabled automatically on the controllers within the Cisco WiSM and the Catalyst 3750G Integrated Wireless LAN Controller Switch. Without LAG, each distribution system port on the controller supports up to 48 access points. With LAG enabled, a 4402 controller's logical port supports up to 50 access points, a 4404 controller's logical port supports up to 100 access points, and the logical port on each Cisco WiSM controller supports up to 150 access points.

Note You can bundle all four ports on a 4404 controller (or two on a 4402 controller) into a single link.

Figure 3-11 illustrates LAG.

Figure 3-11 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.

When configuring bundled ports on the controller, you may want to consider terminating on two different modules within a modular switch such as the Catalyst 6500; however, Cisco does not recommend connecting the LAG ports of a 4400 controller to multiple Catalyst 6500 or 3750G switches.

Terminating on two different modules within a single Catalyst 6500 switch provides redundancy and ensures that connectivity between the switch and the controller is maintained when one module fails. Figure 3-12 illustrates this use of redundant modules. A 4402-50 controller is connected to two different Gigabit modules (slots 2 and 3) within the Catalyst 6500. 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. Both switch ports are assigned to the same channel group.

When a 4404 controller or WiSM controller module 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-dest-ip (CLI command: **port-channel load-balance** *src_dest_ip*).

- 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 the 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* guide 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:

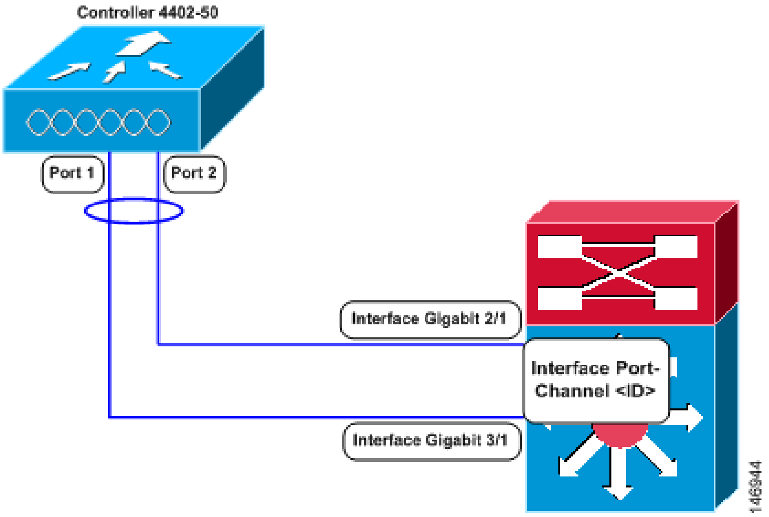
```
# show platform hardware pfc mode PFC operating mode
PFC operating mode : PFC3B
# show EtherChannel load-balance
EtherChannel Load-Balancing Configuration:
src-dst-ip
```

  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.

```
# 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.

Figure 3-12 Link Aggregation with Catalyst 6500 Neighbor Switch



Link Aggregation Guidelines

Keep these guidelines in mind when using LAG:

- 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. Therefore, you must configure LAG for all of the connected ports in the neighbor switch.
- When you enable LAG on the Cisco WiSM, you must enable port-channeling/Ether-channeling for all of the controller’s ports on the switch.
- When you enable LAG, port mirroring is not supported.
- 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 4400 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.

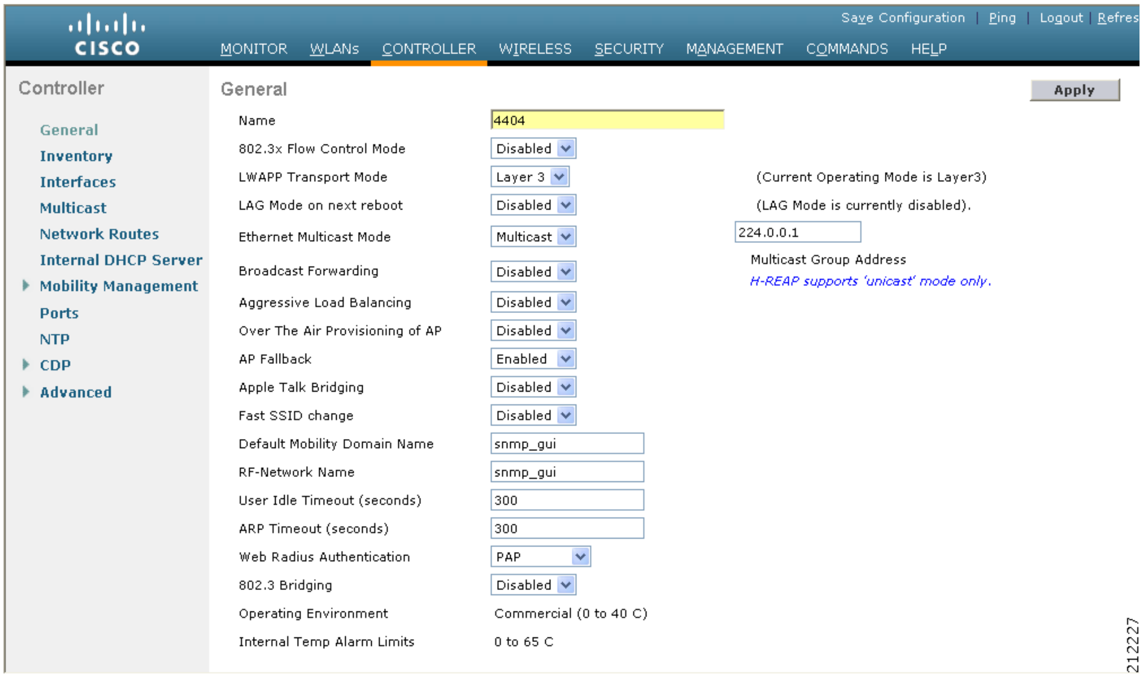
Note LAG is enabled by default and is the only option on the WiSM controller and the controller in the Catalyst 3750G Integrated Wireless LAN Controller Switch.

Using the GUI to Enable Link Aggregation

Follow these steps to enable LAG on your controller using the GUI.

Step 1 Click **Controller > General** to open the General page (see Figure 3-13).

Figure 3-13 General Page



General

Name	4404	
802.3x Flow Control Mode	Disabled	
LWAPP Transport Mode	Layer 3	(Current Operating Mode is Layer3)
LAG Mode on next reboot	Disabled	(LAG Mode is currently disabled).
Ethernet Multicast Mode	Multicast	224.0.0.1
Broadcast Forwarding	Disabled	Multicast Group Address H-REAP supports 'unicast' mode only.
Aggressive Load Balancing	Disabled	
Over The Air Provisioning of AP	Disabled	
AP Fallback	Enabled	
Apple Talk Bridging	Disabled	
Fast SSID change	Disabled	
Default Mobility Domain Name	snmp_gui	
RF-Network Name	snmp_gui	
User Idle Timeout (seconds)	300	
ARP Timeout (seconds)	300	
Web Radius Authentication	PAP	
802.3 Bridging	Disabled	
Operating Environment	Commercial (0 to 40 C)	
Internal Temp Alarm Limits	0 to 65 C	

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 4400 series controllers but enabled by default on the Cisco WiSM.

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.

Using the CLI to Enable Link Aggregation

Follow these steps to enable LAG on your controller using the CLI.

Step 1 Enter **config lag enable** to enable LAG.

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

Step 2 Enter **save config** to save your settings.

Step 3 Reboot the controller.

Using the CLI to Verify Link Aggregation Settings

To verify your LAG settings, enter this command:

show lag summary

Information similar to the following appears:

```
LAG Enabled
```

Configuring Neighbor Devices to Support LAG

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 a 4400 Series Controller to Support More Than 48 Access Points

As noted earlier, 4400 series controllers can support up to 48 access points per port. However, you can configure your 4400 series controller to support more access points using one of the following methods:

- Link aggregation, page 3-35
- Multiple AP-manager interfaces, page 3-35

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

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

- With link aggregation, 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 "Using Multiple AP-Manager Interfaces" section below) when port redundancy is a concern.

Using Link Aggregation

See the "Enabling Link Aggregation" section on page 3-29 for more information and instructions on enabling link aggregation.

Note Link aggregation is the only method that can be used for the Cisco WiSM and Catalyst 3750G Integrated Wireless LAN Controller Switch controllers.

Using Multiple AP-Manager Interfaces

Note This method can be used only with Cisco 4400 series stand-alone controllers.

When you create two or more AP-manager interfaces, each one is mapped to a different port (see Figure 3-14). The ports should be configured in sequential order such 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.

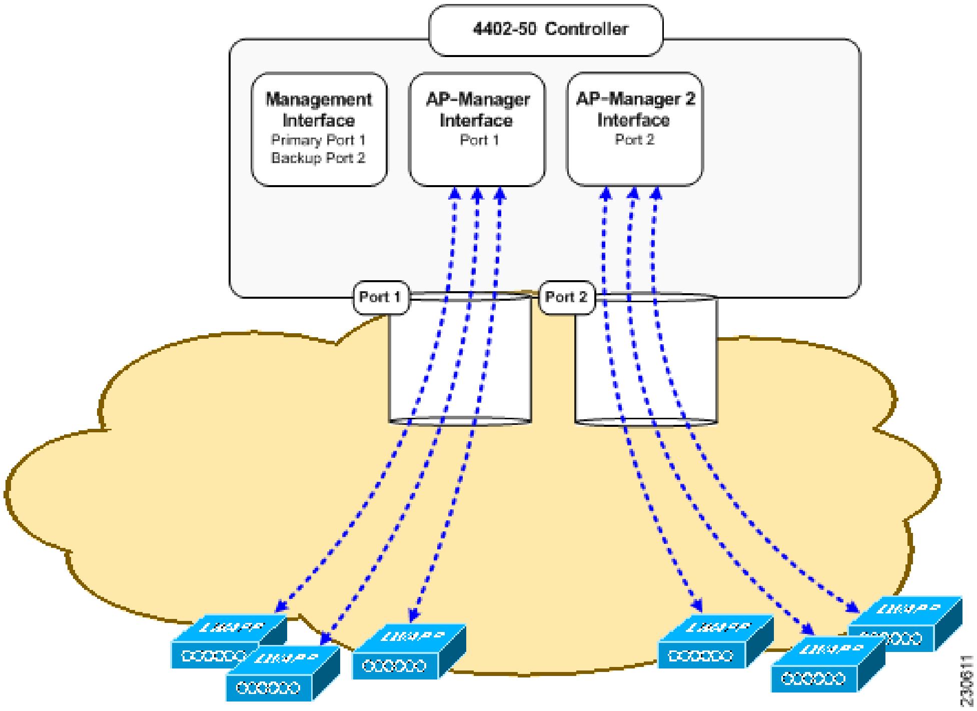
Note AP-manager interfaces need not be on the same VLAN or IP subnet, and they may or may not be on the same VLAN or IP subnet as the management interface. However, Cisco recommends that you configure all AP-manager interfaces on the same VLAN or IP subnet.

Note You must assign an AP-manager interface to each port on the controller.

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 3-14 Two AP-Manager Interfaces



Before implementing multiple AP-manager interfaces, you should consider how they would impact your controller's port redundancy.

Examples:

1. The 4402-50 controller supports a maximum of 50 access points and has two ports. To support the maximum number of access points, you would need to create two AP-manager interfaces (see Figure 3-14) because a controller can support only 48 access points on one port.
2. The 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 3-15). 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.

Figure 3-15 Three AP-Manager Interfaces

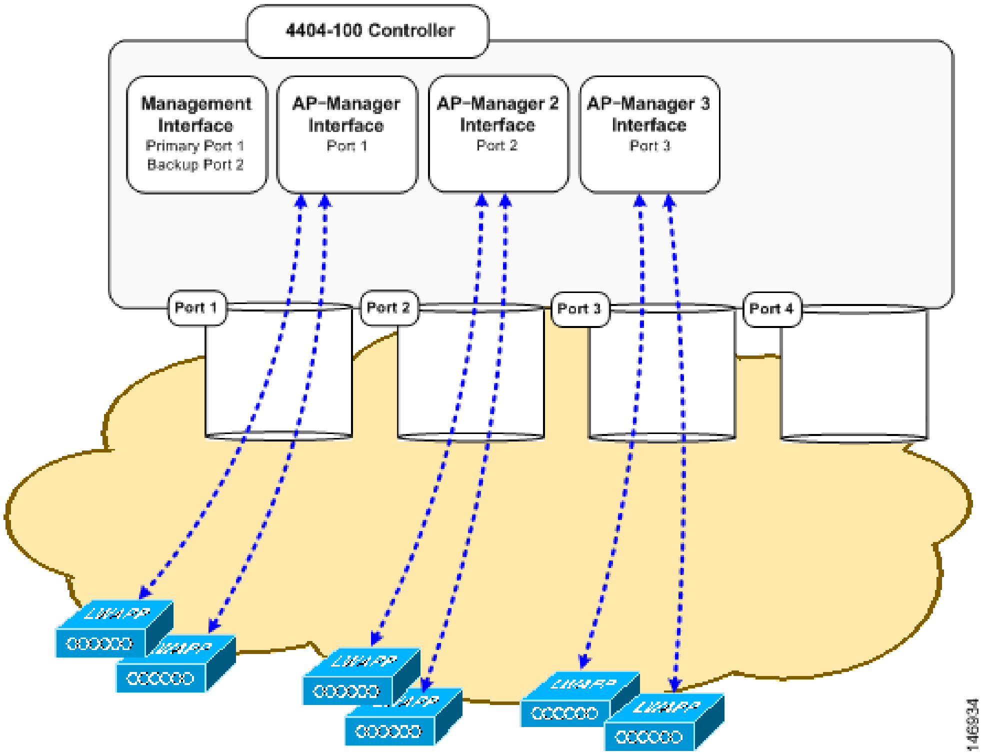
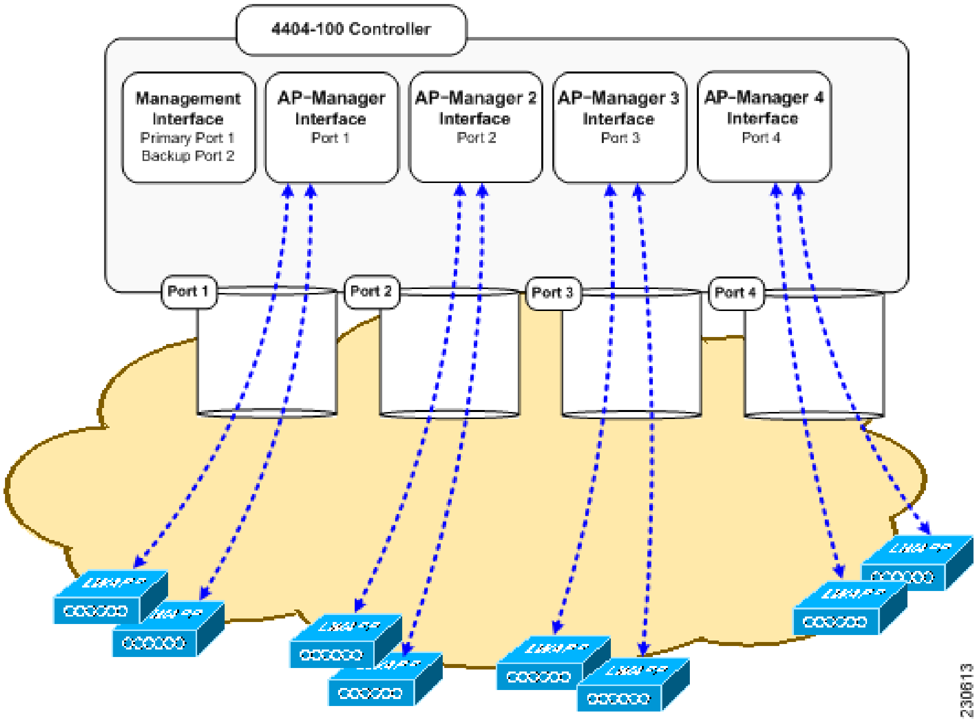


Figure 3-16 illustrates the use of four AP-manager interfaces to support 100 access points.

Figure 3-16 Four AP-Manager Interfaces



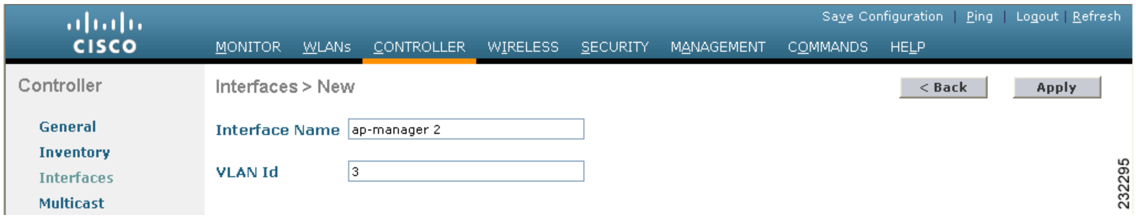
This configuration has the advantage of load-balancing all 100 access points evenly across all four AP-manager interfaces. If one of the AP-manager interfaces fails, all of the access points connected to the controller would be evenly distributed among the three available AP-manager interfaces. For example,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

Follow these steps to create multiple AP-manager interfaces.

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

Step 2 Click **New**. The Interfaces > New page appears (see Figure 3-18).

Figure 3-17 Interfaces > New Page


cisco
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Controller
General
Inventory
Interfaces
Multicast
< Back
Apply
232295

Interfaces > New

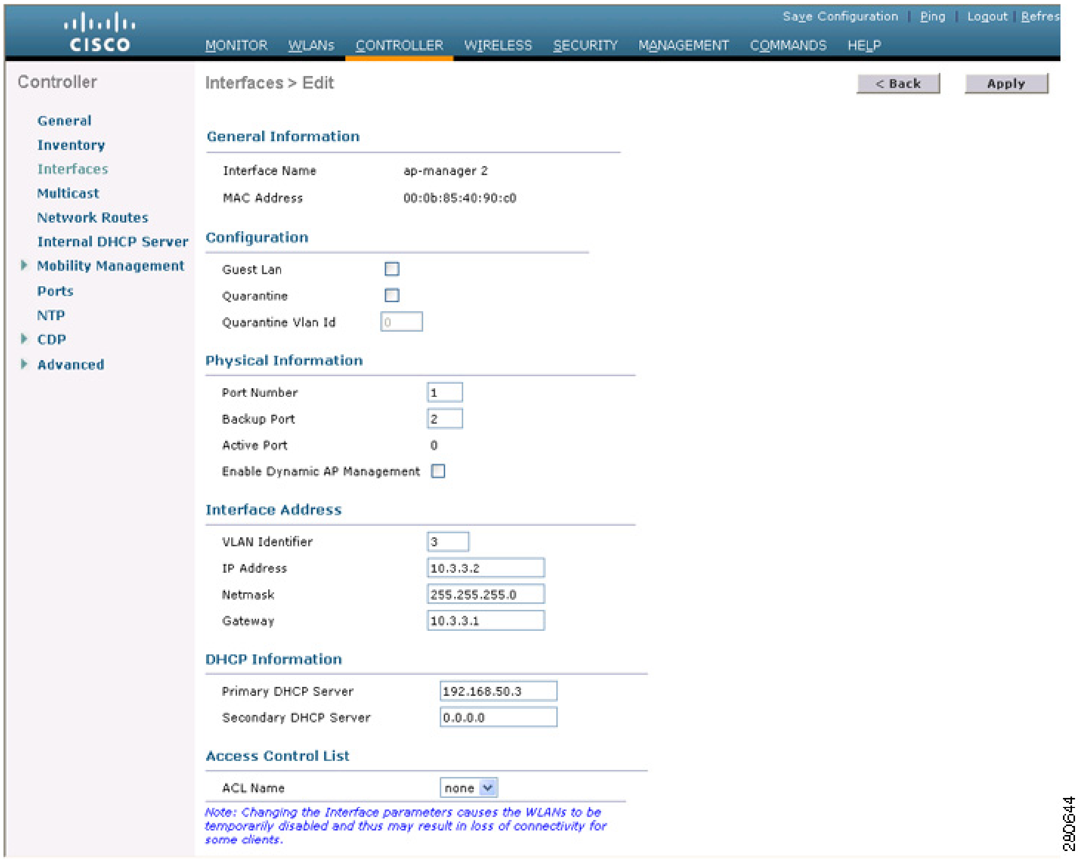
Interface Name: ap-manager 2

VLAN Id: 3

Step 3 Enter an AP-manager interface name and a VLAN identifier, as shown above.

Step 4 Click **Apply** to commit your changes. The Interfaces > Edit page appears (see Figure 3-18).

Figure 3-18 Interfaces > Edit Page



Interfaces > Edit

General Information

Interface Name	ap-manager 2
MAC Address	00:0b:85:40:90:c0

Configuration

Guest Lan	□
Quarantine	□
Quarantine Vlan Id	0

Physical Information

Port Number	1
Backup Port	2
Active Port	0
Enable Dynamic AP Management	□

Interface Address

VLAN Identifier	3
IP Address	10.3.3.2
Netmask	255.255.255.0
Gateway	10.3.3.1

DHCP Information

Primary DHCP Server	192.168.50.3
Secondary DHCP Server	0.0.0.0

Access Control List

ACL Name	none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

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 the interface an AP-manager interface, check the **Enable Dynamic AP Management** check box.

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.

CHAPTER 4

Configuring Controller SettingsWireless Device Access

This chapter describes how to configure settings on the controllers. It contains these sections:

- Using the Configuration Wizard, page 4-2
- Using the AutoInstall Feature for Controllers Without a Configuration, page 4-6
- Managing the System Date and Time, page 4-10
- Configuring 802.11 Bands, page 4-14
- Configuring 802.11n Parameters, page 4-17
- Configuring DHCP Proxy, page 4-22
- Configuring Administrator Usernames and Passwords, page 4-23
- Configuring SNMP, page 4-24
- Changing the Default Values of SNMP Community Strings, page 4-25
- Changing the Default Values for SNMP v3 Users, page 4-27
- Configuring Aggressive Load Balancing, page 4-29
- Configuring Fast SSID Changing, page 4-31
- Enabling 802.3X Flow Control, page 4-31
- Configuring 802.3 Bridging, page 4-32
- Configuring Multicast Mode, page 4-34
- Configuring Client Roaming, page 4-40
- Configuring IP-MAC Address Binding, page 4-44
- Configuring Quality of Service, page 4-45
- Configuring Voice and Video Parameters, page 4-52
- Configuring EDCA Parameters, page 4-67
- Configuring Cisco Discovery Protocol, page 4-69
- Configuring RFID Tag Tracking, page 4-79
- Configuring and Viewing Location Settings, page 4-84
- Configuring the Supervisor 720 to Support the WiSM, page 4-89
- Using the Wireless LAN Controller Network Module, page 4-91

Using the Configuration Wizard

This section describes how to configure basic settings on a controller for the first time or after the configuration has been reset to factory defaults. The contents of this chapter are similar to the instructions in the quick start guide that shipped with your controller.

You use the configuration wizard to configure basic settings. You can run the wizard on the CLI or the GUI. This section explains how to run the wizard on the CLI.

This section contains these sections:

- Before You Start, page 4-2
- Resetting the Device to Default Settings, page 4-3
- Running the Configuration Wizard on the CLI, page 4-4

Before You Start

You should collect these basic configuration parameters before configuring the controller:

- System name for the controller
- 802.11 protocols supported: 802.11a/n or 802.11b/g/n or both
- Administrator usernames and passwords (optional)
- Distribution system (network) port static IP address, netmask, and optional default gateway IP address
- Service port static IP address and netmask (optional)
- Distribution system physical port (1000BASE-T, 1000BASE-SX, or 10/100BASE-T)

Note Each 1000BASE-SX connector provides a 100/1000-Mbps wired connection to a network through an 850nM (SX) fiber-optic link using an LC physical connector.

- Distribution system port VALN assignment (optional)
- Distribution system port web and secure web mode settings: enabled or disabled
- Distribution system port Spanning Tree Protocol: enabled/disabled, 802.1D/fast/off mode per port, path cost per port, priority per port, bridge priority, forward delay, hello time, maximum age
- WLAN configuration: SSID, VLAN assignments, Layer 2 security settings, Layer 3 security settings, QoS assignments
- Mobility Settings: Mobility Group Name (optional)
- RADIUS Settings
- SNMP Settings
- NTP server settings (the wizard prompts you for NTP server settings when you run the wizard on a wireless controller network module installed in a Cisco Integrated Services router)
- Other port and parameter settings: service port, Radio Resource Management (RRM), third-party access points, console port, 802.3x flow control, and system logging

Resetting the Device to Default Settings

If you need to start over during the initial setup process, you can reset the controller to factory default settings.

Note After resetting the configuration to defaults, you need a serial connection to the controller to use the configuration wizard.

Resetting to Default Settings Using the CLI

Follow these steps to reset the configuration to factory default settings using the CLI.

Step 1 Enter **reset system**. At the prompt that asks whether you need to save changes to the configuration, enter **Y** or **N**. The unit reboots.

Step 2 When you are prompted for a username, enter **recover-config** 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.

Resetting to Default Settings Using the GUI

Follow these steps to return to default settings using the GUI.

Step 1 Open your Internet browser. The GUI is fully compatible with Microsoft Internet Explorer version 6.0 or later on s platforms.

Step 2 Enter the controller IP address in the browser address line and press **Enter**. An Enter Network Password s appears.

Step 3 Enter your username in the User Name field. The default username is *admin*.

Step 4 Enter the wireless device password in the Password field and press **Enter**. The default password is *admin*.

Step 5 Browse to the Commands > Reset to Factory Defaults page.

Step 6 Click **Reset**. At the prompt, confirm the reset.

Step 7 Reboot the unit and do not save changes.

Step 8 Use the configuration wizard to enter configuration settings.

Running the Configuration Wizard on the CLI

When the controller boots at factory defaults, the bootup script runs the configuration wizard, which prompts the installer for initial configuration settings. Follow these steps to enter settings using the wizard on the CLI.

Note To configure the controller in the Catalyst 3750G Integrated Wireless LAN Controller Switch, Cisco recommends that you use the GUI configuration wizard that launches from the 3750 Device Manager. Refer to the *Catalyst 3750G Integrated Wireless LAN Controller Switch Getting Started Guide* for instructions.

Note The available options appear in brackets after each configuration parameter. The default value appears in all uppercase letters.

Note 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.

Note Press the hyphen key if you ever need to return to the previous command line.

Step 1 Connect your computer to the controller using a DB-9 null-modem serial cable.

Step 2 Open a terminal emulator session using these settings:

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

Step 3 At the prompt, log into the CLI. The default username is *admin* and the default password is *admin*.

Step 4 If necessary, enter **reset system** to reboot the unit and start the wizard.

Step 5 Enter the system name, which is the name you want to assign to the controller. You can enter up to 32 ASCII characters.

Step 6 Enter the administrative username and password to be assigned to this controller. You can enter up to 24 ASCII characters for each. The default administrative username and password are *admin* and *admin*, respectively.

Step 7 Enter the service-port interface IP configuration protocol: **none** or **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**.

Step 8 If you entered **none** in step 7 and need to enter a static IP address for the service port, enter the service-port interface IP address and netmask for the next two prompts.

Step 9 Enable or disable link aggregation (LAG) by choosing **yes** or **NO**. Refer to Chapter 3 for more information on LAG.

Step 10 Enter the IP address of the management interface.

Step 11 Enter the IP address of the management interface netmask.

Step 12 Enter the IP address of the default router.

Step 13 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 14 Enter the network interface (distribution system) physical port number. For the controller, the possible ports are 1 through 4 for a front panel GigE port.

Step 15 Enter the IP address of the default DHCP server that will supply IP addresses to clients, the management interface, and the service port interface if you use one.

Step 16 Enter the IP address of the access point manager interface.

Step 17 Enter the IP address of the controller's virtual interface. You should enter a fictitious, unassigned IP address such as 1.1.1.1.

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 18 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. See Chapter 11 and Chapter 12 for more information.

Step 19 Enable or disable symmetric mobility tunneling by entering **yes** or **no**. Symmetric mobility tunneling allows inter-subnet mobility to continue when reverse path filtering (RPF) is enabled on a router on any of the subnets. Refer to Chapter 12 for more information.

Step 20 Enter the network name, or service set identifier (SSID). The initial SSID enables basic functionality of the controller and allows access points that have joined the controller to enable their radios.

Step 21 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 22 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 documentation for more details."

Step 23 Enter the code for the country in which the network is located. 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. See the "Configuring Country Codes" section on page 7-49 for instructions.

Step 24 When you run the wizard on a wireless controller network module installed in a Cisco Integrated Services Router, the wizard prompts you for NTP server settings. The controller network module 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.

Step 25 Enable or disable support for each of the 802.11b, 802.11a, and 802.11g lightweight access point networks by entering **yes** or **no**.

Step 26 Enable or disable the radio resource management (RRM) auto-RF feature by entering **yes** or **no**. Refer to Chapter 11 for more information on RRM.

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.

The controller saves your configuration, reboots, and prompts you to log in or to enter **recover-config** to reset to the factory default configuration and return to the wizard.

Using the AutoInstall Feature for Controllers Without a Configuration

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.

Note The Cisco WiSM controllers do not support the AutoInstall feature.

Overview of AutoInstall

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]:
```

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.

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

AutoInstall uses the following interfaces:

- 4400 series controllers
  - eth0—Service port (untagged)
  - dtl0—Gigabit port 1 through the NPU (untagged)
- 2100 series controllers
  - dtl0—FastEthernet port 1 (untagged)

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 host name, this name (truncated at the first period [.]) is used as the host name 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) field is valid, AutoInstall performs a DNS lookup on this sname. If the DNS lookup is successful, the IP address that is returned is used as the IP address of the TFTP server.
  - 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) field is non-zero, 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.

Note For more information on configuring DHCP on a controller, see the "Configuring DHCP" section on page 6-8.

Note For more information on configuring a TFTP server on a controller, see Chapter 9.

Note For more information on configuring DHCP and TFTP servers through WCS, see Chapter 10 of the *Cisco Wireless Control System Configuration Guide, Release 5.2.*

Selecting a Configuration File

After the host name 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 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 field
- *host name*-confg
- *host name*.cfg
- *base MAC address*-confg (for example, 0011.2233.4455-confg)
- *serial number*-confg
- ciscowlc-confg
- 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 For information about creating and uploading a configuration file that AutoInstall can obtain from a TFTP server, see Chapter 9.

Note WCS release 5.0 or later provides 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 5.2*.

Example of 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-config'
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: interation 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-config'
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-config'
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 ==> 255.255.254.0
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-config'
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 System Date and Time

You can configure the controller to obtain the date and time from a Network Time Protocol (NTP) server, or you can configure the date and time manually. Greenwich Mean Time (GMT) is used as the standard for setting the time zone on the controller.

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:

1. To specify the NTP server for the controller, enter this command:

   config time ntp server *index ip_address*

2. To specify the polling interval (in seconds), enter this command:

   config time ntp *interval*

Configuring the Date and Time Manually

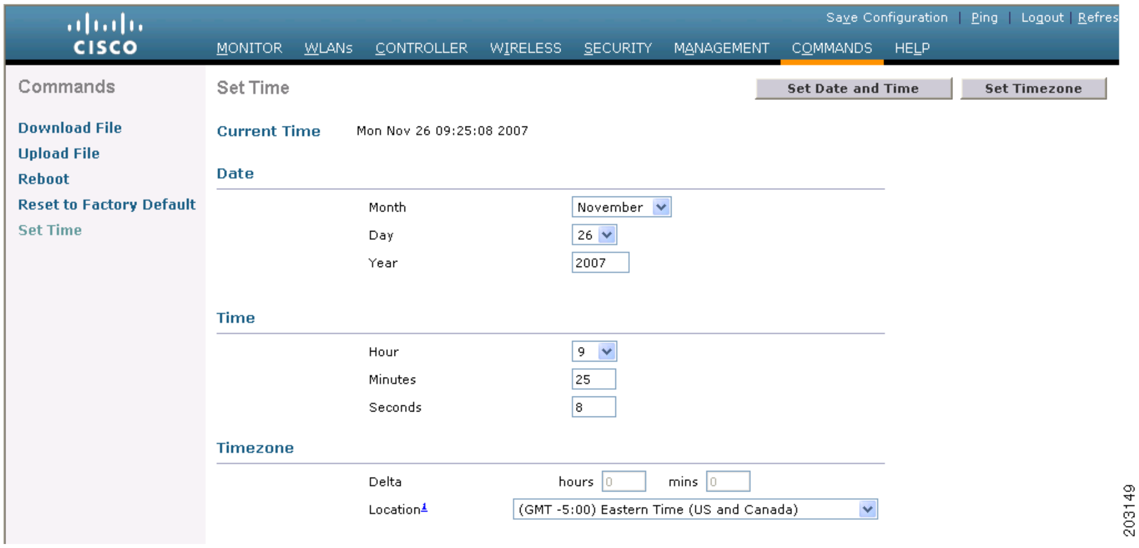
Follow the instructions in this section to configure the date and time manually using the controller GUI or CLI.

Using the GUI to Configure the Date and Time

Using the controller GUI, follow these steps to configure the local date and time.

Step 1 Click **Commands** > **Set Time** to open the Set Time page (see Figure 4-1).

Figure 4-1 Set Time Page



Set Time

Current Time Mon Nov 26 09:25:08 2007

Date

Month November

Day 26

Year 2007

Time

Hour 9

Minutes 25

Seconds 8

Timezone

Delta hours 0 mins 0

Location (GMT -5:00) Eastern Time (US and Canada)

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

Step 2 In the Timezone section, choose your local time zone from the Location drop-down box.

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 fields on the controller GUI.

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

Step 4 In the Date section, choose the current local month and day from the Month and Day drop-down boxes, and enter the year in the Year field.

Step 5 In the Time section, choose the current local hour from the Hour drop-down box, and enter the minutes and seconds in the Minutes and Seconds fields.

Note If you change the time zone location after setting the date and time, the values in the Time section 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.

Using the CLI to Configure the Date and Time

Using the controller CLI, follow these steps to configure the local date and time.

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, Jakatar
  - 25. (GMT +8:00) Hong Kong, Bejing, Chongquing
  - 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

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:

  config time timezone *delta_hours delta_mins*

  where *delta_hours* is the local hour difference from GMT, and *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:

save config

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

show time

Information similar to the following appears:

```
Time.......................................... Mon Nov 26 10:25:33 2007

Timezone delta................................ 0:0
Timezone location............................. (GMT -5:00) Eastern Time (US and Canada)

NTP Servers
    NTP Polling Interval.........................     86400

     Index              NTP Server
    -------  -------------------------------
       1     19.1.1.1
```

Note If you configured the time zone location, the Timezone Delta value is set to “0:0.” If you manually configured the time zone using the time zone delta, the Timezone Location is blank.

Configuring 802.11 Bands

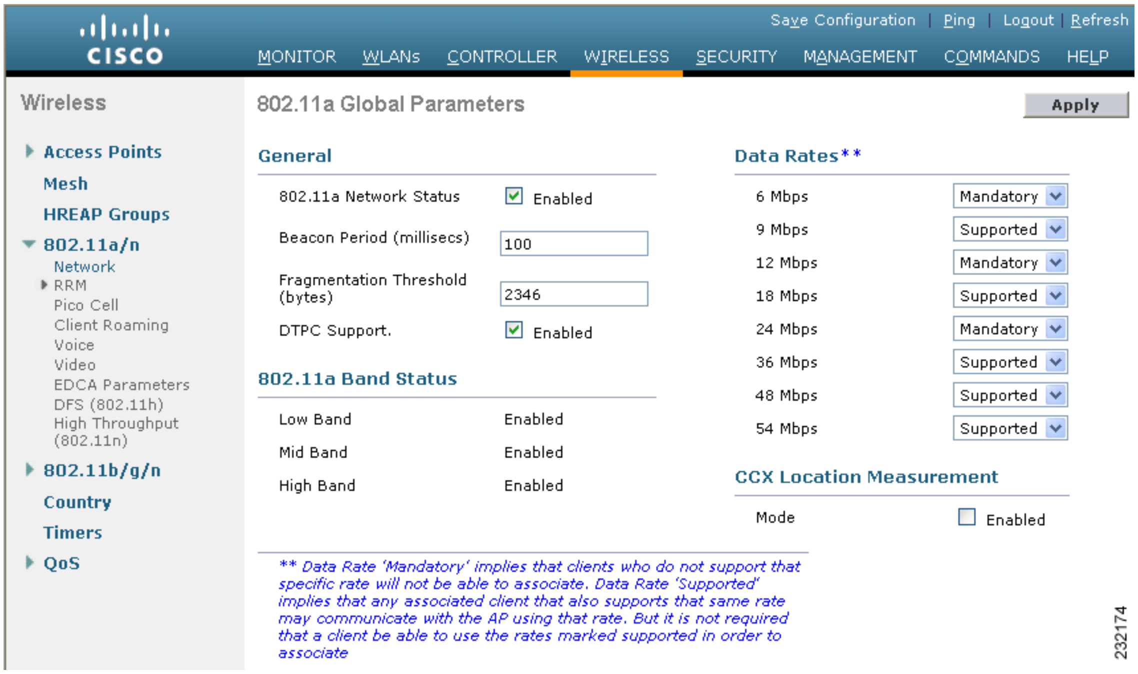
You can configure the 802.11b/g/n (2.4-GHz) and 802.11a/n (5-GHz) bands for the controller to comply with the regulatory requirements in your country. By default, both 802.11b/g/n and 802.11a/n are enabled.

Using the GUI to Configure 802.11 Bands

Using the controller GUI, follow these steps to configure 802.11 bands.

Step 1 Click **Wireless** > **802.11a/n** or **802.11b/g/n** > **Network** to open the 802.11a (or 802.11b/g) Global Parameters page (see Figure 4-2).

Figure 4-2 802.11a Global Parameters Page



802.11a Global Parameters

General

802.11a Network Status	☑ Enabled
Beacon Period (millisecs)	100
Fragmentation Threshold (bytes)	2346
DTPC Support.	☑ Enabled

802.11a Band Status

Low Band	Enabled
Mid Band	Enabled
High Band	Enabled

Data Rates**

6 Mbps	Mandatory
9 Mbps	Supported
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Mandatory
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

CCX Location Measurement

Mode	□ Enabled

*** Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate*

Step 2 To enable the 802.11a or 802.11b/g band, check the **802.11a** (or **802.11b/g**) **Network Status** check box. To disable the band, uncheck 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, check 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 To specify the rate at which the SSID is broadcast by the access point, enter a value between 100 and 600 milliseconds (inclusive) in the Beacon Period field. The default value is 100 milliseconds.

Step 5 To specify the size at which packets are fragmented, enter a value between 256 and 2346 bytes (inclusive) in the Fragmentation Threshold field. Enter a low number for areas where communication is poor or where there is a great deal of radio interference.

Step 6 To make access points advertise their channel and transmit power level in beacons and probe responses, check the **DTPC Support** check box. Otherwise, uncheck 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.

Note On access points that run Cisco IOS software, this feature is called *world mode*.

Step 7 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 8 Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your changes.

Using the CLI to Configure 802.11 Bands

Using the controller CLI, follow these steps to configure 802.11 bands.

Step 1 To disable the 802.11a band, enter 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 To disable the 802.11b/g band, enter 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 To specify the rate at which the SSID is broadcast by the access point, enter this command:

config {**802.11a** | **802.11b**} **beaconperiod** *time_unit*

where *time_unit* is the beacon interval in time units (TU). One TU is 1024 micro seconds. You can configure the access point to send a beacon every 20 to 1000 milliseconds.

Step 4 To specify the size at which packets are fragmented, enter 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 To make access points advertise their channel and transmit power level in beacons and probe responses, enter 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 To specify the rates at which data can be transmitted between the controller and the client, enter this command:

config {**802.11a** | **802.11b**} **rate** {**disabled** | **mandatory** | **supported**} *rate*

where

- **disabled**—The clients specify the data rates used for communication.
- **mandatory**—Specifies that 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 7 To enable the 802.11a band, enter this command:

config 802.11a enable network

The default value is enabled.

Step 8 To enable the 802.11b band, enter this command:

config 802.11b enable network

The default value is enabled.

Step 9 To enable or disable 802.11g network support, enter 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 10 To save your changes, enter this command:

save config

Step 11 To view the configuration settings for the 802.11a or 802.11b/g band, enter 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
...
```

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.

Note The 802.11n high-throughput rates are available only on 1140 and 1250 series access points for WLANs using WMM with no Layer 2 encryption or with WPA2/AES encryption enabled.

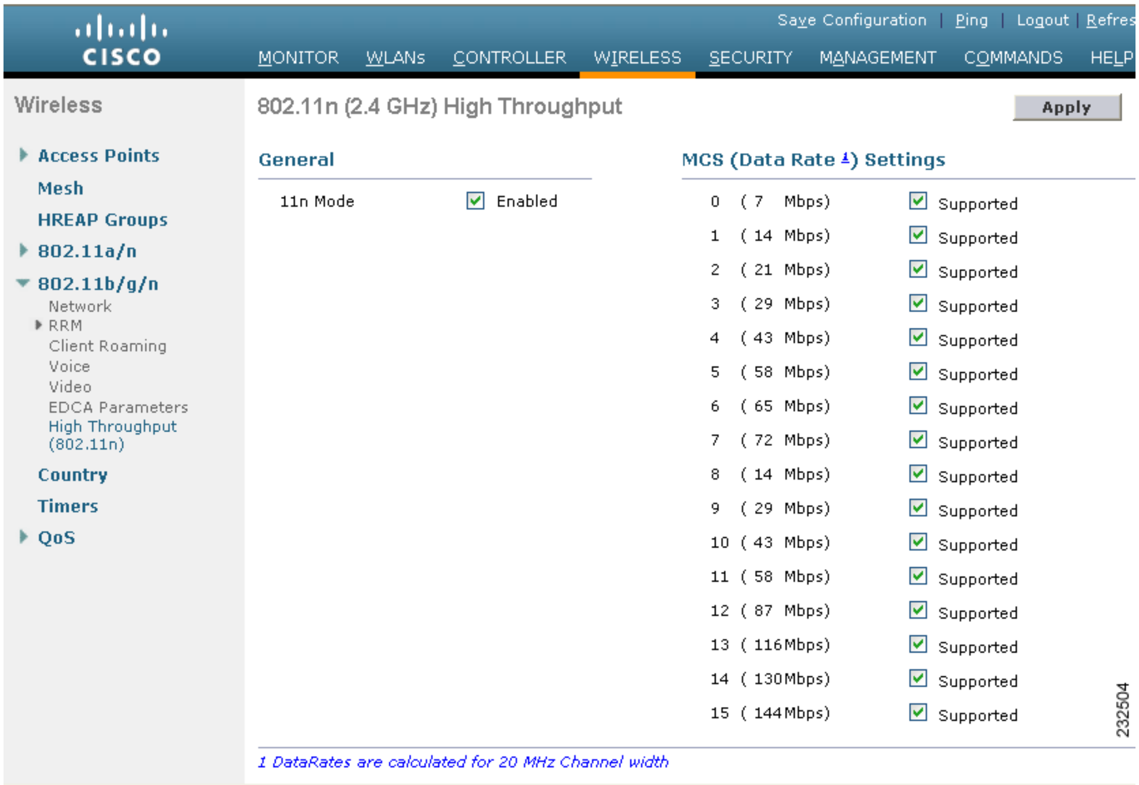
Note For information on configuring radio resource management (RRM) parameters or statically assigning radio parameters for 802.11n access points, refer to Chapter 11.

Using the GUI to Configure 802.11n Parameters

Using the controller GUI, follow these steps to configure 802.11n parameters.

Step 1 Click **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 (see Figure 4-3).

Figure 4-3 802.11n (2.4 GHz) High Throughput Page



802.11n (2.4 GHz) High Throughput

General

11n Mode ☑ Enabled

MCS (Data Rate 1) Settings

0	(7 Mbps)	☑ Supported
1	(14 Mbps)	☑ Supported
2	(21 Mbps)	☑ Supported
3	(29 Mbps)	☑ Supported
4	(43 Mbps)	☑ Supported
5	(58 Mbps)	☑ Supported
6	(65 Mbps)	☑ Supported
7	(72 Mbps)	☑ Supported
8	(14 Mbps)	☑ Supported
9	(29 Mbps)	☑ Supported
10	(43 Mbps)	☑ Supported
11	(58 Mbps)	☑ Supported
12	(87 Mbps)	☑ Supported
13	(116Mbps)	☑ Supported
14	(130Mbps)	☑ Supported
15	(144Mbps)	☑ Supported

1 DataRates are calculated for 20 MHz Channel width

Step 2 Check the **11n Mode** check box to enable 802.11n support on the network. The default value is enabled.

Step 3 To specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client, check the check boxes of the desired rates. 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)
- 10 (43 Mbps)
- 11 (58 Mbps)
- 12 (87 Mbps)

- 13 (116 Mbps)
- 14 (130 Mbps)
- 15 (144 Mbps)

Any associated clients that support the selected rates may communicate with the access point using those rates. However, the clients are not required to be able to use this rate in order to associate. The MCS settings determine the number of spatial streams, the modulation, the coding rate, and the data rate values that are used.

Step 4 Click **Apply** to commit your changes.

Step 5 To use the 802.11n data rates that you configured, you need to enable WMM on the WLAN. Follow these steps to do so:

a. Click **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, click the **QoS** tab to open the WLANs > Edit (Qos) page.

d. From the WMM Policy drop-down box, 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 field 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.

Using the CLI to Configure 802.11n Parameters

Using the controller CLI, follow these steps to configure 802.11n parameters.

Step 1 To enable 802.11n support on the network, enter this command:

config {**802.11a** | **802.11b**} **11nsupport** {**enable** | **disable**}

Step 2 To specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client, enter 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 "Using the GUI to Configure 802.11n Parameters" section on page 4-17.

Step 3 To use the 802.11n data rates that you configured, you need to enable WMM on the WLAN. Enter this command to do so:

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 To specify the aggregation method used for 802.11n packets, follow these steps:

a. To disable the network, enter this command:

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

b. To specify the aggregation method, enter 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). A-MPDU is performed in the software whereas A-MSDU is performed in the hardware.

You can specify the aggregation method for various types of traffic from the access point to the clients. Table 4-1 defines the priority levels (0-7) assigned per traffic type.

Table 4-1 Traffic Type Priority Levels

User Priority	Traffic Type
0	Best effort
1	Background
2	Spare
3	Excellent effort
4	Controlled load
5	Video, less than 100-ms latency and jitter
6	Voice, less than 10-ms latency and jitter
7	Network control

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, only priority level 0 is enabled.

c. To re-enable the network, enter this command:

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

Step 5 To save your changes, enter this command:

save config

Step 6 To view the configuration settings for the 802.11a/n or 802.11b/g/n band, enter 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
Pico-Cell Status............................... Disabled
Pico-Cell-V2 Status............................ Disabled
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
   Voice AC - Admission control (ACM)........... Enabled
   Voice max RF bandwidth....................... 75
   Voice reserved roaming bandwidth............. 6
   Voice load-based CAC mode.................... Disabled
   Voice tspec inactivity timeout............... Disabled
   Video AC - Admission control (ACM)........... Enabled
```

```
Voice Stream-Size............................ 84000
Voice Max-Streams............................ 2
Video max RF bandwidth....................... Infinite
Video reserved roaming bandwidth........... 0
```

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.

You can use the controller GUI or CLI to enable or disable DHCP proxy on a global basis, rather than on a WLAN basis. DHCP proxy is enabled by default.

Note DHCP proxy must be enabled in order for DHCP option 82 to operate correctly. Refer to the "Configuring DHCP Option 82" section on page 5-53 for information on DHCP option 82.

Note All controllers that will communicate must have the same DHCP proxy setting.

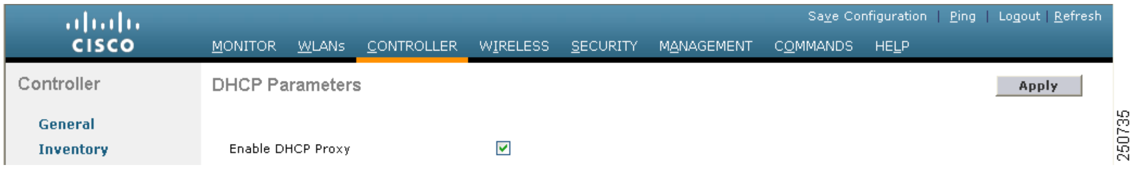
Note Refer to Chapter 6 for information on configuring DHCP servers.

Using the GUI to Configure DHCP Proxy

Using the controller GUI, follow these steps to configure DHCP proxy.

Step 1 Click **Controller** > **Advanced** > **DHCP** to open the DHCP Parameters page (see Figure 4-4).

Figure 4-4 DHCP Parameters Page



DHCP Parameters

Enable DHCP Proxy ☑

Step 2 To enable DHCP proxy on a global basis, check the **Enable DHCP Proxy** check box. Otherwise, uncheck the check box. The default value is checked.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuratio**n to save your changes.

Using the CLI to Configure DHCP Proxy

Using the controller CLI, follow these steps to configure DHCP proxy.

Step 1 To enable or disable DHCP proxy, enter this command:

config dhcp proxy {**enable** | **disable**}

Step 2 To view the DHCP proxy configuration, enter this command:

show dhcp proxy

Information similar to the following appears:

```
DHCP Proxy Behavior: enabled
```

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

Using the controller CLI, follow these steps to configure administrator usernames and passwords:

Step 1 To configure a username and password, enter 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 this command: **config mgmtuser password** *username new_password*

Step 2 To list configured users, enter this command:

show mgmtuser

Restoring Passwords

If you ever forget your password, follow these steps to configure a new username and password at boot-up using the CLI from the controller's serial console:

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, re-enter 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

Cisco recommends that you use the GUI to configure SNMP settings on the controller. To use the CLI, follow these steps:

Step 1 Enter **config snmp community create** *name* to create an SNMP community name.

Step 2 Enter **config snmp community delete** *name* to delete an SNMP community name.

Step 3 Enter **config snmp community accessmode ro** *name* 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 **config snmp community ipaddr** *ip-address ip-mask name* 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. The requesting entity's IP address is ANDed with 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.

Note The controller can use only one IP address range to manage an SNMP community.

Step 5 Enter **config snmp community mode enable** to enable a community name. Enter **config snmp community mode disable** to disable a community name.

Step 6 Enter **config snmp trapreceiver create** *name ip-address* to configure a destination for a trap.

Step 7 Enter **config snmp trapreceiver delete** *name* to delete a trap.

Step 8 Enter **config snmp trapreceiver ipaddr** *old-ip-address name new-ip-address* to change the destination for a trap.

Step 9 Enter **config snmp trapreceiver mode enable** to enable traps. Enter **config snmp trapreceiver mode disable** to disable traps.

Step 10 Enter **config snmp syscontact** *syscontact-name* to configure the name of the SNMP contact. Enter up to 31 alphanumeric characters for the contact name.

Step 11 Enter **config snmp syslocation** *syslocation-name* to configure the SNMP system location. Enter up to 31 alphanumeric characters for the location.

Step 12 Use the **show snmpcommunity** and **show snmptrap** commands to verify that the SNMP traps and communities are correctly configured.

Step 13 Use the **show trapflags** command to see the enabled and disabled trapflags. If necessary, use the **config trapflags** commands to enable or disable trapflags.

Changing the Default Values of SNMP Community Strings

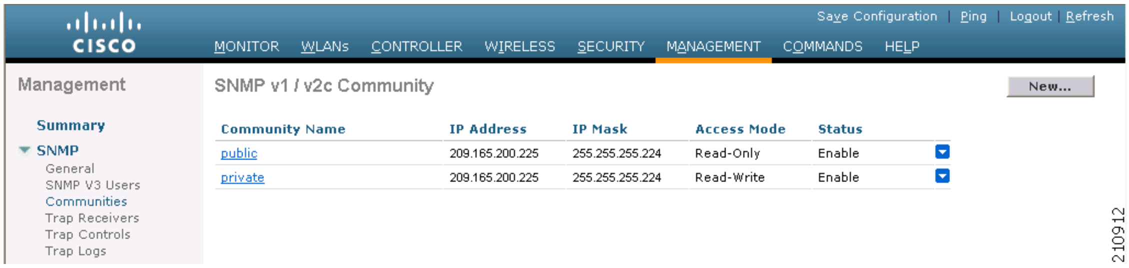
The controller has commonly known default values of "public" and "private" for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values.

Using the GUI to Change the SNMP Community String Default Values

Follow these steps to change the SNMP community string default values through the controller GUI.

Step 1 Click **Management** and then **Communities** under SNMP. The SNMP v1 / v2c Community page appears (see Figure 4-5).

Figure 4-5 SNMP v1 / v2c Community Page



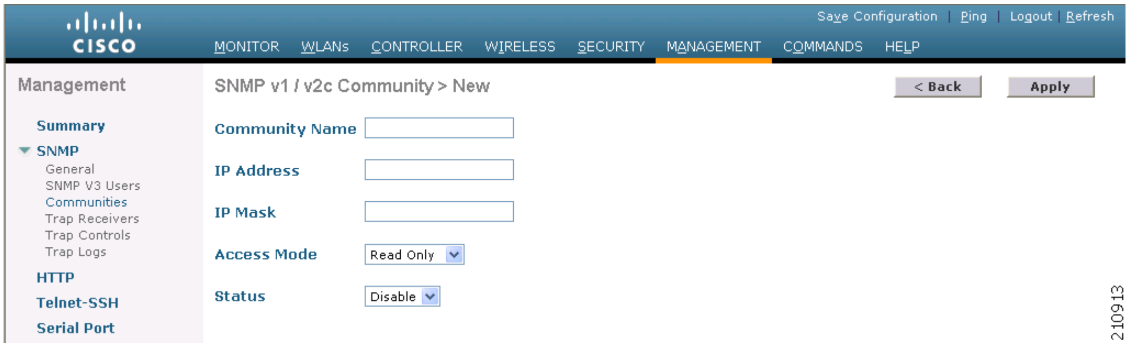
SNMP v1 / v2c Community

Community Name	IP Address	IP Mask	Access Mode	Status
public	209.165.200.225	255.255.255.224	Read-Only	Enable
private	209.165.200.225	255.255.255.224	Read-Write	Enable

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 (see Figure 4-6).

Figure 4-6 SNMP v1 / v2c Community > New Page



SNMP v1 / v2c Community > New

Community Name

IP Address

IP Mask

Access Mode: Read Only

Status: Disable

Step 4 In the Community Name field, enter a unique name containing up to 16 alphanumeric characters. Do not enter "public" or "private."

Step 5 In the next two fields, 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 box to specify the access level for this community.

Step 7 Choose **Enable** or **Disable** from the Status drop-down box 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.

Using the CLI to Change the SNMP Community String Default Values

Follow these steps to change the SNMP community string default values through the controller CLI.

Step 1 To see the current list of SNMP communities for this controller, enter 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:

config snmp community delete *name*

The *name* parameter is the community name (in this case, "public" or "private").

Step 3 To create a new community, enter 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 To enter the IP address from which this device accepts SNMP packets with the associated community, enter this command:

config snmp community ipaddr *ip_address ip_mask name*

Step 5 To specify the access level for this community, enter this command, where **ro** is read-only mode and **rw** is read/write mode:

config snmp community accessmode {**ro** | **rw**} *name*

Step 6 To enable or disable this SNMP community, enter this command:

config snmp community mode {**enable** | **disable**} *name*

Step 7 To save your changes, enter **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 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.

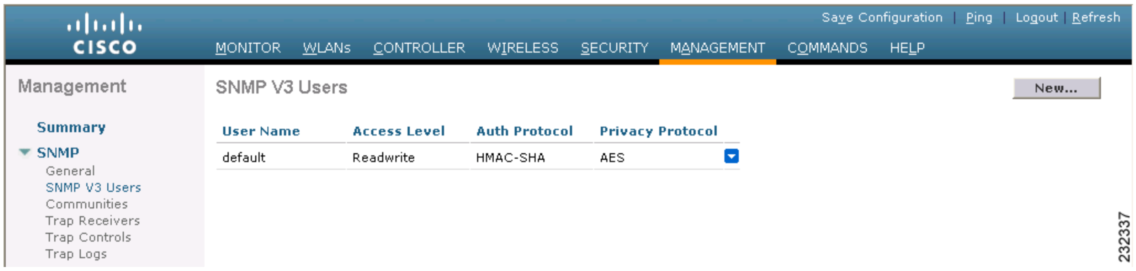
Note SNMP v3 is time sensitive. Make sure that you have configured the correct time and time zone on your controller.

Using the GUI to Change the SNMP v3 User Default Values

Follow these steps to change the SNMP v3 user default values through the controller GUI.

Step 1 Click **Management > SNMP > SNMP V3 Users** to open the SNMP V3 Users page (see Figure 4-7).

Figure 4-7 SNMP V3 Users Page



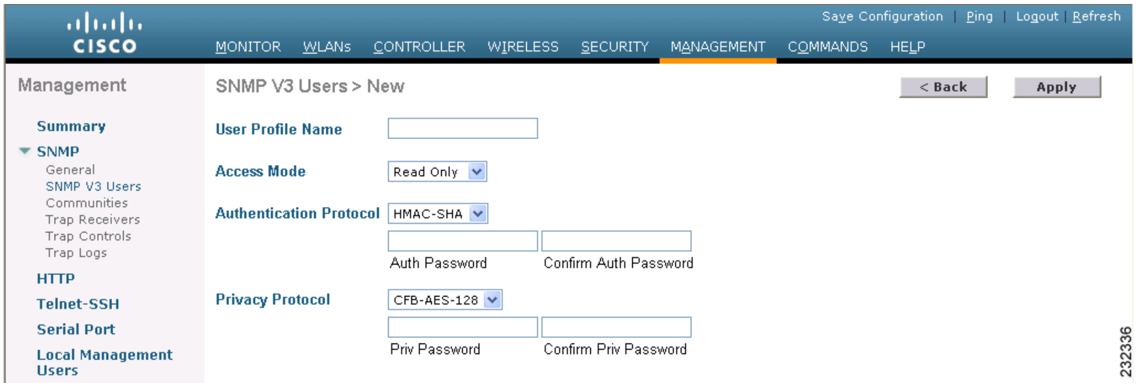
SNMP V3 Users

User Name	Access Level	Auth Protocol	Privacy Protocol
default	Readwrite	HMAC-SHA	AES

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 (see Figure 4-8).

Figure 4-8 SNMP V3 Users > New Page



SNMP V3 Users > New

User Profile Name

Access Mode: Read Only

Authentication Protocol: HMAC-SHA

Auth Password / Confirm Auth Password

Privacy Protocol: CFB-AES-128

Priv Password / Confirm Priv Password

Step 4 In the User Profile Name field, enter a unique name. Do not enter “default.”

Step 5 Choose **Read Only** or **Read Write** from the Access Mode drop-down box to specify the access level for this user. The default value is Read Only.

Step 6 From the Authentication Protocol drop-down box, 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 fields, 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 box, 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 fields, 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.

Using the CLI to Change the SNMP v3 User Default Values

Follow these steps to change the SNMP v3 user default values through the controller CLI.

Step 1 To see the current list of SNMP v3 users for this controller, enter this command:

show snmpv3user

Step 2 If “default” appears in the SNMP v3 User Name column, enter this command to delete this user:

config snmp v3user delete *username*

The *username* parameter is the SNMP v3 username (in this case, “default”).

Step 3 To create a new SNMP v3 user, enter this command:

config snmp v3user create *username* {**ro** | **rw**} {**none** | **hmacmd5** | **hmacsha**} {**none** | **des** | **aescfb128**} *auth_key encrypt_key*

where

- *username* is the SNMP v3 username;
- **ro** is read-only mode and **rw** is read-write mode;
- **none**, **hmacmd5**, and **hmacsha** are the authentication protocol options;
- **none**, **des**, and **aescfb128** are the privacy protocol options;
- *auth_key* is the authentication shared secret key; and
- *encrypt_key* is the encryption shared secret key.

Do not enter “default” for the *username*, *auth_key*, and *encrypt_key* parameters.

Step 4 To save your changes, enter **save config**.

Step 5 To reboot the controller so that the SNMP v3 user that you added takes effect, enter **reset system**.

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 GUI or CLI.

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 that the access point is too busy to accept any more associations. The client then attempts to associate to a different access point. For example, if load balancing is enabled and the client count is configured as 5 clients, when a sixth client tries to associate to the access point, the client receives an 802.11 response packet with status code 17, indicating that the access point is busy.

Note When you use Cisco 7921 and 7920 Wireless IP Phones with controllers, make sure that aggressive load balancing is disabled for each controller. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.

Using the GUI to Configure Aggressive Load Balancing

Follow these steps to configure aggressive load balancing using the GUI.

Step 1 Click **Controller** > **General** to open the General page.

Step 2 From the Aggressive Load Balancing drop-down box, choose either **Enabled** or **Disabled** to configure this feature.

Step 3 Click **Apply** to commit your changes.

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

Using the CLI to Configure Aggressive Load Balancing

Follow these steps to configure aggressive load balancing using the CLI.

Step 1 To enable or disable aggressive load balancing, enter this command:

config load-balancing status {**enable** | **disable**}

Step 2 To set the client count for aggressive load balancing, enter this command:

config load-balancing window *clients*

You can enter a value between 0 and 20 for the *clients* parameter.

Step 3 To save your changes, enter this command:

save config

Step 4 To verify your settings, enter this command:

show load-balancing

Information similar to the following appears:

```
Aggressive Load Balancing....................... Enabled
Aggressive Load Balancing Window............. 5 clients
```

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.

Using the GUI to Configure Fast SSID Changing

Using the controller GUI, follow these steps to configure fast SSID changing for mobile clients.

Step 1 Click **Controller** to open the General page.

Step 2 From the Fast SSID Change drop-down box, 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.

Using the CLI to Configure Fast SSID Changing

Using the controller CLI, follow these steps to configure fast SSID changing for mobile clients.

Step 1 To enable or disable fast SSID changing, enter this command:

config network fast-ssid-change {**enable** | **disable**}

Step 2 To save your changes, enter this command:

save config

Enabling 802.3X Flow Control

802.3X Flow Control is disabled by default. To enable it, enter **config switchconfig flowcontrol enable**.

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.

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 and through the controller CLI in software release 4.0 or later.

Note In controller software release 5.2, the software-based forwarding architecture for 2100-series-based controllers is being replaced with a new forwarding plane architecture. As a result, 2100 series controllers and the Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers 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.

Note By default, 2100-series-based controllers running software release 5.2 bridge all non-IPv4 packets (such as Appletalk, IPv6, and so on).

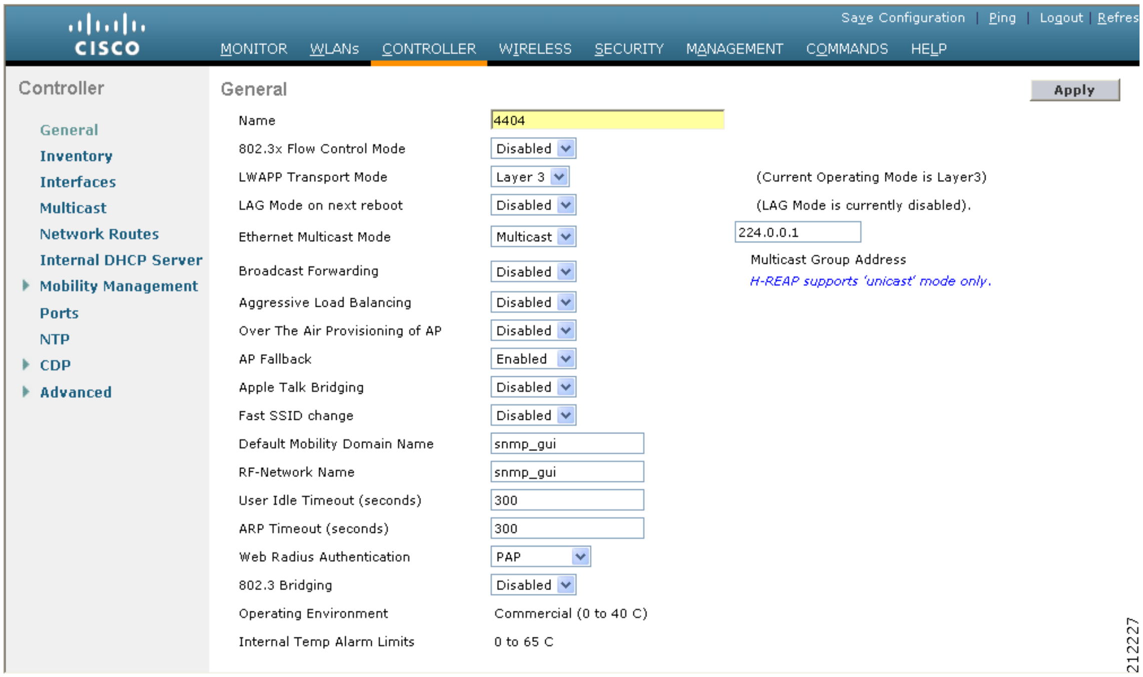
Note You can also configure 802.3 bridging using the Cisco Wireless Control System (WCS). Refer to the *Cisco Wireless Control System Configuration Guide* for instructions.

Using the GUI to Configure 802.3 Bridging

Follow these steps to configure 802.3 bridging using the controller GUI.

Step 1 Click **Controller** > **General** to open the General page (see Figure 4-9).

Figure 4-9 General Page



General

Name	4404	
802.3x Flow Control Mode	Disabled	
LWAPP Transport Mode	Layer 3	(Current Operating Mode is Layer3)
LAG Mode on next reboot	Disabled	(LAG Mode is currently disabled).
Ethernet Multicast Mode	Multicast	224.0.0.1 Multicast Group Address
Broadcast Forwarding	Disabled	H-REAP supports 'unicast' mode only.
Aggressive Load Balancing	Disabled	
Over The Air Provisioning of AP	Disabled	
AP Fallback	Enabled	
Apple Talk Bridging	Disabled	
Fast SSID change	Disabled	
Default Mobility Domain Name	snmp_gui	
RF-Network Name	snmp_gui	
User Idle Timeout (seconds)	300	
ARP Timeout (seconds)	300	
Web Radius Authentication	PAP	
802.3 Bridging	Disabled	
Operating Environment	Commercial (0 to 40 C)	
Internal Temp Alarm Limits	0 to 65 C	

Step 2 From the 802.3 Bridging drop-down box, 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, 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.

Using the CLI to Configure 802.3 Bridging

Follow these steps to configure 802.3 bridging using the controller CLI.

Step 1 To see the current status of 802.3 bridging for all WLANs, enter this command:

show network

Step 2 To enable or disable 802.3 bridging globally on all WLANs, enter this command:

config network 802.3-bridging {**enable** | **disable**}

The default value is disabled.

Note In controller software release 5.2, you can disable 802.3 bridging only for 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch.

Step 3 To save your settings, enter this command:

save config

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.

You can enable multicast mode using the controller GUI or CLI.

Understanding Multicast Mode

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.

In controller software release 4.2 or later, 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 checking 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.

Note The MGIDs are controller specific. The same multicast group packets coming from the same VLAN in two different controllers may be mapped to two different MGIDs.

Note If Layer 2 multicast is enabled, a single MGID is assigned to all the multicast addresses coming from an interface (see Figure 4-12).

Guidelines for Using Multicast Mode

Follow these guidelines when you enable multicast mode on your network:

- 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).

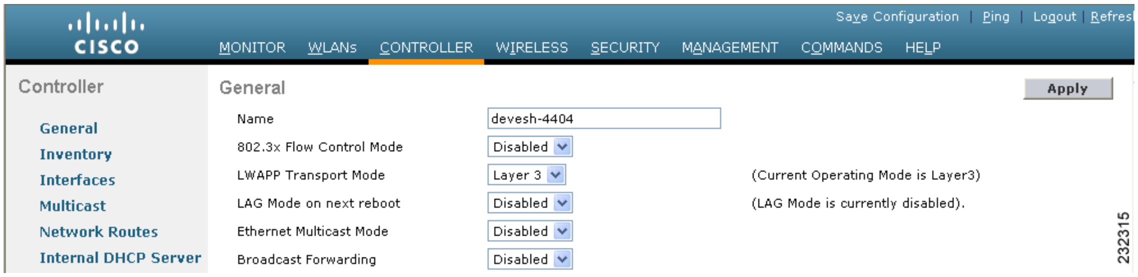
- For LWAPP, the controller drops multicast packets sent to UDP control port 12223. For CAPWAP, the controller drops multicast packets sent to UDP control and data ports 5246 and 5247, respectively. Therefore, you may want to consider not using these port numbers with the multicast applications on your network.
- Cisco recommends that any multicast applications on your network not use the multicast address configured as the CAPWAP multicast group address on the controller.
- 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.

Using the GUI to Enable Multicast Mode

Follow these steps to enable multicast mode using the controller GUI.

Step 1 Click **Controller** to open the General page (see Figure 4-10).

Figure 4-10 General Page



General

Name	devesh-4404	
802.3x Flow Control Mode	Disabled	
LWAPP Transport Mode	Layer 3	(Current Operating Mode is Layer3)
LAG Mode on next reboot	Disabled	(LAG Mode is currently disabled).
Ethernet Multicast Mode	Disabled	
Broadcast Forwarding	Disabled	

Step 2 Choose one of the following options from the Ethernet Multicast Mode drop-down box:

- **Disabled**—Disables multicasting on the controller. This is the default value.
- **Unicast**—Configures the controller to use the unicast method to send multicast packets.
- **Multicast**—Configures the controller to use the multicast method to send multicast packets to a CAPWAP multicast group.

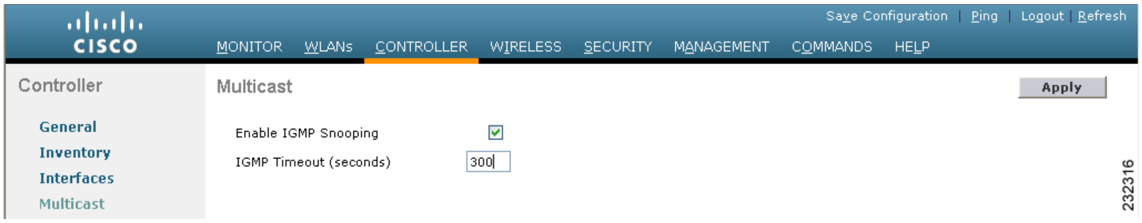
Note Hybrid REAP supports unicast mode only.

Step 3 If you chose Multicast in Step 2, enter the IP address of the multicast group in the Multicast Group Address field.

Step 4 Click **Apply** to commit your changes.

Step 5 Click **Multicast** to open the Multicast page (see Figure 4-11).

Figure 4-11 *Multicast Page*


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Controller
General
Inventory
Interfaces
Multicast
Multicast
Apply
232316

Enable IGMP Snooping ☑
IGMP Timeout (seconds) 300

Step 6 If you want to enable IGMP snooping, check the **Enable IGMP Snooping** check box. If you want to disable IGMP snooping, leave the check box unchecked. The default value is disabled.

Step 7 To set the IGMP timeout, enter a value between 30 and 300 seconds in the **IGMP Timeout** field. 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 8 Click **Apply** to commit your changes.

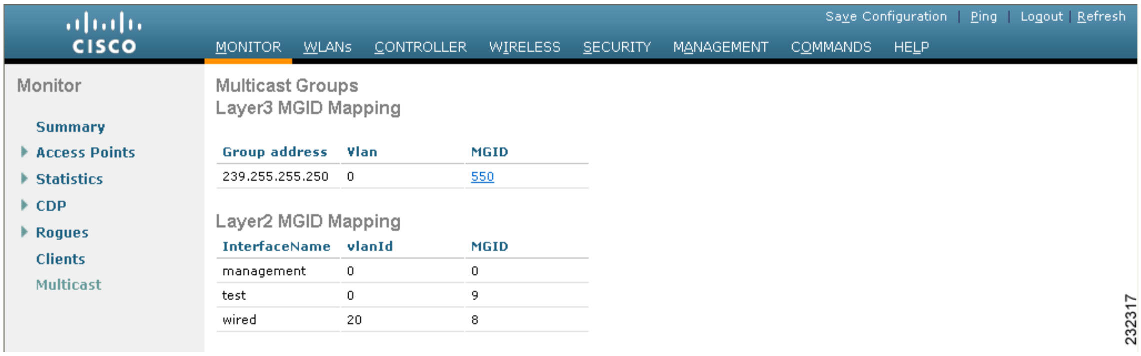
Step 9 Click **Save Configuration** to save your changes.

Using the GUI to View Multicast Groups

Follow these steps to view multicast groups using the controller GUI.

Step 1 Click **Monitor** > **Multicast**. The Multicast Groups page appears (see Figure 4-12).

Figure 4-12 *Multicast Groups Page*


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Access Points
Statistics
CDP
Rogues
Clients
Multicast
232317

Multicast Groups
Layer3 MGID Mapping

Group address	Vlan	MGID
239.255.255.250	0	550

Layer2 MGID Mapping

InterfaceName	vlanId	MGID
management	0	0
test	0	9
wired	20	8

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.

Using the CLI to Enable Multicast Mode

Follow these steps to enable multicast mode using the controller CLI.

Step 1 To enable or disable multicasting on the controller, enter 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 one of the following:

a. To configure the controller to use the unicast method to send multicast packets, enter this command:

config network multicast mode unicast

b. To configure the controller to use the multicast method to send multicast packets to a CAPWAP multicast group, enter this command:

config network multicast mode multicast *multicast_group_ip_address*

Step 3 To enable or disable IGMP snooping, enter this command:

config network multicast igmp snooping {**enable** | **disable**}

The default value is disabled.

Step 4 To set the IGMP timeout value, enter this command:

config network multicast igmp timeout *timeout*

You can enter a *timeout* value between 30 and 300 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 To save your changes, enter this command:

save config

Using the CLI to View Multicast Groups

Use these commands to view multicast groups using the controller CLI.

- To see all the multicast groups and their corresponding MGIDs, enter this command:

  show network multicast mgid summary

  Information similar to the following appears:

```
Layer2 MGID Mapping:
-------------------
InterfaceName                    vlanId   MGID
-------------------------------- ------   ----
management                       0        0
test                             0        9
wired                            20       8

Layer3 MGID Mapping:
-------------------
Number of Layer3 MGIDs........................... 1

 Group address    Vlan  MGID
 ---------------  ----  ----
 239.255.255.250  0     550
```

- To see all the clients joined to the multicast group in a specific MGID, enter this command:

  show network multicast mgid detail *mgid_value*

  where the *mgid_value* parameter is a number between 550 and 4095.

  Information similar to the following appears:

```
Mgid........................................ 550
Multicast Group Address..................... 239.255.255.250
Vlan........................................ 0
Rx Packet Count............................. 807399588
No of clients............................... 1
Client List.................................
        Client MAC             Expire Time (mm:ss)
        00:13:02:23:82:ad      0:20
```

Using the CLI to View an Access Point's Multicast Client Table

To help troubleshoot roaming events, you can view an access point's multicast client table from the controller by performing a remote debug of the access point. Follow these steps to do so using the controller CLI:

Step 1 To initiate a remote debug of the access point, enter this command:

debug ap enable *Cisco_AP*

Step 2 To see all of the MGIDs on the access point and the number of clients per WLAN, enter this command:

debug ap command "**show capwap mcast mgid all**" *Cisco_AP*

Step 3 To see all of the clients per MGID on the access point and the number of clients per WLAN, enter this command:

debug ap command "**show capwap mcast mgid id** *mgid_value*" *Cisco_AP*

Configuring 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, 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.

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.

  Note To see whether a particular client supports E2E, click **Wireless** > **Clients** on the controller GUI, click the **Detail** link for the desired client, and look at the E2E Version field under Client Properties.

- **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.

Controller software release 4.2 or later 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 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 6-39 for more information on CCX.

The roaming enhancements mentioned above are enabled automatically, with the appropriate CCX support.

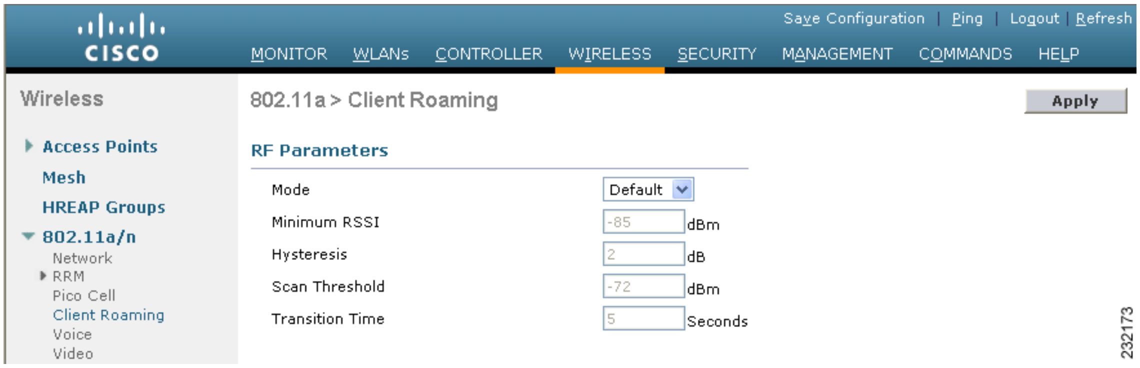
Note Hybrid-REAP access points in standalone mode do not support CCX Layer 2 roaming.

Using the GUI to Configure CCX Client Roaming Parameters

Follow these steps to configure CCX client roaming parameters using the GUI.

Step 1 Click **Wireless** > **802.11a/n** (or **802.11b/g/n**) > **Client Roaming**. The 802.11a (or 802.11b) > Client Roaming page appears (see Figure 4-13).

Figure 4-13   802.11a > Client Roaming Page



802.11a > Client Roaming

RF Parameters

Mode	Default	
Minimum RSSI	-85	dBm
Hysteresis	2	dB
Scan Threshold	-72	dBm
Transition Time	5	Seconds

Step 2 If you want to fine-tune the RF parameters that affect client roaming, choose **Custom** from the Mode drop-down box 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 field, 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.

Range: –80 to –90 dBm

Default: –85 dBm

Step 4 In the Hysteresis field, 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.

Range: 2 to 4 dB

Default: 2 dB

Step 5 In the Scan Threshold field, 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 below the threshold.

Range: –70 to –77 dBm

Default: –72 dBm

Step 6 In the Transition Time field, 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.

Range: 1 to 10 seconds

Default: 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).

Using the CLI to Configure CCX Client Roaming Parameters

To configure CCX Layer 2 client roaming parameters, enter 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 "Using the GUI to Configure CCX Client Roaming Parameters" section on page 4-42.

Using the CLI to Obtain CCX Client Roaming Information

Use these commands to view information about CCX Layer 2 client roaming.

1. To view the current RF parameters configured for client roaming for the 802.11a or 802.11b/g network, enter this command:

   show {**802.11a** | **802.11b**} **l2roam rf-param**

2. To view the CCX Layer 2 client roaming statistics for a particular access point, enter 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

3. To view the roaming history for a particular client, enter 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

Using the CLI to Debug CCX Client Roaming Issues

If you experience any problems with CCX Layer 2 client roaming, enter this command:

debug l2roam [**detail** | **error** | **packet** | **all]** {**enable** | **disable**}

Configuring IP-MAC Address Binding

In controller software release 5.2, 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.

Using the controller CLI, follow these steps to configure IP-MAC address binding.

Step 1 To enable or disable IP-MAC address binding, enter 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).

Step 2 To save your changes, enter this command:

save config

Step 3 To view the status of IP-MAC address binding, enter 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

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 levels:

- 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.

VoIP clients should be set to Platinum, Gold, or Silver while low-bandwidth clients can be set to Bronze.

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.

Configuring Quality of Service Profiles

You can use the controller GUI or CLI to configure the Platinum, Gold, Silver, and Bronze QoS profiles.

Using the GUI to Configure QoS Profiles

Follow these steps to configure QoS profiles using the controller GUI.

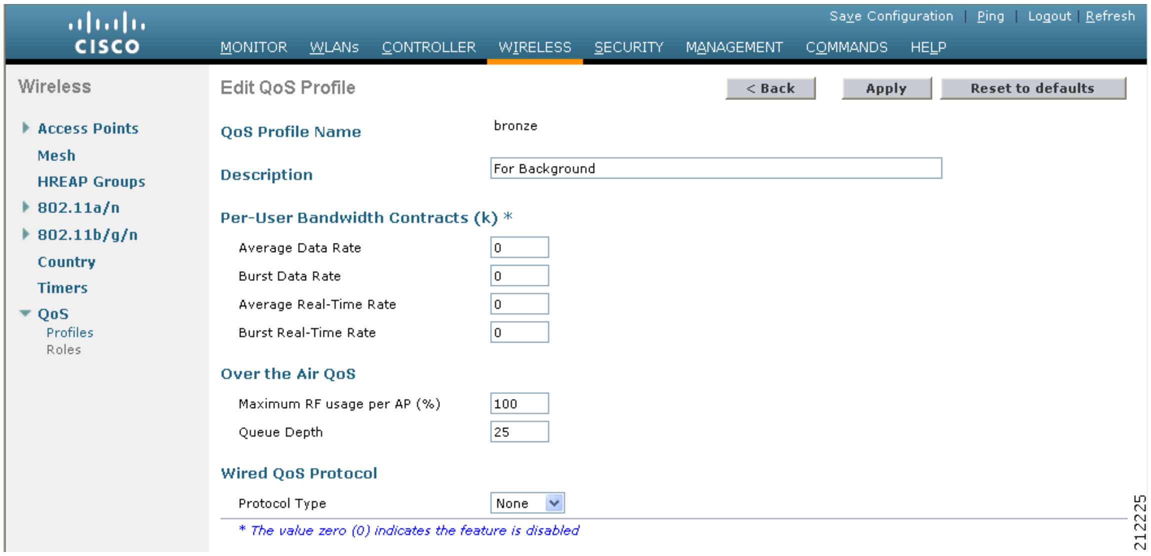
Step 1 Disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles.

To disable the radio networks, click **Wireless > 802.11a/n** or **802.11b/g/n > Network**, uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 2 Click **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 (see Figure 4-14).

Figure 4-14   Edit QoS Profile Page



Edit QoS Profile

QoS Profile Name	bronze
Description	For Background
Per-User Bandwidth Contracts (k) *	
Average Data Rate	0
Burst Data Rate	0
Average Real-Time Rate	0
Burst Real-Time Rate	0
Over the Air QoS	
Maximum RF usage per AP (%)	100
Queue Depth	25
Wired QoS Protocol	
Protocol Type	None

** The value zero (0) indicates the feature is disabled*

Step 4 To change the description of the profile, modify the contents of the Description field.

Step 5 To define the average data rate for TCP traffic per user, enter the rate in Kbps in the Average Data Rate field. 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 To define the peak data rate for TCP traffic per user, enter the rate in Kbps in the Burst Data Rate field. 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 To define the average real-time rate for UDP traffic on a per user basis, enter the rate in Kbps in the Average Real-Time Rate field. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the profile.

Step 8 To define the peak real-time rate for UDP traffic on a per user basis, enter the rate in Kbps in the Burst Real-Time Rate field. 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.

Step 9 In the Maximum RF Usage Per AP field, enter the maximum percentage of bandwidth given to a user class.

For example, if you set 50% for Bronze QoS, all the Bronze WLAN users combined will not get more than 50% of the available RF bandwidth. Actual throughput could be less than 50%, but it will never be more than 50%.

Step 10 In the Queue Depth field, enter the maximum number of packets that access points keep in their queues. Any additional packets are dropped.

Step 11 To define the maximum value (0–7) for the priority tag associated with packets that fall within the profile, choose **802.1p** from the Protocol Type drop-down box and enter the maximum priority value in the 802.1p Tag field.

The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network.

Step 12 Click **Apply** to commit your changes.

Step 13 Click **Save Configuration** to save your changes.

Step 14 Re-enable the 802.11a and 802.11b/g networks.

To enable the radio networks, click **Wireless > 802.11a/n** or **802.11b/g/n > Network**, check the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 15 Follow the instructions in the "Assigning a QoS Profile to a WLAN" section on page 6-30 to assign a QoS profile to a WLAN.

Using the CLI to Configure QoS Profiles

Follow these steps to configure the Platinum, Gold, Silver, and Bronze QoS profiles using the CLI.

Step 1 To disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles, enter these commands:

config 802.11a disable network

config 802.11b disable network

Step 2 To change the profile description, enter this command:

config qos description {bronze | silver | gold | platinum} *description*

Step 3 To define the average data rate in Kbps for TCP traffic per user, enter this command:

config qos average-data-rate {bronze | silver | gold | platinum} *rate*

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 To define the peak data rate in Kbps for TCP traffic per user, enter this command:

config qos burst-data-rate {bronze | silver | gold | platinum} *rate*

Step 5 To define the average real-time rate in Kbps for UDP traffic per user, enter this command:

config qos average-realtime-rate {bronze | silver | gold | platinum} *rate*

Step 6 To define the peak real-time rate in Kbps for UDP traffic per user, enter this command:

config qos burst-realtime-rate {bronze | silver | gold | platinum} *rate*

Step 7 To specify the maximum percentage of RF usage per access point, enter this command:

config qos max-rf-usage {bronze | silver | gold | platinum} *usage_percentage*

Step 8 To specify the maximum number of packets that access points keep in their queues, enter this command:

config qos queue_length {bronze | silver | gold | platinum} *queue_length*

Step 9 To define the maximum value (0–7) for the priority tag associated with packets that fall within the profile, enter these commands:

config qos protocol-type {bronze | silver | gold | platinum} dot1p

config qos dot1p-tag {bronze | silver | gold | platinum} *tag*

Step 10 To re-enable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles, enter these commands:

config 802.11a enable network

config 802.11b enable network

Step 11 Follow the instructions in the "Assigning a QoS Profile to a WLAN" section on page 6-30 to assign a QoS profile to a WLAN.

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 use the controller GUI or CLI to configure up to ten QoS roles for guest users.

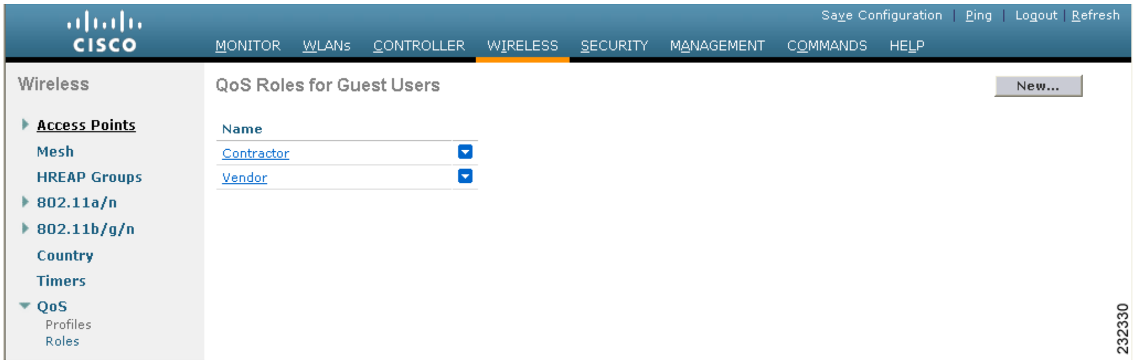
Note If you choose to create an entry on the RADIUS server for a guest user and enable RADIUS authentication for the WLAN on which web authentication is performed rather than adding a guest user to the local user database from the controller, you need to assign the QoS role on the RADIUS server itself. 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.

Using the GUI to Configure QoS Roles

Follow these steps to configure QoS roles using the controller GUI.

Step 1 Click **Wireless** > **QoS > Roles** to open the QoS Roles for Guest Users page (see Figure 4-15).

Figure 4-15 QoS Roles for Guest Users Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Wireless
Access Points
Mesh
HREAP Groups
802.11a/n
802.11b/g/n
Country
Timers
QoS
Profiles
Roles
New...
232330

QoS Roles for Guest Users

Name
Contractor
Vendor

This page shows any existing QoS roles for guest users.

Note If you want to delete a QoS role, hover your cursor over the blue drop-down arrow for that role and choose **Remove**.

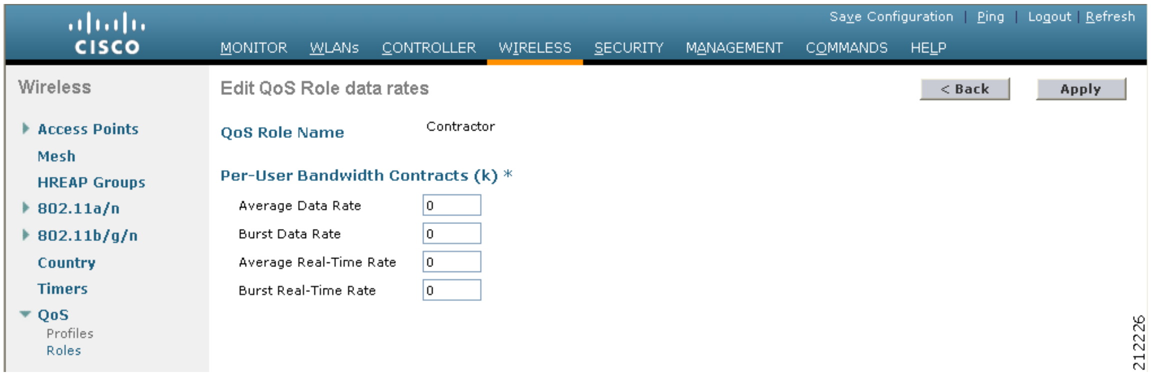
Step 2 To create a new QoS role, click **New**. The QoS Role Name > New page appears.

Step 3 In the Role Name field, 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 To edit the bandwidth of a QoS role, click the name of the QoS role. The Edit QoS Role Data Rates page appears (see Figure 4-16).

Figure 4-16 Edit QoS Role Data Rates Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Wireless
Access Points
Mesh
HREAP Groups
802.11a/n
802.11b/g/n
Country
Timers
QoS
Profiles
Roles
< Back
Apply
212226

Edit QoS Role data rates

QoS Role Name Contractor

Per-User Bandwidth Contracts (k) *

Average Data Rate 0
Burst Data Rate 0
Average Real-Time Rate 0
Burst Real-Time Rate 0

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 To define the average data rate for TCP traffic on a per user basis, enter the rate in Kbps in the Average Data Rate field. 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 To define the peak data rate for TCP traffic on a per user basis, enter the rate in Kbps in the Burst Data Rate field. 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 To define the average real-time rate for UDP traffic on a per user basis, enter the rate in Kbps in the Average Real-Time Rate field. 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 To define the peak real-time rate for UDP traffic on a per user basis, enter the rate in Kbps in the Burst Real-Time Rate field. 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 To apply a QoS role to a guest user, follow the steps in the "Using the GUI to Configure Local Network Users" section on page 5-30.

Using the CLI to Configure QoS Roles

Follow these steps to configure QoS roles using the controller CLI.

Step 1 To create a QoS role for a guest user, enter this command:

config netuser guest-role create *role_name*

Note If you want to delete a QoS role, enter this command:
config netuser guest-role delete *role_name*

Step 2 To configure the bandwidth contracts for a QoS role, enter 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 To apply a QoS role to a guest user, enter 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 field 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 this command: **config netuser guest-role apply** *username* **default**. This user now uses the bandwidth contracts defined in the QoS profile for the WLAN.

Step 4 To save your changes, enter this command:

save config

Step 5 To see a list of the current QoS roles and their bandwidth parameters, enter 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

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 Cisco Client Extensions" section on page 6-39 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.

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 4-32 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 co-located 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 over-subscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

Note 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 4-2 for examples of TSPEC request handling for normal TSPEC requests and expedited bandwidth requests.

Table 4-2 TSPEC Request Handling Examples

CAC Mode	Reserved bandwidth for voice calls[1]	Usage[2]	Normal TSPEC Request	TSPEC with Expedited Bandwidth Request
Bandwidth-based CAC	75% (default setting)	Less than 75%	Admitted	Admitted
		Between 75% and 90% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 90%	Rejected	Rejected
Load-based CAC		Less than 75%	Admitted	Admitted
		Between 75% and 85% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 85%	Rejected	Rejected

[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 When video ACM is enabled, the controller rejects a video TSPEC if the Nom-MSDU size in the TSPEC is greater than 149 or the mean data rate is greater than 1 Kb/s.

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. An administrator 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. 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 in both local and hybrid-REAP modes.

Using the GUI to Configure Voice Parameters

Follow these steps to configure voice parameters using the GUI.

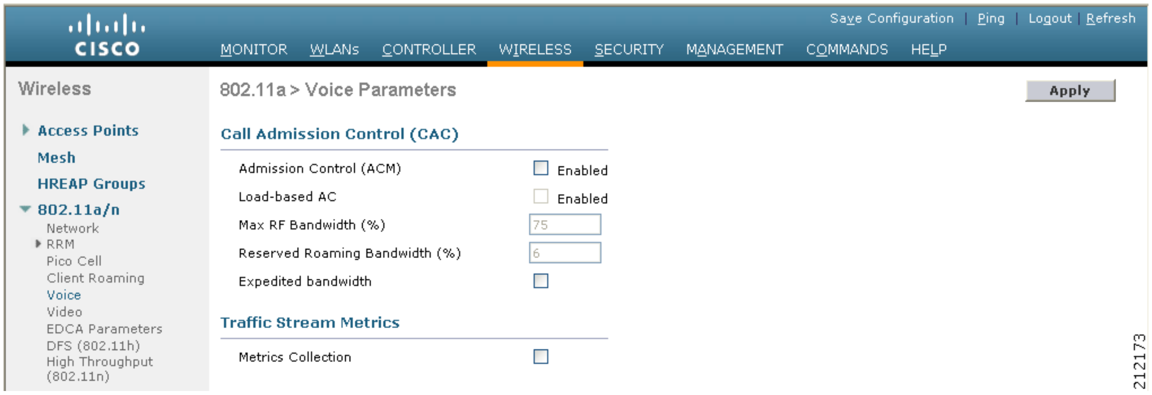
Step 1 Make sure that the WLAN is configured for WMM and the Platinum QoS level.

Step 2 Disable all WLANs with WMM enabled and click **Apply**.

Step 3 To disable the radio network, click **Wireless** and then **Network** under 802.11a/n or 802.11b/g/n, uncheck the 802.11a (or 802.11b/g) Network Status check box, and click **Apply**.

Step 4 Click **Voice** under 802.11a/n or 802.11b/g/n. The 802.11a (or 802.11b) > Voice Parameters page appears (see Figure 4-17).

Figure 4-17 802.11a > Voice Parameters Page



802.11a > Voice Parameters

Call Admission Control (CAC)

Admission Control (ACM)	□ Enabled
Load-based AC	□ Enabled
Max RF Bandwidth (%)	75
Reserved Roaming Bandwidth (%)	6
Expedited bandwidth	□

Traffic Stream Metrics

Metrics Collection	□

Step 5 To enable bandwidth-based CAC for this radio band, check the **Admission Control (ACM)** check box. The default value is disabled.

Step 6 To enable load-based CAC for this radio band, check both the **Admission Control (ACM)** check box and the **Load-based AC** check box. The default value for both check boxes is disabled.

Step 7 In the Max RF Bandwidth field, 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.

Range: 40 to 85%

Default: 75%

Step 8 In the Reserved Roaming Bandwidth field, enter the percentage of maximum allocated bandwidth reserved for roaming voice clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients.

Range: 0 to 25%

Default: 6%

Step 9 To enable expedited bandwidth requests, check the **Expedited Bandwidth** check box. The default value is disabled.

Step 10 To enable TSM, check the **Metrics Collection** check box. The default value is disabled.

Step 11 Click **Apply** to commit your changes.

Step 12 Re-enable all WMM WLANs and click **Apply**.

Step 13 To re-enable the radio network, click **Network** under 802.11a/n or 802.11b/g/n, check the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 14 Click **Save Configuration** to save your changes.

Step 15 Repeat this procedure if you want to configure voice parameters for another radio band (802.11a or 802.11b/g).

Using the GUI to Configure Video Parameters

Follow these steps to configure video parameters using the GUI.

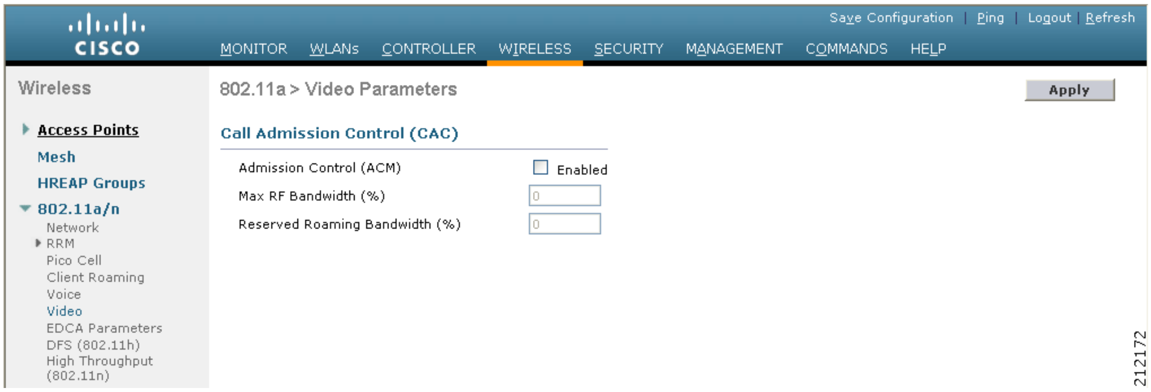
Step 1 Make sure that the WLAN is configured for WMM and the Gold QoS level.

Step 2 Disable all WLANs with WMM enabled and click **Apply**.

Step 3 To disable the radio network, click **Wireless** and then **Network** under 802.11a/n or 802.11b/g/n, uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 4 Click **Video** under 802.11a/n or 802.11b/g/n. The 802.11a (or 802.11b) > Video Parameters page appears (see Figure 4-17).

Figure 4-18 802.11a > Video Parameters Page



802.11a > Video Parameters

Call Admission Control (CAC)

Admission Control (ACM) □ Enabled

Max RF Bandwidth (%) 0

Reserved Roaming Bandwidth (%) 0

Step 5 To enable video CAC for this radio band, check the **Admission Control (ACM)** check box. The default value is disabled.

Step 6 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.

Range: 0 to 100% (However, the maximum RF bandwidth cannot exceed 100% for voice + video.)

Default: 0%

Note If this parameter is set to zero (0), the controller assumes that the operator does not want to do any bandwidth allocation and, therefore, allows all bandwidth requests.

Step 7 In the Reserved Roaming Bandwidth field, enter the percentage of maximum allocated bandwidth reserved for roaming video clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming video clients.

Range: 0 to 25%

Default: 0%

Step 8 Click **Apply** to commit your changes.

Step 9 Re-enable all WMM WLANs and click **Apply**.

Step 10 To re-enable the radio network, click **Network** under 802.11a/n or 802.11b/g/n, check the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 11 Click **Save Configuration** to save your changes.

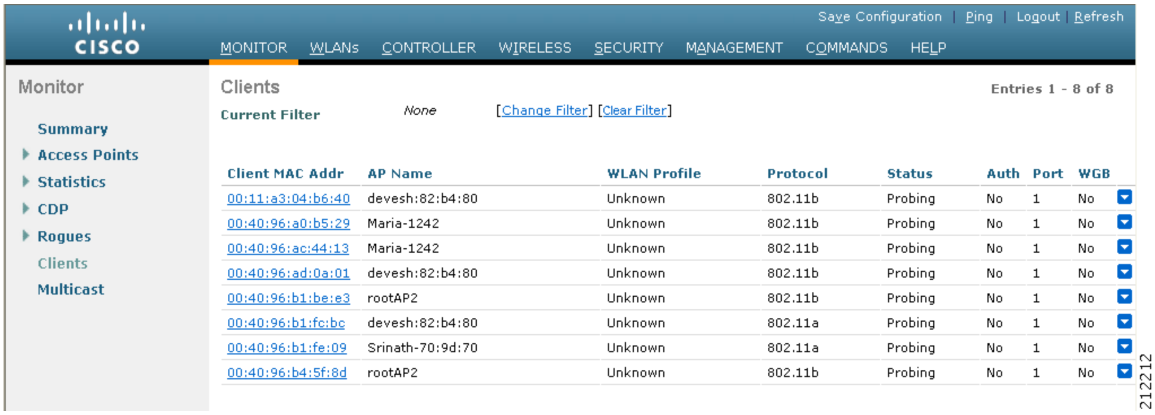
Step 12 Repeat this procedure if you want to configure video parameters for another radio band (802.11a or 802.11b/g).

Using the GUI to View Voice and Video Settings

Follow these steps to view voice and video settings using the GUI.

Step 1 Click **Monitor > Clients** to open the Clients page (see Figure 4-19).

Figure 4-19 Clients Page



Clients

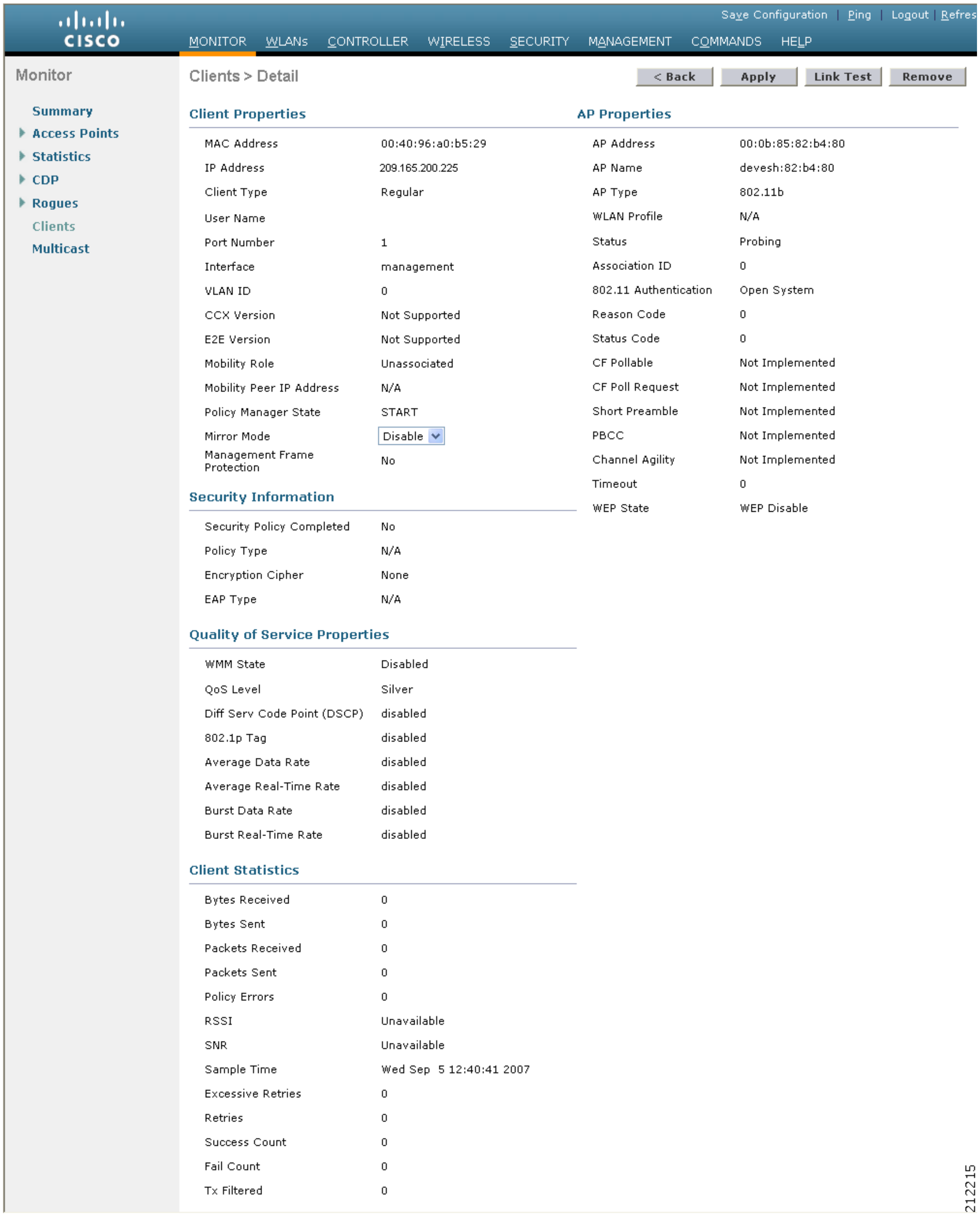
Entries 1 - 8 of 8

Current Filter *None* [Change Filter] [Clear Filter]

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:11:a3:04:b6:40	devesh:82:b4:80	Unknown	802.11b	Probing	No	1	No
00:40:96:a0:b5:29	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:40:96:ac:44:13	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:40:96:ad:0a:01	devesh:82:b4:80	Unknown	802.11b	Probing	No	1	No
00:40:96:b1:be:e3	rootAP2	Unknown	802.11b	Probing	No	1	No
00:40:96:b1:fc:bc	devesh:82:b4:80	Unknown	802.11a	Probing	No	1	No
00:40:96:b1:fe:09	Srinath-70:9d:70	Unknown	802.11a	Probing	No	1	No
00:40:96:b4:5f:8d	rootAP2	Unknown	802.11b	Probing	No	1	No

Step 2 Click the MAC address of the desired client to open the Clients > Detail page (see Figure 4-20).

Figure 4-20   Clients > Detail Page


Save Configuration | Ping | Logout | Refres
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Access Points
Statistics
CDP
Rogues
Clients
Multicast
Clients > Detail
< Back
Apply
Link Test
Remove
212215

Client Properties

MAC Address	00:40:96:a0:b5:29
IP Address	209.165.200.225
Client Type	Regular
User Name	
Port Number	1
Interface	management
VLAN ID	0
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Unassociated
Mobility Peer IP Address	N/A
Policy Manager State	START
Mirror Mode	Disable
Management Frame Protection	No

AP Properties

AP Address	00:0b:85:82:b4:80
AP Name	devesh:82:b4:80
AP Type	802.11b
WLAN Profile	N/A
Status	Probing
Association ID	0
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Disable

Security Information

Security Policy Completed	No
Policy Type	N/A
Encryption Cipher	None
EAP Type	N/A

Quality of Service Properties

WMM State	Disabled
QoS Level	Silver
Diff Serv Code Point (DSCP)	disabled
802.1p Tag	disabled
Average Data Rate	disabled
Average Real-Time Rate	disabled
Burst Data Rate	disabled
Burst Real-Time Rate	disabled

Client Statistics

Bytes Received	0
Bytes Sent	0
Packets Received	0
Packets Sent	0
Policy Errors	0
RSSI	Unavailable
SNR	Unavailable
Sample Time	Wed Sep 5 12:40:41 2007
Excessive Retries	0
Retries	0
Success Count	0
Fail Count	0
Tx Filtered	0

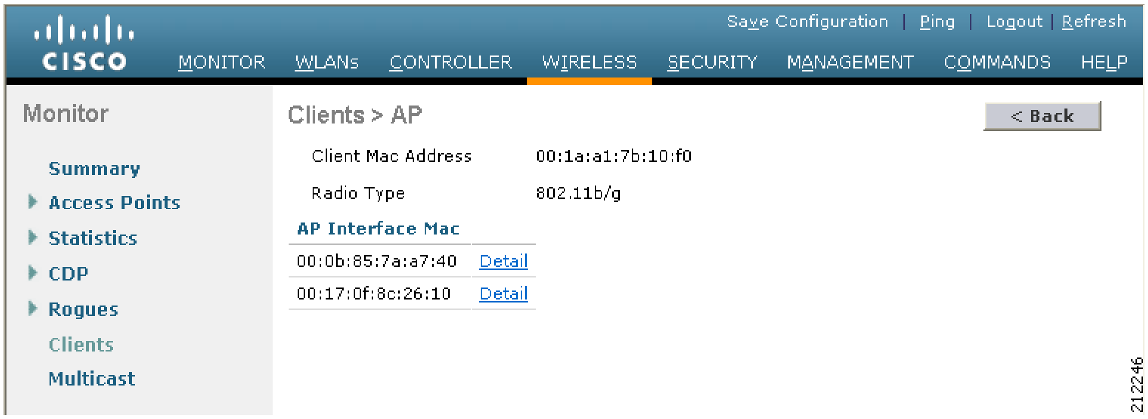
This page shows the U-APSD status (if enabled) for this client under Quality of Service Properties.

Step 3 Click **Back** to return to the Clients page.

Step 4 Follow these steps to see the TSM statistics for a particular client and the access point to which this client is associated.

a. Hover your cursor over the blue drop-down arrow for the desired client and choose **802.11aTSM** or **802.11b/gTSM**. The Clients > AP page appears (see Figure 4-21).

Figure 4-21 Clients > AP Page


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Access Points
Statistics
CDP
Rogues
Clients
Multicast
< Back
212246

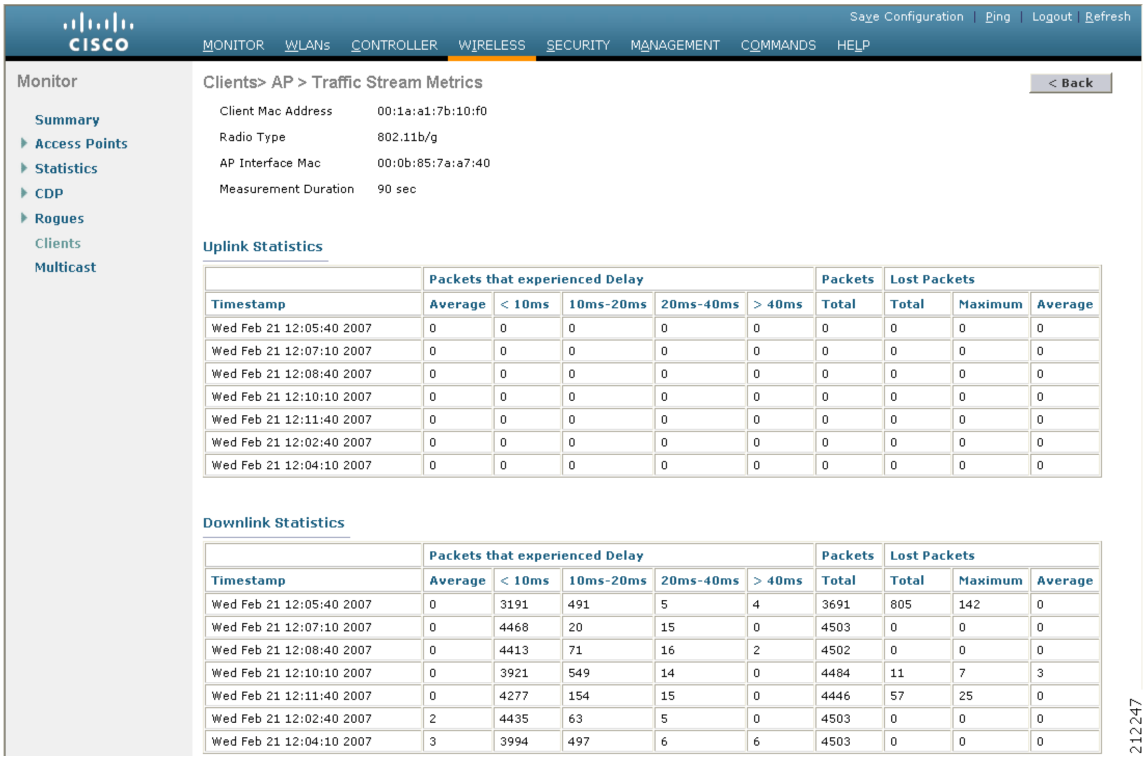
Clients > AP

Client Mac Address	00:1a:a1:7b:10:f0
Radio Type	802.11b/g

AP Interface Mac	
00:0b:85:7a:a7:40	Detail
00:17:0f:8c:26:10	Detail

b. Click the **Detail** link for the desired access point to open the Clients > AP > Traffic Stream Metrics page (see Figure 4-22).

Figure 4-22 Clients > AP > Traffic Stream Metrics Page


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Access Points
Statistics
CDP
Rogues
Clients
Multicast
< Back
212247

Clients> AP > Traffic Stream Metrics

Client Mac Address	00:1a:a1:7b:10:f0
Radio Type	802.11b/g
AP Interface Mac	00:0b:85:7a:a7:40
Measurement Duration	90 sec

Uplink Statistics

	Packets that experienced Delay					Packets	Lost Packets		
Timestamp	Average	< 10ms	10ms-20ms	20ms-40ms	> 40ms	Total	Total	Maximum	Average
Wed Feb 21 12:05:40 2007	0	0	0	0	0	0	0	0	0
Wed Feb 21 12:07:10 2007	0	0	0	0	0	0	0	0	0
Wed Feb 21 12:08:40 2007	0	0	0	0	0	0	0	0	0
Wed Feb 21 12:10:10 2007	0	0	0	0	0	0	0	0	0
Wed Feb 21 12:11:40 2007	0	0	0	0	0	0	0	0	0
Wed Feb 21 12:02:40 2007	0	0	0	0	0	0	0	0	0
Wed Feb 21 12:04:10 2007	0	0	0	0	0	0	0	0	0

Downlink Statistics

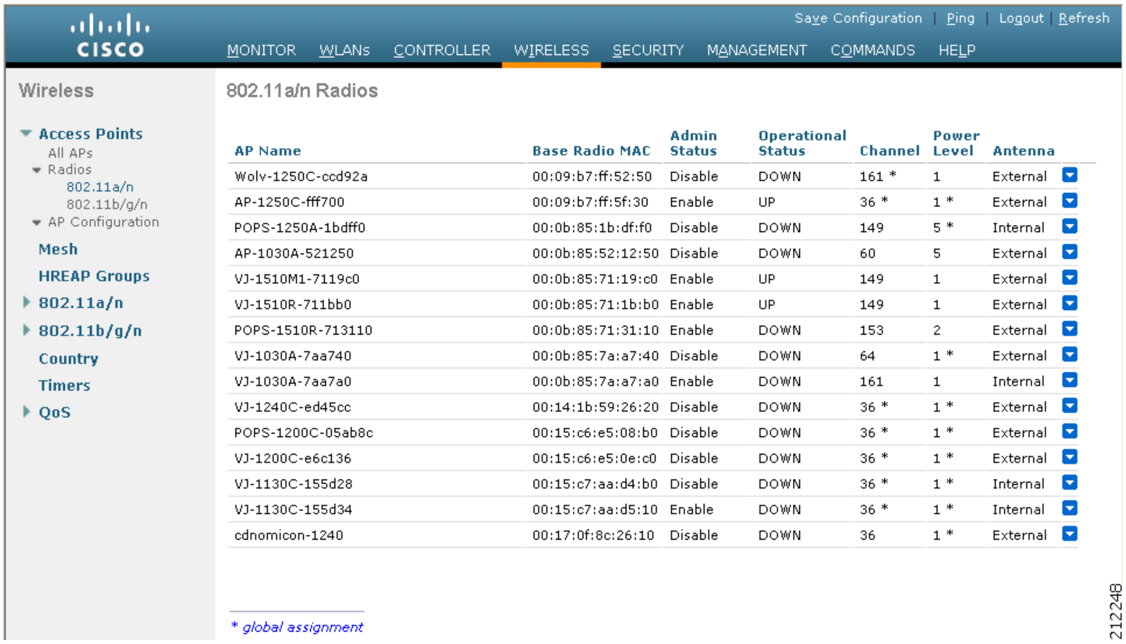
	Packets that experienced Delay					Packets	Lost Packets		
Timestamp	Average	< 10ms	10ms-20ms	20ms-40ms	> 40ms	Total	Total	Maximum	Average
Wed Feb 21 12:05:40 2007	0	3191	491	5	4	3691	805	142	0
Wed Feb 21 12:07:10 2007	0	4468	20	15	0	4503	0	0	0
Wed Feb 21 12:08:40 2007	0	4413	71	16	2	4502	0	0	0
Wed Feb 21 12:10:10 2007	0	3921	549	14	0	4484	11	7	3
Wed Feb 21 12:11:40 2007	0	4277	154	15	0	4446	57	25	0
Wed Feb 21 12:02:40 2007	2	4435	63	5	0	4503	0	0	0
Wed Feb 21 12:04:10 2007	3	3994	497	6	6	4503	0	0	0

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 field shows the specific interval when the statistics were collected.

Step 5 Follow these steps to see the TSM statistics for a particular access point and a particular client associated to this access point.

a. Click **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 (see Figure 4-23).

Figure 4-23 802.11a/n Radios Page



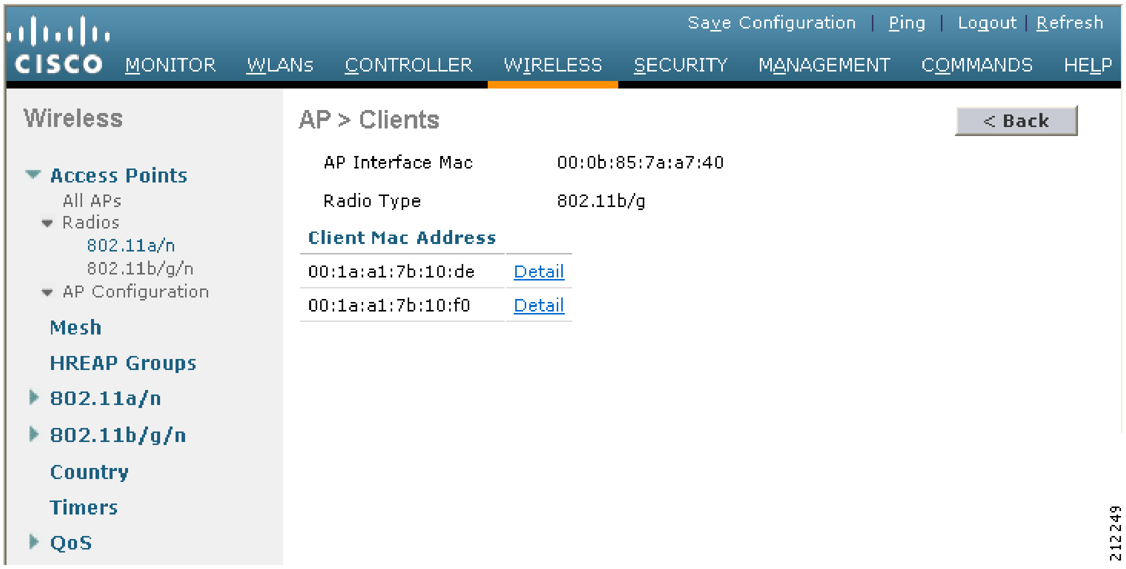
802.11a/n Radios

AP Name	Base Radio MAC	Admin Status	Operational Status	Channel	Power Level	Antenna	
Wolv-1250C-ccd92a	00:09:b7:ff:52:50	Disable	DOWN	161 *	1	External	▼
AP-1250C-fff700	00:09:b7:ff:5f:30	Enable	UP	36 *	1 *	External	▼
POPS-1250A-1bdff0	00:0b:85:1b:df:f0	Disable	DOWN	149	5 *	Internal	▼
AP-1030A-521250	00:0b:85:52:12:50	Disable	DOWN	60	5	External	▼
VJ-1510M1-7119c0	00:0b:85:71:19:c0	Enable	UP	149	1	External	▼
VJ-1510R-711bb0	00:0b:85:71:1b:b0	Enable	UP	149	1	External	▼
POPS-1510R-713110	00:0b:85:71:31:10	Enable	DOWN	153	2	External	▼
VJ-1030A-7aa740	00:0b:85:7a:a7:40	Disable	DOWN	64	1 *	External	▼
VJ-1030A-7aa7a0	00:0b:85:7a:a7:a0	Enable	DOWN	161	1	Internal	▼
VJ-1240C-ed45cc	00:14:1b:59:26:20	Disable	DOWN	36 *	1 *	External	▼
POPS-1200C-05ab8c	00:15:c6:e5:08:b0	Disable	DOWN	36 *	1 *	External	▼
VJ-1200C-e6c136	00:15:c6:e5:0e:c0	Disable	DOWN	36 *	1 *	External	▼
VJ-1130C-155d28	00:15:c7:aa:d4:b0	Disable	DOWN	36 *	1 *	Internal	▼
VJ-1130C-155d34	00:15:c7:aa:d5:10	Enable	DOWN	36 *	1 *	Internal	▼
cdnomicon-1240	00:17:0f:8c:26:10	Disable	DOWN	36	1 *	External	▼

* global assignment

b. Hover your cursor over the blue drop-down arrow for the desired access point and choose **802.11aTSM** or **802.11b/gTSM**. The AP > Clients page appears (see Figure 4-24).

Figure 4-24 AP > Clients Page



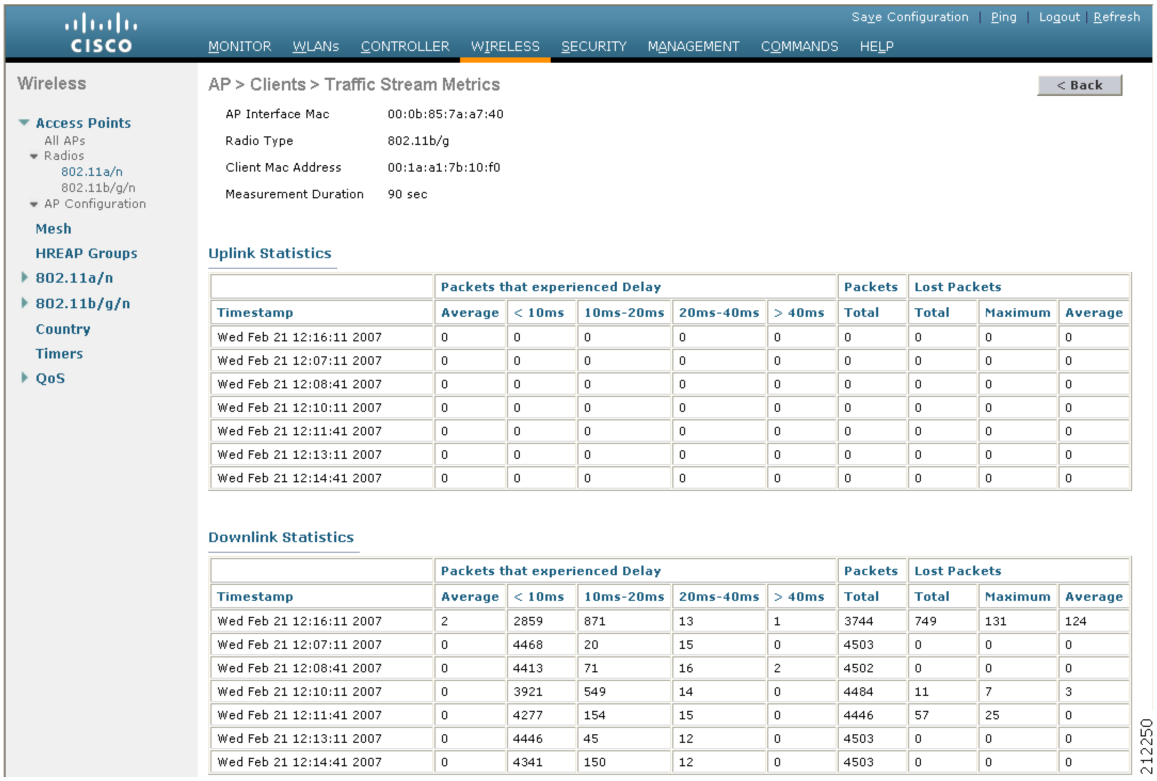
AP > Clients

AP Interface Mac	00:0b:85:7a:a7:40
Radio Type	802.11b/g

Client Mac Address	
00:1a:a1:7b:10:de	Detail
00:1a:a1:7b:10:f0	Detail

c. Click the **Detail** link for the desired client to open the AP > Clients > Traffic Stream Metrics page (see Figure 4-25).

Figure 4-25 AP > Clients > Traffic Stream Metrics Page



AP > Clients > Traffic Stream Metrics

AP Interface Mac	00:0b:85:7a:a7:40
Radio Type	802.11b/g
Client Mac Address	00:1a:a1:7b:10:f0
Measurement Duration	90 sec

Uplink Statistics

	Packets that experienced Delay					Packets	Lost Packets		
Timestamp	Average	< 10ms	10ms-20ms	20ms-40ms	> 40ms	Total	Total	Maximum	Average
Wed Feb 21 12:16:11 2007	0	0	0	0	0	0	0	0	0
Wed Feb 21 12:07:11 2007	0	0	0	0	0	0	0	0	0
Wed Feb 21 12:08:41 2007	0	0	0	0	0	0	0	0	0
Wed Feb 21 12:10:11 2007	0	0	0	0	0	0	0	0	0
Wed Feb 21 12:11:41 2007	0	0	0	0	0	0	0	0	0
Wed Feb 21 12:13:11 2007	0	0	0	0	0	0	0	0	0
Wed Feb 21 12:14:41 2007	0	0	0	0	0	0	0	0	0

Downlink Statistics

	Packets that experienced Delay					Packets	Lost Packets		
Timestamp	Average	< 10ms	10ms-20ms	20ms-40ms	> 40ms	Total	Total	Maximum	Average
Wed Feb 21 12:16:11 2007	2	2859	871	13	1	3744	749	131	124
Wed Feb 21 12:07:11 2007	0	4468	20	15	0	4503	0	0	0
Wed Feb 21 12:08:41 2007	0	4413	71	16	2	4502	0	0	0
Wed Feb 21 12:10:11 2007	0	3921	549	14	0	4484	11	7	3
Wed Feb 21 12:11:41 2007	0	4277	154	15	0	4446	57	25	0
Wed Feb 21 12:13:11 2007	0	4446	45	12	0	4503	0	0	0
Wed Feb 21 12:14:41 2007	0	4341	150	12	0	4503	0	0	0

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 field shows the specific interval when the statistics were collected.

Using the CLI to Configure Voice Parameters

Follow these steps to configure voice parameters using the CLI.

Step 1 To see all of the WLANs configured on the controller, enter this command:

show wlan summary

Step 2 To make sure that the WLAN you are planning to modify is configured for WMM and the QoS level is set to Platinum, enter this command:

show wlan *wlan_id*

Step 3 To disable all WLANs with WMM enabled prior to changing the voice parameters, enter this command:

config wlan disable *wlan_id*

Step 4 To disable the radio network, enter this command:

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

Step 5 To save your settings, enter this command:

save config

Step 6 To enable or disable bandwidth-based voice CAC for the 802.11a or 802.11b/g network, enter this command:

config {**802.11a** | **802.11b**} **cac voice acm** {**enable** | **disable**}

Step 7 To set the percentage of maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network, enter this command:

config {**802.11a** | **802.11b**} **cac voice max-bandwidth** *bandwidth*

The *bandwidth* range is 40 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 To set the percentage of maximum allocated bandwidth reserved for roaming voice clients, enter 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 To process or ignore the TSPEC inactivity timeout received from an access point, enter this command:

config {**802.11a** | **802.11b**} **cac voice tspec-inactivity-timeout** {**enable** | **ignore**}

Step 10 To enable or disable load-based CAC for the 802.11a or 802.11b/g network, enter this command:

config {**802.11a** | **802.11b**} **cac voice load-based** {**enable** | **disable**}

Step 11 To configure the number of aggregated voice WMM traffic specification (TSPEC) streams at a specified data rate for the 802.11a or 802.11b/g network, enter this command:

config {**802.11a** | **802.11b**} **cac voice stream-size** *number* **max-streams** *mean_datarate*

The *number* range is 1 to 5 voice streams, and the default value is 2. The *mean_datarate* range is 84 to 91.2 Kbps, and the default value is 84 Kbps.

Step 12 To enable or disable expedited bandwidth requests for the 802.11a or 802.11b/g network, enter this command:

config {**802.11a** | **802.11b**} **exp-bwreq** {**enable** | **disable**}

Step 13 To enable or disable TSM for the 802.11a or 802.11b/g network, enter this command:

config {**802.11a** | **802.11b**} **tsm** {**enable** | **disable**}

Step 14 To re-enable all WLANs with WMM enabled, enter this command:

config wlan enable *wlan_id*

Step 15 To re-enable the radio network, enter this command:

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

Step 16 To save your settings, enter this command:

save config

Using the CLI to Configure Video Parameters

Follow these steps to configure video parameters using the CLI.

Step 1 To see all of the WLANs configured on the controller, enter this command:

show wlan summary

Step 2 To make sure that the WLAN you are planning to modify is configured for WMM and the QoS level is set to Gold, enter this command:

show wlan *wlan_id*

Step 3 To disable all WLANs with WMM enabled prior to changing the video parameters, enter this command:

config wlan disable *wlan_id*

Step 4 To disable the radio network, enter this command:

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

Step 5 To save your settings, enter this command:

save config

Step 6 To enable or disable video CAC for the 802.11a or 802.11b/g network, enter this command:

config {**802.11a** | **802.11b**} **cac video acm** {**enable** | **disable**}

Step 7 To set the percentage of maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network, enter this command:

config {**802.11a | 802.11b**} **cac video max-bandwidth** *bandwidth*

The *bandwidth* range is 0 to 100%, and the default value is 0%. However, the maximum RF bandwidth cannot exceed 100% for voice + video. Once the client reaches the value specified, the access point rejects new calls on this network.

Note If this parameter is set to zero (0), the controller assumes that the operator does not want to do any bandwidth allocation and, therefore, allows all bandwidth requests.

Step 8 To set the percentage of maximum allocated bandwidth reserved for roaming video clients, enter this command:

config {**802.11a | 802.11b**} **cac video roam-bandwidth** *bandwidth*

The *bandwidth* range is 0 to 25%, and the default value is 0%. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming video clients.

Step 9 To process or ignore the TSPEC inactivity timeout received from an access point, enter this command:

config {**802.11a | 802.11b**} **cac video tspec-inactivity-timeout** {**enable | ignore**}

Step 10 To re-enable all WLANs with WMM enabled, enter this command:

config wlan enable *wlan_id*

Step 11 To re-enable the radio network, enter this command:

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

Step 12 To save your settings, enter this command:

save config

Using the CLI to View Voice and Video Settings

Use these commands to view voice and video settings using the CLI.

1. To see the CAC configuration for the 802.11a or 802.11b/g network, enter this command:

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

2. To see the CAC statistics for a particular access point, enter 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.

3. To see the U-APSD status for a particular client, enter this command:

   show client detail *client_mac*

4. To see the TSM statistics for a particular client and the access point to which this client is associated, enter this command:

   show client tsm {**802.11a** | **802.11b**} *client_mac* [*ap_ma*c | **all**]

   The optional **all** command shows all access points to which this client has associated. 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(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 field shows the specific interval when the statistics were collected.

5. To see the TSM statistics for a particular access point and a particular client associated to this access point, enter 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(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 field shows the specific interval when the statistics were collected.

6. To enable or disable debugging for call admission control (CAC) messages, events, or packets, enter 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.

Configuring 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.

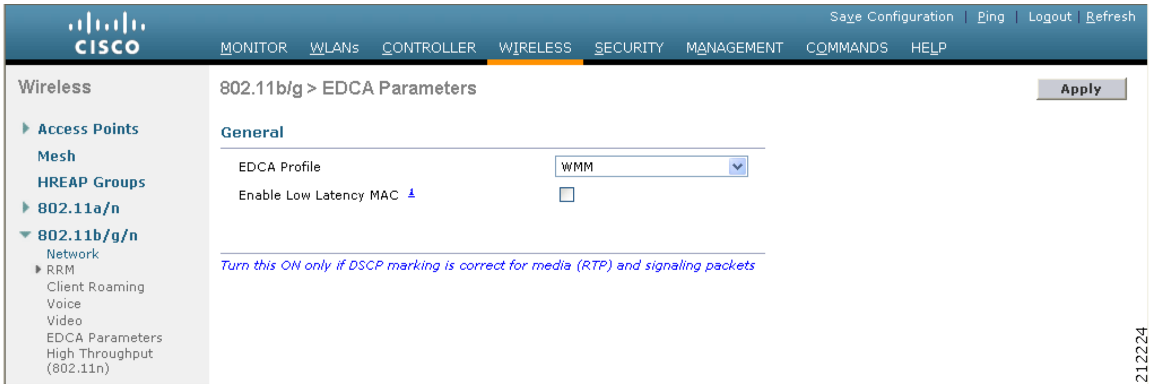
Using the GUI to Configure EDCA Parameters

Follow these steps to configure EDCA parameters using the controller GUI.

Step 1 To disable the radio network, click **Wireless** and then **Network** under 802.11a/n or 802.11b/g/n, uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 2 Click **EDCA Parameters** under 802.11a/n or 802.11b/g/n. The 802.11a (or 802.11b/g) > EDCA Parameters page appears (see Figure 4-26).

Figure 4-26 802.11a > EDCA Parameters Page



802.11b/g > EDCA Parameters

General

EDCA Profile: WMM

Enable Low Latency MAC [1] ☐

Turn this ON only if DSCP marking is correct for media (RTP) and signaling packets

Step 3 Choose one of the following options from the EDCA Profile drop-down box:

- **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.

Note If you deploy video services, admission control (ACM) must be disabled.

Step 4 If you want to enable MAC optimization for voice, check the **Enable Low Latency MAC** check box. Otherwise, leave this check box unchecked, which is the default value. This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, thereby improving the number of voice calls serviced per access point.

Note You should enable low latency MAC only if the WLAN allows WMM clients. If WMM is enabled, then low latency MAC can be used with any of the EDCA profiles. See the "Configuring QoS Enhanced BSS" section on page 6-32 for instructions on enabling WMM.

Caution We recommend that you not use the low latency MAC feature if you are using the 1140, 1250, 1260, and 3500 series access points that are based on the Marvell platform. If used, the data packets are retried at the data rate specified multiple times without downshifting the rates.

We also recommend that you not use the low latency MAC feature if you are using the 1120, 1130, 1230, and 1240 series access points (not based on the Marvell platform). If used, the number of retries is reduced to 3 with the first retry at the initial rate.

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

Step 6 To re-enable the radio network, click **Network** under 802.11a/n or 802.11b/g/n, check the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

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

Using the CLI to Configure EDCA Parameters

Follow these steps to configure EDCA parameters using the CLI.

Step 1 To disable the radio network, enter this command:

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

Step 2 To save your settings, enter this command:

save config

Step 3 To enable a specific EDCA profile, enter this command:

config advanced {**802.11a** | **802.11b**} **edca-parameters** *?*

where *?* is one of the following:

- **wmm-default**
- **svp-voice**
- **optimized-voice**
- **optimized-video-voice**

Note Refer to the "Using the GUI to Configure EDCA Parameters" section above for a description of each option.

Caution We recommend that you not use the low latency MAC feature if you are using the 1140, 1250, 1260, and 3500 series access points that are based on the Marvell platform. If used, the data packets are retried at the data rate specified multiple times without downshifting the rates.

We also recommend that you not use the low latency MAC feature if you are using the 1120, 1130, 1230, and 1240 series access points (not based on the Marvell platform). If used, the number of retries is reduced to 3 with the first retry at the initial rate.

Step 4 To view the current status of MAC optimization for voice, enter this command:

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

Information similar to the following appears:

```
Voice-mac-optimization..................Disabled
To enable or disable MAC optimization for voice, enter this command:
```

config advanced {**802.11a** | **802.11b**} **voice-mac-optimization** {**enable** | **disable**}

This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, thereby improving the number of voice calls serviced per access point. The default value is disabled.

Step 5 To re-enable the radio network, enter this command:

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

Step 6 To save your settings, enter this command:

save config

Configuring Cisco Discovery Protocol

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, thereby reducing down time.

CDPv1 and CDPv2 are supported on the following devices:

- 2100 and 4400 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 2100 series controller

This support enables network management applications to discover Cisco devices.

These 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.

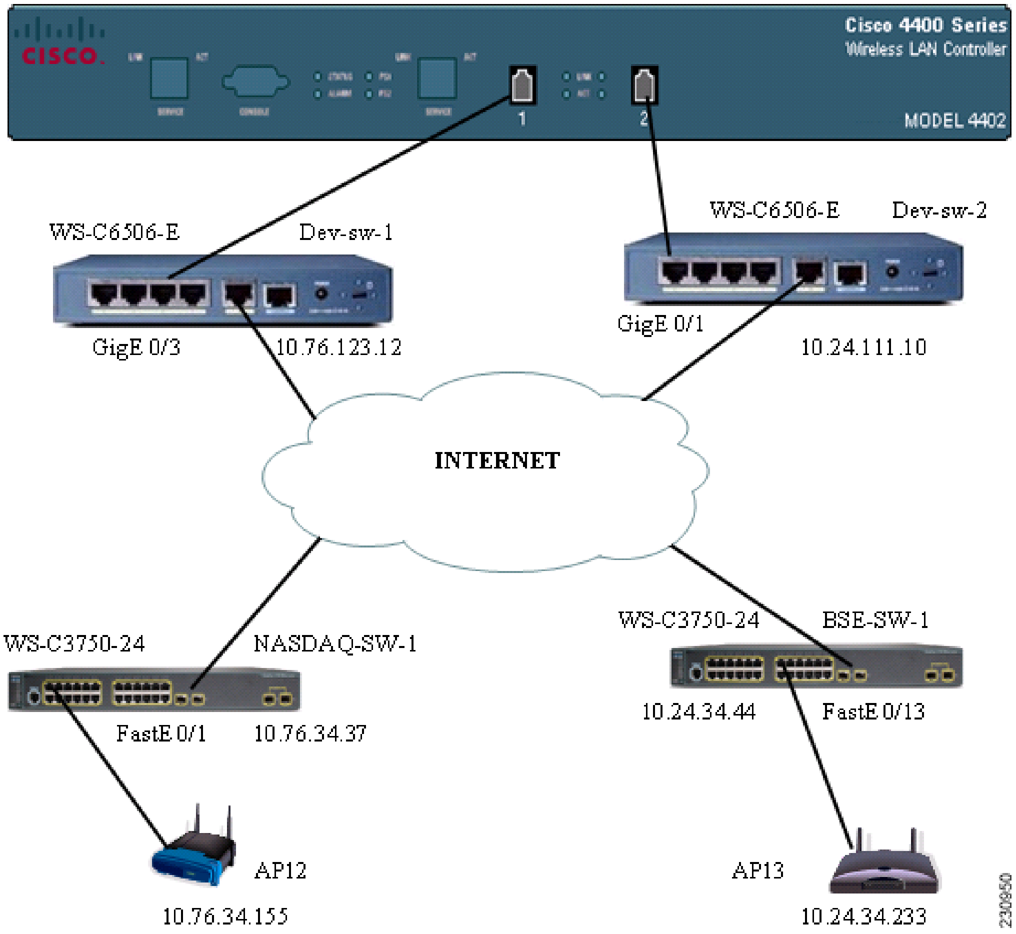
These TLVs are supported only by the access point:

- **Full/Half Duplex TLV: 0x000b**—The full- or half-duplex mode of the Ethernet link on which CDP packets are sent out. This TLV is not supported on access points that are connected directly to a 2100 series controller.
- **Power Consumption TLV: 0x0010**—The maximum amount of power consumed by the access point. This TLV is not supported on access points that are connected directly to a 2100 series controller.

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. Figure 4-27 shows a sample network that you can use as a reference when performing the procedures in this section.

Note Changing the CDP configuration on the controller does not change the CDP configuration on the access points connected to the controller. You must enable and disable CDP separately for each access point.

Figure 4-27 Sample Network Illustrating CDP

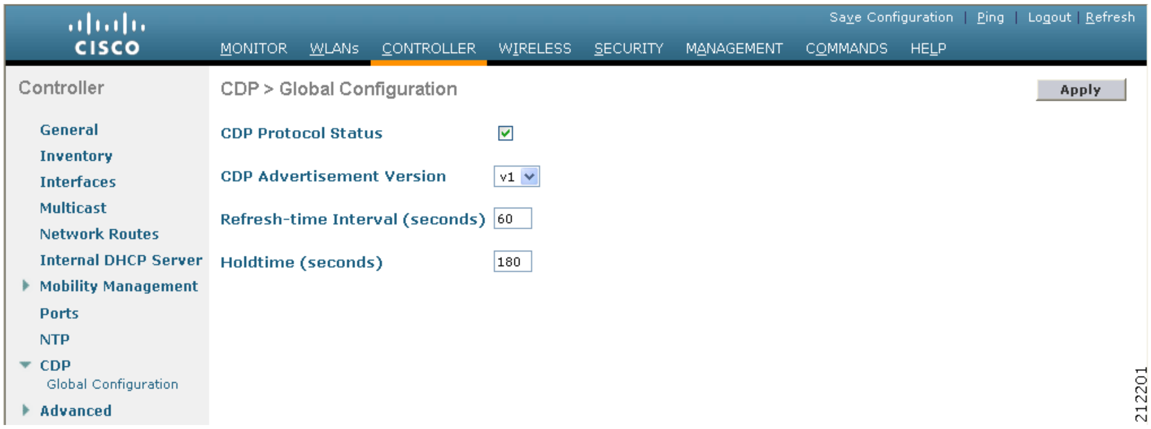


Using the GUI to Configure Cisco Discovery Protocol

Follow these steps to configure CDP using the controller GUI.

Step 1 Click **Controller** > **CDP** > **Global Configuration** to open the CDP > Global Configuration page (see Figure 4-28).

Figure 4-28 CDP > Global Configuration Page



CDP > Global Configuration

CDP Protocol Status ☑

CDP Advertisement Version v1

Refresh-time Interval (seconds) 60

Holdtime (seconds) 180

Step 2 Check the **CDP Protocol Status** check box to enable CDP on the controller or uncheck it to disable this feature. The default value is checked.

Step 3 From the CDP Advertisement Version drop-down box, 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 field, 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 field, 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:

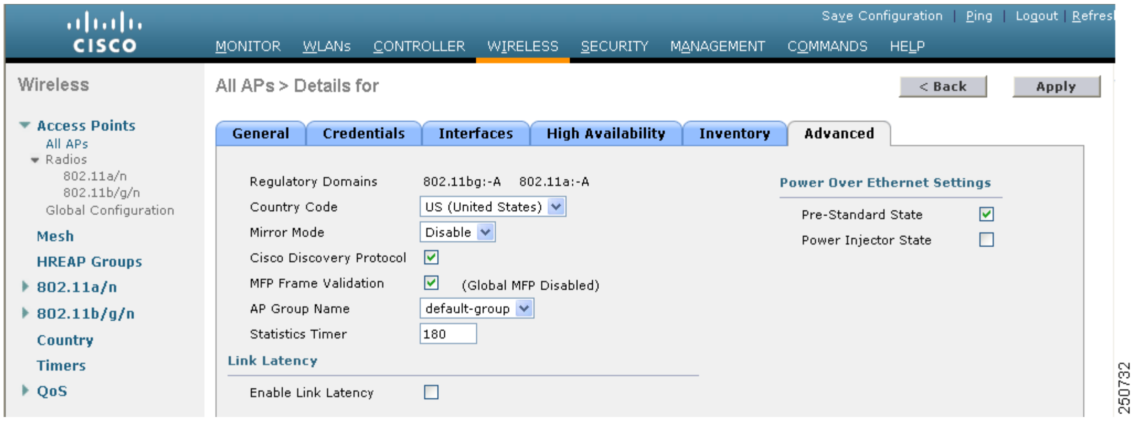
- To enable or disable CDP on a specific access point, follow these steps:

  a. Click **Wireless** > **Access Points** > **All APs** to open the All APs page.

  b. Click the link for the desired access point.

  c. Click the **Advanced** tab to open the All APs > Details for (Advanced) page (see Figure 4-29).

Figure 4-29 All APs > Details for (Advanced) Page



Regulatory Domains	802.11bg:-A 802.11a:-A
Country Code	US (United States)
Mirror Mode	Disable
Cisco Discovery Protocol	☑
MFP Frame Validation	☑ (Global MFP Disabled)
AP Group Name	default-group
Statistics Timer	180

Link Latency

Enable Link Latency	□

Power Over Ethernet Settings

Pre-Standard State	☑
Power Injector State	□

d. Check the **Cisco Discovery Protocol** check box to enable CDP on this access point or uncheck it to disable this feature. The default value is enabled.

e. Click **Apply** to commit your changes.

- To enable or disable CDP on all access points currently associated to the controller, follow these steps:

a. Click **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

b. Check the **CDP State** check box to enable CDP on all access points associated to the controller or uncheck it to disable CDP on all access points. The default value is checked.

c. Click **Apply** to commit your changes.

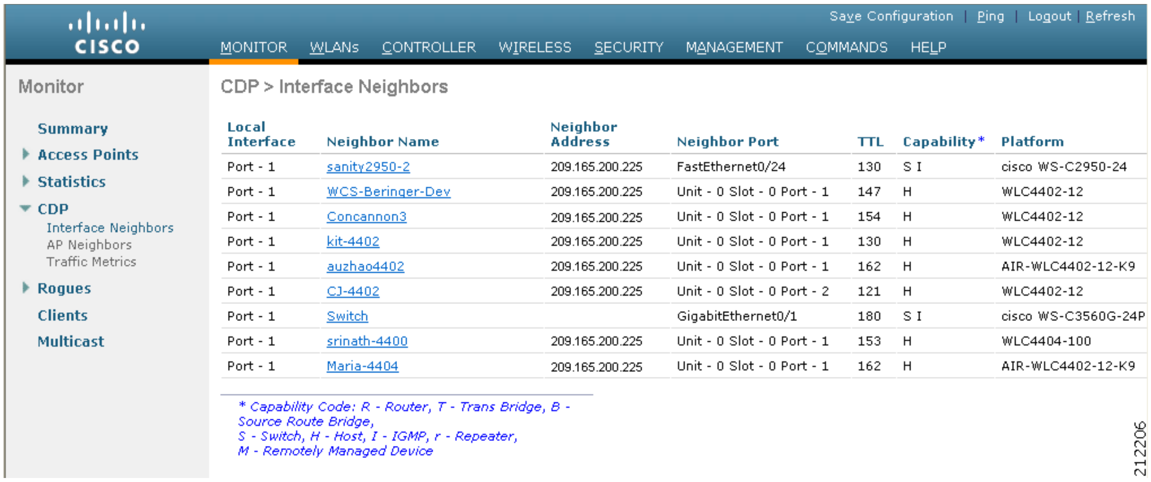
Step 9 Click **Save Configuration** to save your changes.

Using the GUI to View Cisco Discovery Protocol Information

Follow these steps to view CDP information using the controller GUI.

Step 1 To see a list of all CDP neighbors on all interfaces, click **Monitor** > **CDP** > **Interface Neighbors**. The CDP > Interface Neighbors page appears (see Figure 4-30).

Figure 4-30 CDP > Interface Neighbors Page



CDP > Interface Neighbors

Local Interface	Neighbor Name	Neighbor Address	Neighbor Port	TTL	Capability*	Platform
Port - 1	sanity2950-2	209.165.200.225	FastEthernet0/24	130	S I	cisco WS-C2950-24
Port - 1	WCS-Beringer-Dev	209.165.200.225	Unit - 0 Slot - 0 Port - 1	147	H	WLC4402-12
Port - 1	Concannon3	209.165.200.225	Unit - 0 Slot - 0 Port - 1	154	H	WLC4402-12
Port - 1	kit-4402	209.165.200.225	Unit - 0 Slot - 0 Port - 1	130	H	WLC4402-12
Port - 1	auzhao4402	209.165.200.225	Unit - 0 Slot - 0 Port - 1	162	H	AIR-WLC4402-12-K9
Port - 1	CJ-4402	209.165.200.225	Unit - 0 Slot - 0 Port - 2	121	H	WLC4402-12
Port - 1	Switch		GigabitEthernet0/1	180	S I	cisco WS-C3560G-24P
Port - 1	srinath-4400	209.165.200.225	Unit - 0 Slot - 0 Port - 1	153	H	WLC4404-100
Port - 1	Maria-4404	209.165.200.225	Unit - 0 Slot - 0 Port - 1	162	H	AIR-WLC4402-12-K9

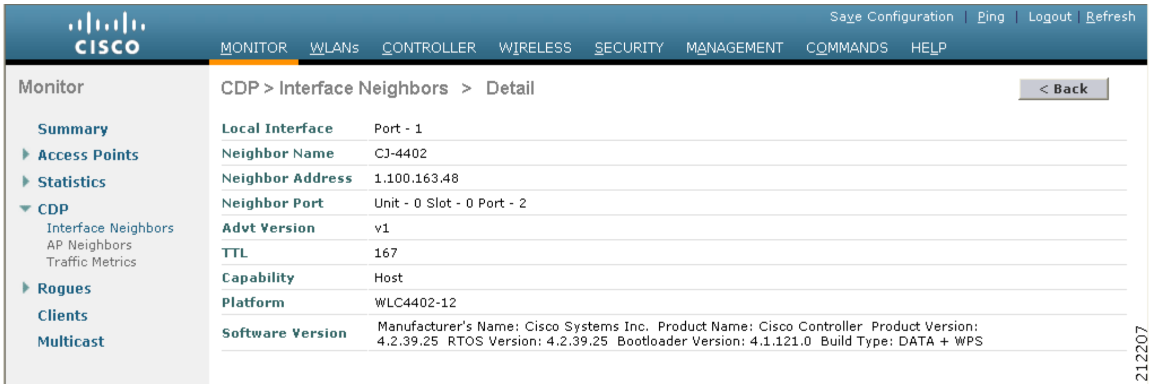
* Capability Code: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, M - Remotely Managed Device

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 To see more detailed information about each interface's CDP neighbor, click the name of the desired interface neighbor. The CDP > Interface Neighbors > Detail page appears (see Figure 4-31).

Figure 4-31 CDP > Interface Neighbors > Detail Page



CDP > Interface Neighbors > Detail

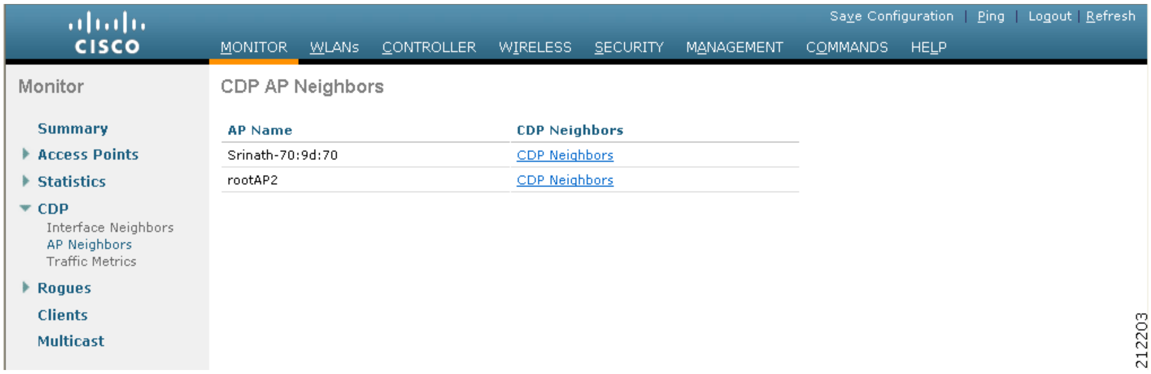
Local Interface	Port - 1
Neighbor Name	CJ-4402
Neighbor Address	1.100.163.48
Neighbor Port	Unit - 0 Slot - 0 Port - 2
Advt Version	v1
TTL	167
Capability	Host
Platform	WLC4402-12
Software Version	Manufacturer's Name: Cisco Systems Inc. Product Name: Cisco Controller Product Version: 4.2.39.25 RTOS Version: 4.2.39.25 Bootloader Version: 4.1.121.0 Build Type: DATA + WPS

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 To see a list of CDP neighbors for all access points connected to the controller, click **AP Neighbors**. The CDP AP Neighbors page appears (see Figure 4-32).

Figure 4-32 CDP AP Neighbors Page

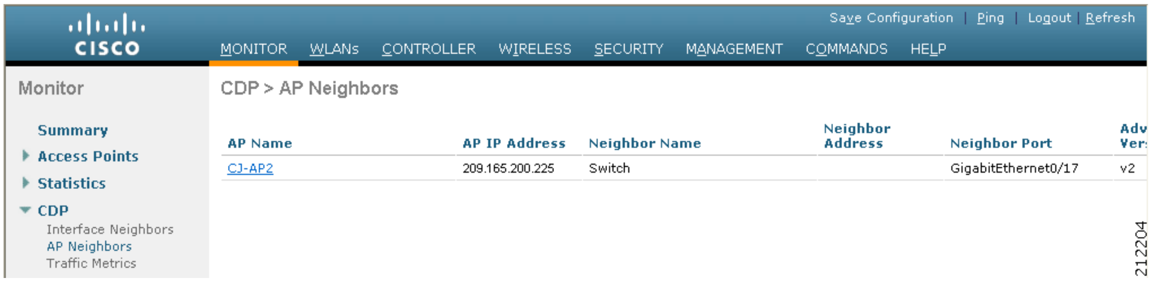


CDP AP Neighbors

AP Name	CDP Neighbors
Srinath-70:9d:70	CDP Neighbors
rootAP2	CDP Neighbors

Step 4 To see a list of CDP neighbors for a specific access point, click the **CDP Neighbors** link for the desired access point. The CDP > AP Neighbors page appears (see Figure 4-34).

Figure 4-33 CDP > AP Neighbors Page



CDP > AP Neighbors

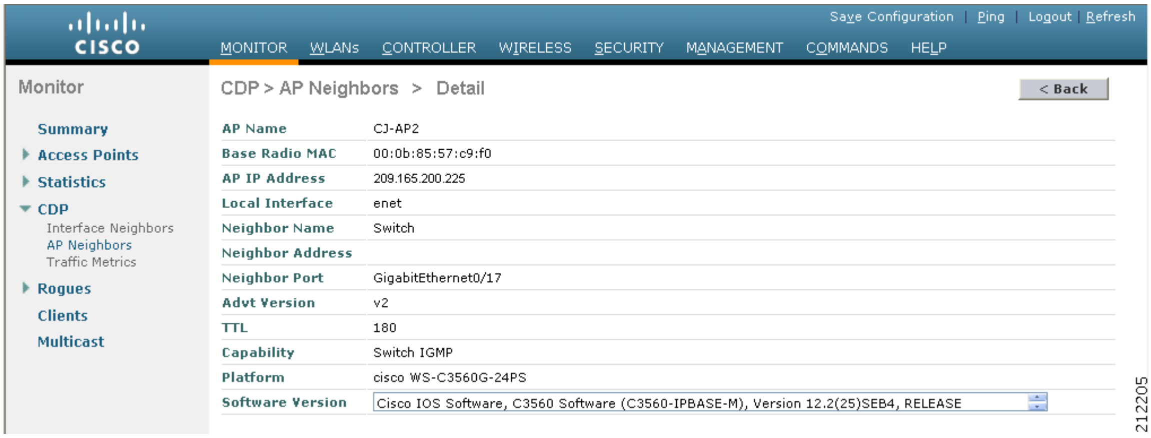
AP Name	AP IP Address	Neighbor Name	Neighbor Address	Neighbor Port	Adv Ver:
CJ-AP2	209.165.200.225	Switch		GigabitEthernet0/17	v2

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 To see detailed information about an access point's CDP neighbors, click the name of the desired access point. The CDP > AP Neighbors > Detail page appears (see Figure 4-34).

Figure 4-34 CDP > AP Neighbors > Detail Page



CDP > AP Neighbors > Detail

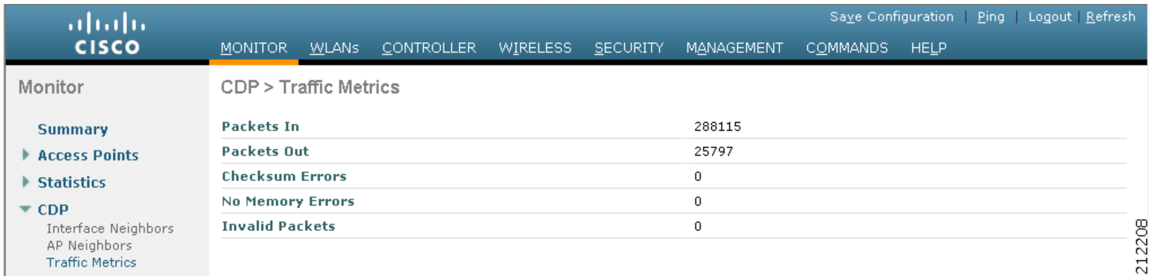
AP Name	CJ-AP2
Base Radio MAC	00:0b:85:57:c9:f0
AP IP Address	209.165.200.225
Local Interface	enet
Neighbor Name	Switch
Neighbor Address	
Neighbor Port	GigabitEthernet0/17
Advt Version	v2
TTL	180
Capability	Switch IGMP
Platform	cisco WS-C3560G-24PS
Software Version	Cisco IOS Software, C3560 Software (C3560-IPBASE-M), Version 12.2(25)SEB4, RELEASE

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
- 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 To see CDP traffic information, click **Traffic Metrics**. The CDP > Traffic Metrics page appears (see Figure 4-35).

Figure 4-35 CDP > Traffic Metrics Page



CDP > Traffic Metrics

Packets In	288115
Packets Out	25797
Checksum Errors	0
No Memory Errors	0
Invalid Packets	0

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

Using the CLI to Configure Cisco Discovery Protocol

Use these commands to configure CDP using the controller CLI.

1. To enable or disable CDP on the controller, enter this command:

   config cdp {**enable** | **disable**}

   CDP is enabled by default.

2. To specify the interval at which CDP messages are to be generated, enter this command:

   config cdp timer *seconds*

   The range is 5 to 254 seconds, and the default value is 60 seconds.

3. To specify the amount of time to be advertised as the time-to-live value in generated CDP packets, enter this command:

   config cdp holdtime *seconds*

   The range is 10 to 255 seconds, and the default value is 180 seconds.

4. To specify the highest CDP version supported on the controller, enter this command:

   config cdp advertise {**v1** | **v2**}

   The default value is v1.

5. To enable or disable CDP on all access points that are joined to the controller, enter this command:

   config ap cdp {**enable** | **disable**} **all**

   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 **config ap cdp enable all**.

Note After you enable CDP on all access points joined to the controller, you may disable and then re-enable CDP on individual access points using the command in #6 below. After you disable CDP on all access points joined to the controller, you may not enable and then disable CDP on individual access points.

6. To enable or disable CDP on a specific access point, enter this command:

   config ap cdp {**enable** | **disable**} *Cisco_AP*

7. To save your settings, enter this command:

   save config

Using the CLI to View Cisco Discovery Protocol Information

Use these commands to obtain information about CDP neighbors on the controller.

1. To see the status of CDP and to view CDP protocol information, enter this command:

   show cdp

2. To see a list of all CDP neighbors on all interfaces, enter 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.

3. To see all CDP entries in the database, enter this command:

   show cdp entry all

4. To see CDP traffic information on a given port (for example, packets sent and received, CRC errors, and so on), enter this command:

   show cdp traffic

5. To see the CDP status for a specific access point, enter this command:

   show ap cdp ap-name *Cisco_AP*

6. To see the CDP status for all access points that are connected to the controller, enter this command:

   show ap cdp all

7. To see a list of all CDP neighbors for a specific access point, enter 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.

8. To see a list of all CDP neighbors for all access points connected to the controller, enter these commands:

   show ap cdp neighbors all

   show ap cdp neighbors detail all

   Information similar to the following appears when you enter **show ap cdp neighbors all**:

```
AP Name            AP IP          Neighbor Name  Neighbor IP    Neighbor Port
--------           --------       -------------  -----------    -------------
AP0013.601c.0a0    10.76.108.123        6500-1   10.76.108.207  GigabitEthernet1/26
AP0013.601c.0b0    10.76.108.111        6500-1   10.76.108.207  GigabitEthernet1/27
AP0013.601c.0c0   10.76.108.125        6500-1    10.76.108.207  GigabitEthernet1/28
```

   Information similar to the following appears when you enter **show ap cdp neighbors detail all**:

```
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:
Cisco Internetwork Operating System Software  IOS (tm) s72033_rp Software
(s72033_rp-PSV-M), Version 12.2(18)SXD5, RELEASE SOFTWARE (fc3) Technical Support:
http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Fri 13-Ma
```

   Note The access point sends CDP neighbor information to the controller only when the information changes.

Use these commands to obtain CDP debug information for the controller.

1. To obtain debug information related to CDP packets, enter this command:

   debug cdp packets

2. To obtain debug information related to CDP events, enter this command:

   debug cdp events

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.

The controller supports tags from AeroScout, WhereNet, and Pango (an InnerWireless company). Some of the tags from these vendors comply with Cisco Compatible Extensions for RFID Tags. See Table 4-3 for details. The location appliance receives telemetry and chokepoint information from tags that are compliant with this CCX specification.

Table 4-3 Cisco Compatible Extensions for RFID Tags Summary

Partners	AeroScout		WhereNet	Pango (InnerWireless)
Product Name	T2	T3	Wheretag IV	V3
Telemetry				
Temperature	X	X		X
Pressure				
Humidity				
Status				
Fuel				
Quantity				
Distance				
Motion Detection	X	X		X
Number of Panic Buttons	1	2	0	1
Tampering		X	X	X
Battery Information	X	X	X	X
Multiple-Frequency Tags[1]	X	X	X	

[1] For chokepoint systems, note that the tag can work only with chokepoints coming from the same vendor.

Note Network Mobility Services Protocol (NMSP) runs on location appliance software release 3.0 or later. 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. Refer to 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.
- **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 4-4 lists the number of tags supported per controller.

Table 4-4 RFID Tags Supported per Controller

Controller	Number of RFID Tags Supported
Cisco WiSM	5000
4404	2500
4402	1250
Catalyst 3750G Integrated Wireless LAN Controller Switch	1250
2106	500
Controller Network Module within the Cisco 28/37/38xx Series Integrated Services Routers	500

You can configure and view RFID tag tracking information through the controller CLI.

Using the CLI to Configure RFID Tag Tracking

Follow these steps to configure RFID tag tracking parameters using the CLI.

Step 1 To enable or disable RFID tag tracking, enter this command:

config rfid status {**enable** | **disable**}

The default value is enabled.

Step 2 To specify a static timeout value (between 60 and 7200 seconds), enter 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, Cisco recommends that you set the timeout value to 90 seconds (approximately three times the beacon value). The default value is 1200 seconds.

Step 3 To enable or disable RFID tag mobility for specific tags, enter 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 check 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.

Using the CLI to View RFID Tag Tracking Information

Use these commands to view RFID tag tracking information using the controller CLI.

1. To see the current configuration for RFID tag tracking, enter 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
```

2. To see detailed information for a specific RFID tag, enter 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
7f ff ff ff 03 14 00 12 7b 10 48 53 c1 f7 51 4b
50 ba 5b 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 00 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 ag.... -76 dBm
      lap1242(slot 0, chan 1) 50 seconds ago..... -65 dBm
```

3. To see a list of all RFID tags currently connected to the controller, enter this command:

   show rfid summary

   Information similar to the following appears:

```
Total Number of RFID   : 24
----------------- -------- ------------------ ------ ---------------------
     RFID ID      VENDOR       Closest AP      RSSI  Time Since Last Heard
----------------- -------- ------------------ ------ ---------------------
00:04:f1:00:00:03 Wherenet HReap               -70      151 seconds ago
00:04:f1:00:00:05 Wherenet HReap               -66      251 seconds ago
00:0c:cc:5b:f8:1e Aerosct  HReap               -40        5 seconds ago
00:0c:cc:5c:05:10 Aerosct  HReap               -68       25 seconds ago
00:0c:cc:5c:06:69 Aerosct  HReap               -54        7 seconds ago
00:0c:cc:5c:06:6b Aerosct  HReap               -68      245 seconds ago
00:0c:cc:5c:06:b5 Aerosct  cisco1242           -67       70 seconds ago
00:0c:cc:5c:5a:2b Aerosct  cisco1242           -68       31 seconds ago
00:0c:cc:5c:87:34 Aerosct  HReap               -40        5 seconds ago
00:14:7e:00:05:4d Pango    cisco1242           -66      298 seconds ago
```

4. To see a list of RFID tags that are associated to the controller as clients, enter this command:

   show rfid client

   When the RFID tag is in client mode, information similar to the following appears:

```
------------------ -------- --------- ----------------- ------ ----------------
                              Heard
   RFID Mac         VENDOR   Sec Ago    Associated AP    Chnl    Client State
------------------ -------- --------- ----------------- ------ ----------------

00:14:7e:00:0b:b1   Pango      35    AP0019.e75c.fef4   1      Probing
```

   When the RFID tag is not in client mode, the above fields are blank.

Using the CLI to Debug RFID Tag Tracking Issues

If you experience any problems with RFID tag tracking, use these debug commands.

- To configure MAC address debugging, enter this command:

  debug mac addr *mac_address*

  Note Cisco recommends 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.

- To enable or disable RFID debug options, enter 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, and
- **receive** configures debugging of incoming RFID tag messages.

Configuring and Viewing Location Settings

This section provides instructions for configuring and viewing 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 "Synchronizing the Controller and Location Appliance" section on page 4-86 to do so.

Follow these steps to install the location appliance certificate on the controller.

Step 1 To obtain the key hash value of the location appliance certificate, enter 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 036cdb87
5bd20e5a
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Key Data  894c66f4 df1cbcfb 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: SSC Key Hash is
4869b32638c00ffca88abe9b1a8e0525b9344b8b
```

Step 2 To install the location appliance certificate on the controller, enter this command:

config auth-list add lbs-ssc *lbs_mac lbs_key*

where

- *lbs_mac* is the MAC address of the location appliance, and
- *lbs_key* is the 20-byte key hash value of the certificate.

Step 3 To save your changes, enter this command:

save config

Step 4 To verify that the location appliance certificate is installed on the controller, enter this command:

show auth-list

Information similar to the following appears:

```
Authorize APs against AAA ....................... disabled
Allow APs with Self-Signed Certificate (SSC) .... disabled

Mac Addr                  Cert Type    Key Hash
-----------------------   ----------   --------------------------------------------
00:16:36:91:9a:27         LBS-SSC    593f34e7cb151997a28cc7da2a6cac040b329636
```

Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues

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 30 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.

Using the controller CLI, follow these steps to modify the NMSP notification interval value on the controller.

Step 1 To set the NMSP notification interval value for clients, RFID tags, and rogue clients and access points, enter these commands, where *interval* is a value between 1 and 30 seconds:

- **config nmsp notify-interval measurement clients** *interval*
- **config nmsp notify-interval measurement rfid** *interval*
- **config nmsp notify-interval measurement rogues** *interval*

Step 2 To view the NMSP configuration setting, enter this command:

show nmsp notify-interval summary

Information similar to the following appears:

```
NMSP Notification Interval Summary

Client
        Measurement interval: 2 sec
RFID
        Measurement interval: 8 sec
Rogue AP
        Measurement interval: 2 sec
Rogue Client
        Measurement interval: 2 sec
```

Synchronizing the Controller and Location Appliance

For controller software release 4.2 or later, if a location appliance (release 3.1 or later) is installed on your network, the time zone must be set on the controller to ensure proper synchronization between the two systems. Also, Cisco highly recommends that the time be set for networks that do not have location appliances. Refer to the "Managing the System Date and Time" section on page 4-10 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.

Using the CLI to View Location Settings

The controller determines the location of client devices by gathering received signal strength indicator (RSSI) measurements from access points all around the client of interest. The controller can obtain location reports from up to 16 access points for both clients and RFID tags.

Use these commands to view location information using the controller CLI.

1. To view the current location configuration values, enter 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
Rogue AP
        RSSI expiry timeout:             5 sec
        Half life:                       0 sec
        Notify Threshold:                0 db
```

```
RFID Tag
       RSSI expiry timeout:             5 sec
       Half life:                       0 sec
       Notify Threshold:                0 db
```

2. To see the location-based RFID statistics, enter 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
```

3. To clear the location-based RFID statistics, enter this command:

   clear location statistics rfid

4. To clear a specific RFID tag or all of the RFID tags in the entire database, enter this command:

   clear location rfid {*mac_address* | **all**}

5. To see whether location presence (S69) is supported on a client, enter 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
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
...
```

Note See the *Cisco Wireless Control System Configuration Guide* or the *Cisco Location Appliance Configuration Guide* for instructions on enabling location presence on a location appliance.

6. To see the status of active Network Mobility Services Protocol (NMSP) connections, enter this command:

   show nmsp status

   Information similar to the following appears:

```
LocServer IP    TxEchoResp RxEchoReq  TxData  RxData
-------------- ----------- ---------  ------- -------
171.71.132.158   21642       21642  51278   21253
```

7. To see the NMSP counters, enter this command:

   show nmsp statistics {**summary** | **connection all**}

   where

   - **summary** shows the common NMSP counters, and
   - **connection all** 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
Send too big msg:                    0
Failed SSL write:                    0
Partial SSL write:                   0
SSL write attempts to want write:
Transmit Q full:                     0
Max Measure Notify Msg:              0
Max Info Notify Msg:                 0
Max Tx Q Size:                       2
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 Tag Stats Notify Delay:          0
RFID Measurement Periodic:           0
RFID Measurement Immediate:          0
Reconnect Before Conn Timeout:        0
```

   Information similar to the following appears for each active connection when you enter the **show nmsp statistics connection all** command:

```
NMSP Connection Counters

Connection 1:
    Connection status: UP
    Freed Connection:  0
    Nmsp Subscr Req:   0          NMSP Subscr Resp:  0
    Info Req:          1          Info Resp:         1
    Measure Req:       2          Measure Resp:      2
    Stats Req:         2          Stats Resp:        2
    Info Notify:       0          Measure Notify:    0
    Loc Capability:    2
    Location Req:      0          Location Rsp:      0
    Loc Subscr Req:    0          Loc Subscr Rsp:    0
    Loc Notif:         0
    Loc Unsubscr Req:  0          Loc Unsubscr Rsp:  0
    IDS Get Req:       0          IDS Get Resp:      0
    IDS Notif:         0
    IDS Set Req:       0          IDS Set Resp:      0
```

8. To clear the NMSP statistics, enter this command:

clear nmsp statistics

9. To view all mobility services active on the controller, enter this command:

show services mobility summary

Information similar to the following appears:

```
Mobility Services Subscribed:

Server IP          Applications
---------          -------------
172.19.35.218      Client Tracking, Tag Tracking, Rogue Tracking,
                   Handover Client Tracking, FMC, AP Monitor, IDS
```

10. To view detailed mobility services information for all connections or for a specific connection, enter this command:

show services mobility detail {**all** | *IP_address*}

Information similar to the following appears for the **show services mobility detail all** command:

```
Mobility Services Subscribed by 172.19.35.218 -

Application               Services
-----------               --------
Client Tracking           RSSI, Info, Statistics
Tag Tracking              RSSI, Statistics
Rogue Tracking            RSSI, Info
Handover Client Tracking  RSSI, Info,
FMC                       Handover
AP Monitor                AP Status
IDS Services              WIPS
```

Configuring the Supervisor 720 to Support the WiSM

When you install a WiSM in a Cisco Catalyst 6500 switch or a Cisco 7600 series router, you must configure the Supervisor 720 to support the WiSM. When the supervisor detects the WiSM, the supervisor creates ten Gigabit Ethernet interfaces, ranging from Gig*slot*/1 to Gig*slot*/8. For example, if the WiSM is in slot 9, the supervisor creates interfaces Gig9/1 through Gig9/8. The first eight Gigabit Ethernet interfaces must be organized into two Etherchannel bundles of four interfaces each. The remaining two Gigabit Ethernet interfaces are used as service-port interfaces, one for each controller on the WiSM. You must manually create VLANs to communicate with the ports on the WiSM.

Note The WiSM is supported on Cisco 7600 series routers running only Cisco IOS Release 12.2(18)SXF5.

General WiSM Guidelines

Keep these general guidelines in mind when you add a WiSM to your network:

- The switch or router ports leading to the controller service port are automatically configured and cannot be manually configured.
- The switch or router ports leading to the controller data ports should be configured as edge ports to avoid sending unnecessary BPDUs.
- The switch or router ports leading to the controller data ports should not be configured with any additional settings (such as port channel or SPAN destination) other than settings necessary for carrying data traffic to and from the controllers.

Note Refer to Chapter 3 for information on configuring the WiSM's ports and interfaces.

Configuring the Supervisor

Log into the switch or router CLI and, beginning in Privileged Exec mode, follow these steps to configure the supervisor to support the WiSM:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *vlan*	Create a VLAN to communicate with the data ports on the WiSM and enter interface config mode.
Step 3	**ip address** *ip-address gateway*	Assign an IP address and gateway to the VLAN.
Step 4	**ip helper-address** *ip-address*	Assign a helper address to the VLAN.
Step 5	**end**	Return to global config mode.
Step 6	**wism module** *module_number* **controller** { **1** | **2**} **allowed-vlan** *vlan_number*	Create Gigabit port-channel interfaces automatically for the specified WiSM controller and configure the port-channel interfaces as trunk ports. Also, specify the VLAN you created earlier as the allowed VLAN on the port-channel trunk. VLAN traffic is carried on the trunk between the WiSM controller and the supervisor. **Note** Services might be temporarily interrupted (for approximately two pings) after you enter this command.
Step 7	**wism module** *module_number* **controller** { **1** | **2**} **native-vlan** *vlan_number*	For the native VLAN on the ports, specify the VLAN that you created earlier to communicate with the WiSM data ports.
Step 8	**interface** *vlan*	Create a VLAN to communicate with the service ports on the WiSM.
Step 9	**ip address** *ip_address gateway*	Assign an IP address and gateway to the VLAN.
Step 10	**end**	Return to global config mode.
Step 11	**wism service-vlan** *vlan*	Configure the VLAN that you created in steps 8 through 10 to communicate with the WiSM service ports.

	Command	Purpose
Step 12	**end**	Return to global config mode.
Step 13	**show wism status**	Verify that the WiSM is operational.

Note The commands used for communication between the Cisco WiSM, the Supervisor 720, and the 4404 controllers are documented in *Configuring a Cisco Wireless Services Module and Wireless Control System* at this URL:
http://www.cisco.com/en/US/docs/wireless/technology/wism/technical/reference/appnote.html#wp39498

Using the Wireless LAN Controller Network Module

Keep these guidelines in mind 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 to IPSec configuration instructions for routers:

  http://www.cisco.com/en/US/tech/tk583/tk372/tech_configuration_guides_list.html

- 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, Cisco recommends 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.

CHAPTER 5

Configuring Security Solutions

This chapter describes security solutions for wireless LANs. It contains these sections:

- Cisco UWN Solution Security, page 5-2
- Configuring RADIUS, page 5-3
- Configuring TACACS+, page 5-18
- Configuring Local Network Users, page 5-29
- Configuring LDAP, page 5-33
- Configuring Local EAP, page 5-38
- Configuring the System for SpectraLink NetLink Telephones, page 5-50
- Using Management over Wireless, page 5-52
- Configuring DHCP Option 82, page 5-53
- Configuring and Applying Access Control Lists, page 5-54
- Configuring Management Frame Protection, page 5-66
- Configuring Client Exclusion Policies, page 5-73
- Configuring Identity Networking, page 5-74
- Managing Rogue Devices, page 5-80
- Configuring IDS, page 5-103
- Configuring wIPS, page 5-119
- Detecting Active Exploits, page 5-122
- Configuring Maximum Local Database Entries, page 5-122

Cisco UWN Solution Security

Cisco UWN Solution security includes the following sections:

- Security Overview, page 5-2
- Layer 1 Solutions, page 5-2
- Layer 2 Solutions, page 5-2
- Layer 3 Solutions, page 5-3
- Integrated Security Solutions, page 5-3

Security Overview

The Cisco 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. Also, the complexity of add-on security solutions has prevented many IT managers from embracing the benefits of the latest advances in WLAN security.

Layer 1 Solutions

The Cisco UWN security solution ensures that all clients gain access within an operator-set number of attempts. Should a client fail to gain access within that limit, it is automatically excluded (blocked from access) until the operator-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, the network administrator 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 + Michael (temporal key integrity protocol + message integrity code checksum) dynamic keys, or WEP (Wired Equivalent Privacy) static keys. Disabling is also used to automatically block Layer 2 access after an operator-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.

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.

Finally, 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

- Cisco UWN Solution operating system security is built around a robust 802.1X AAA (authorization, authentication and accounting) engine, which allows operators 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. This 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 notify the operator when they are detected.
- Operating system security works with industry-standard authorization, authentication, and accounting (AAA) servers, making system integration simple and easy.

Configuring 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.

  Note 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.

- **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 up to 17 RADIUS authentication and accounting servers each. 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.

Note If multiple RADIUS servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

The primary RADIUS server (the server with 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 forever, 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.

You must configure RADIUS on both your CiscoSecure Access Control Server (ACS) and your controller. You can configure the controller through either the GUI or the CLI.

Configuring RADIUS on the ACS

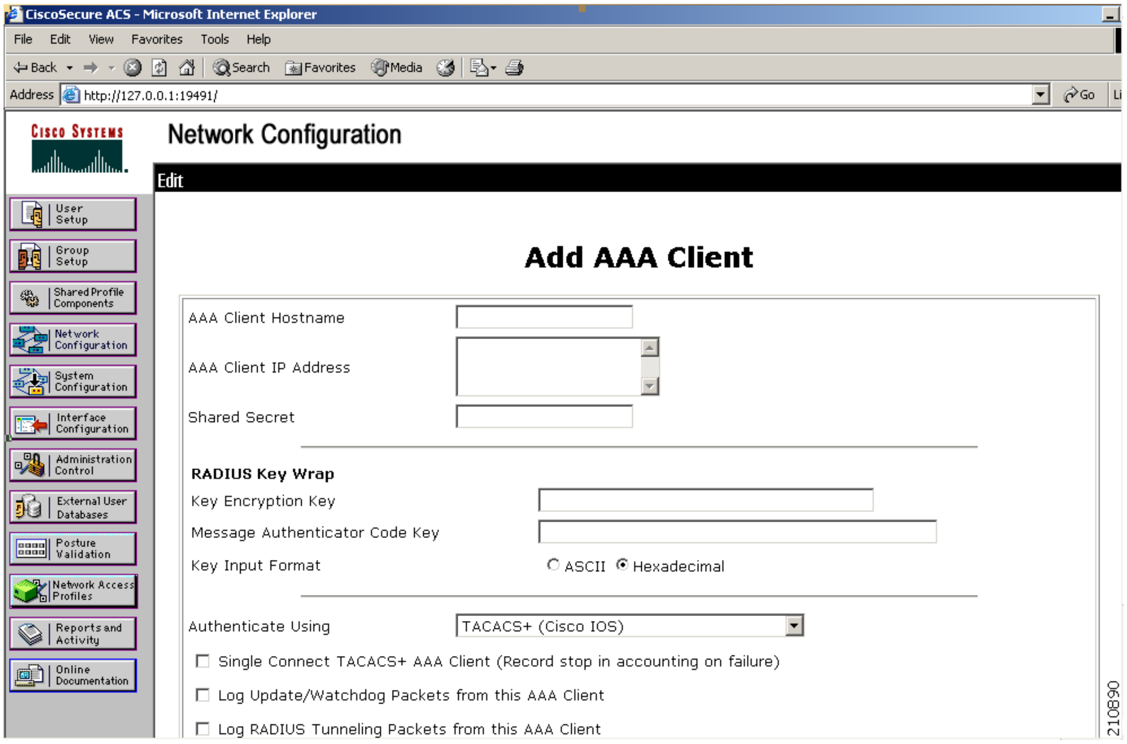
Follow these steps to configure RADIUS on the ACS.

Note RADIUS is supported on CiscoSecure ACS version 3.2 and greater. The instructions and illustrations in this section pertain to ACS version 4.1 and may vary for other versions. Refer to the CiscoSecure ACS documentation for the version you are running.

Step 1 Click **Network Configuration** on the ACS main page.

Step 2 Click **Add Entry** under AAA Clients to add your controller to the server. The Add AAA Client page appears (see Figure 5-1).

Figure 5-1 Add AAA Client Page on CiscoSecure ACS



Add AAA Client

AAA Client Hostname

AAA Client IP Address

Shared Secret

RADIUS Key Wrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format ○ ASCII ● Hexadecimal

Authenticate Using TACACS+ (Cisco IOS)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

Step 3 In the AAA Client Hostname field, enter the name of your controller.

Step 4 In the AAA Client IP Address field, enter the IP address of your controller.

Step 5 In the Shared Secret field, 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 Choose **RADIUS (Cisco Aironet)** from the Authenticate Using drop-down box.

Step 7 Click **Submit + Apply** to save your changes.

Step 8 Click **Interface Configuration** on the ACS main page.

Step 9 Click **RADIUS (Cisco Aironet)**. The RADIUS (Cisco Aironet) page appears.

Step 10 Under User Group, check the **Cisco-Aironet-Session-Timeout** check box.

Step 11 Click **Submit** to save your changes.

Step 12 Click **System Configuration** on the ACS main page.

Step 13 Click **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 Click **Group Setup** on the ACS main page.

Step 16 Choose a previously created group from the Group drop-down box.

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**, check the **Cisco-Aironet-Session-Timeout** check box and enter a session timeout value in the edit box.

Step 19 To specify read-only or read-write access to controllers through RADIUS authentication, set 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 check the **Management** check box on the RADIUS Authentication Servers page of the controller GUI. See Step 17 in the next section for more information.

Note The "RADIUS Authentication Attributes Sent by the Access Point" section on page 5-15 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.

Using the GUI to Configure RADIUS

Using the controller GUI, follow these steps to configure RADIUS.

Step 1 Click **Security** > **AAA** > **RADIUS**.

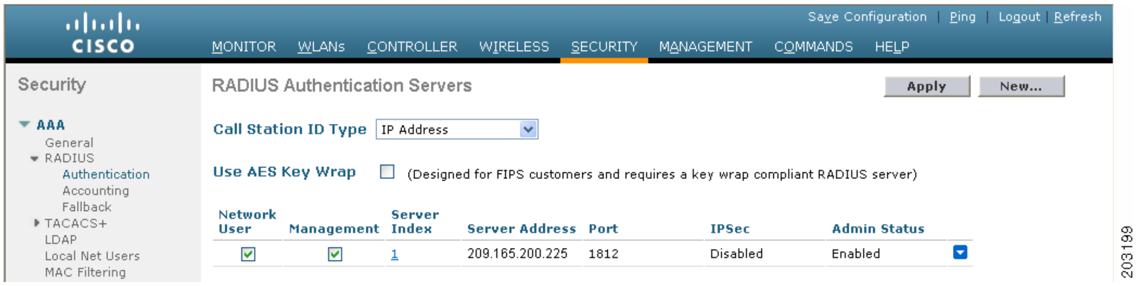
Step 2 Perform one of the following:

- If you want to configure a RADIUS server for authentication, click **Authentication**.
- If you want to configure a RADIUS server for accounting, click **Accounting**.

Note The GUI pages used to configure authentication and accounting contain mostly the same fields. 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 (see Figure 5-2).

Figure 5-2 RADIUS Authentication Servers Page



RADIUS Authentication Servers

Call Station ID Type: IP Address

Use AES Key Wrap □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
☑	☑	1	209.165.200.225	1812	Disabled	Enabled

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 box, 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.

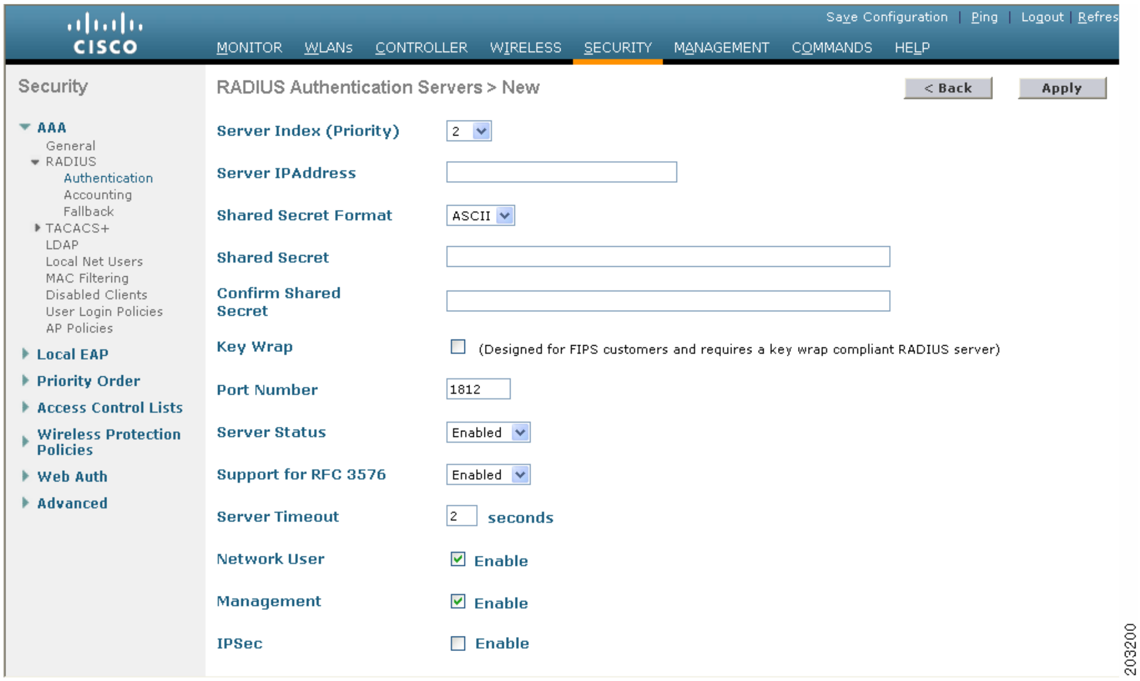
Step 4 To enable RADIUS-to-controller key transport using AES key wrap protection, check the **Use AES Key Wrap** check box. The default value is unchecked. This feature is required for FIPS customers.

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

Step 6 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 (see Figure 5-3).

Figure 5-3 RADIUS Authentication Servers > New Page



RADIUS Authentication Servers > New

Server Index (Priority)	2
Server IPAddress	
Shared Secret Format	ASCII
Shared Secret	
Confirm Shared Secret	
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	☑ Enable
Management	☑ Enable
IPSec	□ Enable

Step 7 If you are adding a new server, choose a number from the Server Index (Priority) drop-down box to specify the priority order of this server in relation to any other configured RADIUS servers providing the same service. You can configure up to 17 servers. If the controller cannot reach the first server, it tries the second one in the list, then the third one if necessary, and so on.

Step 8 If you are adding a new server, enter the IP address of the RADIUS server in the Server IP Address field.

Step 9 From the Shared Secret Format drop-down box, 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 10 In the Shared Secret and Confirm Shared Secret fields, 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 11 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. AES key wrap is designed for Federal Information Processing Standards (FIPS) customers and requires a key-wrap compliant RADIUS authentication server.

a. Check the **Key Wrap** check box.Choose **ASCII** or **Hex** from the Key Wrap Format drop-down box to specify the format of the AES key wrap keys: Key Encryption Key (KEK) and Message Authentication Code Key (MACK).

b. In the Key Encryption Key (KEK) field, enter the 16-byte KEK.

c. In the Message Authentication Code Key (MACK) field, enter the 20-byte KEK.

Step 12 If you are adding a new server, enter the RADIUS server's UDP port number for the interface protocols in the Port Number field. The valid range is 1 to 65535, and the default value is 1812 for authentication and 1813 for accounting.

Step 13 From the Server Status field, choose **Enabled** to enable this RADIUS server or choose **Disabled** to disable it. The default value is Enabled.

Step 14 If you are configuring a new RADIUS authentication server, choose **Enabled** from the Support for RFC 3576 drop-down box 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 whereas CoA messages modify session authorization attributes such as data filters.

Step 15 In the Server Timeout field, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Note Cisco recommends 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 16 Check the **Network User** check box to enable network user authentication (or accounting), or uncheck it to disable this feature. The default value is checked. 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 17 If you are configuring a RADIUS authentication server, check the **Management** check box to enable management authentication, or uncheck it to disable this feature. The default value is checked. 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 18 Check the **IPSec** check box to enable the IP security mechanism, or uncheck it to disable this feature. The default value is unchecked.

Note The IPSec option appears only if a crypto card is installed in the controller.

Step 19 If you enabled IPSec in Step 18, follow these steps to configure additional IPSec parameters:

a. From the IPSec drop-down box, 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 a mechanism 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 box, choose one of the following options to specify the IP security encryption mechanism:

- **DES**—Data Encryption Standard 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 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 box, 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 field, 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 box, 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 20 Click **Apply** to commit your changes.

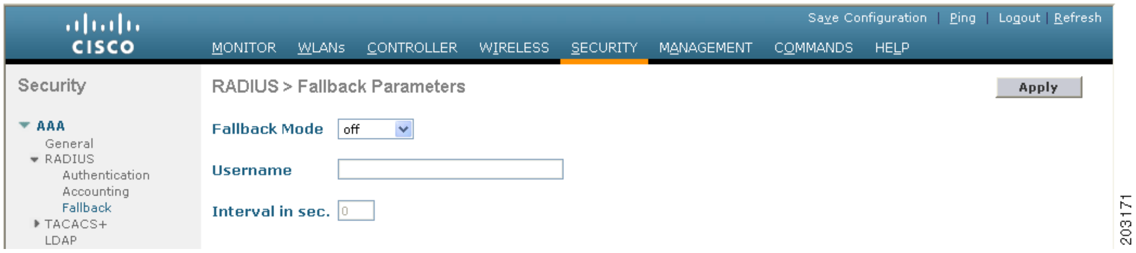
Step 21 Click **Save Configuration** to save your changes.

Step 22 Repeat the previous steps if you want to configure any additional services on the same server or any additional RADIUS servers.

Step 23 To specify the RADIUS server fallback behavior, follow these steps:

a. Click **Security** > **AAA** > **RADIUS** > **Fallback** to open the RADIUS > Fallback Parameters page (see Figure 5-4).

Figure 5-4 RADIUS > Fallback Parameters Page



RADIUS > Fallback Parameters

Fallback Mode: off

Username:

Interval in sec.: 0

b. From the Fallback Mode drop-down box, choose one of the following options:

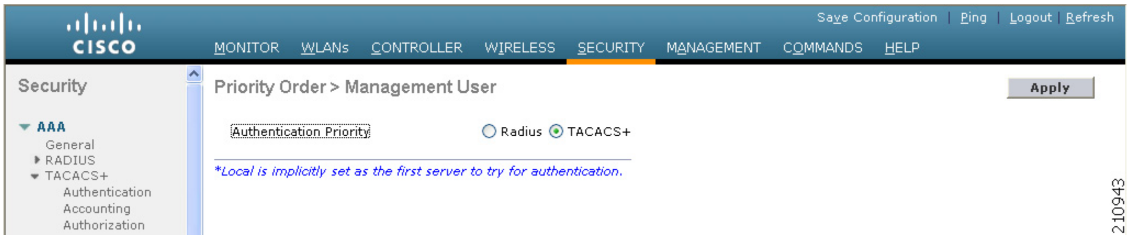
- **Off**—Disables RADIUS server fallback. This is the default value.
- **Passive**—Causes the controller to revert to a server with a lower priority from the available backup servers without using extraneous probe messages. The controller simply ignores all inactive servers for a time period and retries 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.

c. If you enabled Active fallback mode in Step b, enter the name to be sent in the inactive server probes. in the Username field. 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 field. 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 24 To specify the order of authentication when multiple databases are configured, click **Security** > **Priority Order** > **Management User**. The Priority Order > Management User page appears (see Figure 5-5).

Figure 5-5 Priority Order > Management User Page



Priority Order > Management User

Authentication Priority ○ Radius ● TACACS+

*Local is implicitly set as the first server to try for authentication.

Step 25 For Authentication Priority, choose either **Radius** or **TACACS+** to specify which server has priority over the other when the controller attempts to authenticate management users. By default, the local database is always queried first. If the username is not found, the controller switches to the TACACS+ server if configured for TACACS+ or to the RADIUS server if configured for Radius. The default setting is local and then Radius.

Step 26 Click **Apply** to commit your changes.

Step 27 Click **Save Configuration** to save your changes.

Using the CLI to Configure RADIUS

Using the controller CLI, follow these steps to configure RADIUS.

Note Refer to the "Using the GUI to Configure RADIUS" section on page 5-6 for the valid ranges and default values of the parameters used in the CLI commands.

Step 1 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, enter this command:

config radius callStationIdType {*ip_address*, *mac_address*, *ap_mac_address*, *ap_macaddr_ssid*}

Step 2 Use these commands to configure a RADIUS authentication server:

- **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 whereas CoA messages modify session authorization attributes such as data filters.
- **config radius auth retransmit-timeout** *index timeout*—Configures the 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.
- **config radius auth ipsec authentication** {**hmac-md5 | hmac-sha1**} *index*—Configures the authentication protocol to be used for IP security.
- **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 3 Use these commands to configure a RADIUS accounting server:

- **config radius acct add** *index server_ip_address port#* {**ascii | hex**} *shared_secret*—Adds a RADIUS accounting server.
- **config radius acct server-timeout** *index timeout*—Configures the retransmission timeout value for a RADIUS accounting server.
- **config radius acct network** *index* **{enable | disable**}—Enables or disables network user accounting. If you enable this feature, this entry is considered the RADIUS 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.
- **config radius acct ipsec** {**enable | disable**} *index*—Enables or disables the IP security mechanism.

- **config radius acct ipsec authentication** {**hmac-md5** | **hmac-sha1**} *index*—Configures the authentication protocol to be used for IP security.
- **config radius acct ipsec encryption** {**3des** | **aes** | **des** | **none**} *index*—Configures the IP security encryption mechanism.
- **config radius acct ipsec ike dh-group** {**group-1** | **group-2** | **group-5**} *index*—Configures the IKE Diffie Hellman group.
- **config radius acct ipsec ike lifetime** *interval index*—Configures the timeout interval for the session.
- **config radius acct ipsec ike phase1**{**aggressive** | **main**} *index*—Configures the Internet Key Exchange (IKE) protocol.
- **config radius acct** {**enable** | **disable**} *index*—Enables or disables a RADIUS accounting server.
- **config radius acct delete** *index*—Deletes a previously added RADIUS accounting server.

Step 4 To configure the RADIUS server fallback behavior, enter 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 5 If you enabled Active mode in Step 4, 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 6 To save your changes, enter this command:

save config

Step 7 To configure the order of authentication when multiple databases are configured, enter 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 this command:

show aaa auth

Information similar to the following appears:

```
Management authentication server order:
   1....................................... local
   2.................................... radius
```

Step 8 Use these commands to see RADIUS statistics:

- **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.

Information similar to the following appears for the **show radius auth statistics** command:

```
Authentication Servers:

Server Index..................................... 1
Server Address................................... 10.91.104.76
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 1
Retry Requests................................... 0
Accept Responses................................. 0
Reject Responses................................. 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops................................... 0
```

Information similar to the following appears for the **show radius acct statistics** command:

```
Accounting Servers:

Server Index..................................... 1
Server Address................................... 10.10.10.1
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 1
Retry Requests................................... 0
Accounting Responses............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops................................... 0
```

Information similar to the following appears for the **show radius auth statistics** command:

```
RFC-3576 Servers:

Server Index..................................... 1
Server Address................................... 10.91.104.76
Disconnect-Requests.............................. 0
COA-Requests..................................... 0
Retransmitted Requests........................... 0
Malformed Requests............................... 0
Bad Authenticator Requests....................... 0
Other Drops...................................... 0
Sent Disconnect-Ack.............................. 0
Sent Disconnect-Nak.............................. 0
Sent CoA-Ack..................................... 0
Sent CoA-Nak.................................. 0
```

Step 9 To clear the statistics for one or more RADIUS servers, enter this command:

clear stats radius {**auth** | **acct**} {*index* | **all**}

Step 10 To make sure the controller can reach the RADIUS server, enter this command:

ping *server_ip_address*

RADIUS Authentication Attributes Sent by the Access Point

The tables in this section identify the RADIUS authentication attributes sent by a lightweight access point to a client in access-request and access-accept packets.

Table 5-1 Authentication Attributes Sent in Access-Request Packets

Attribute ID	Description
1	User-Name
2	Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type[1]
12	Framed-MTU
30	Called-Station-ID (MAC address)
31	Calling-Station-ID (MAC address)
32	NAS-Identifier
33	Proxy-State
60	CHAP-Challenge
61	NAS-Port-Type
79	EAP-Message
243	TPLUS-Role

[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 5-2 Authentication Attributes Honored in Access-Accept Packets (Cisco)

Attribute ID	Description
1	Cisco-LEAP-Session-Key
2	Cisco-Keywrap-Msg-Auth-Code
3	Cisco-Keywrap-NonCE
4	Cisco-Keywrap-Key
5	Cisco-URL-Redirect
6	Cisco-URL-Redirect-ACL

Note These Cisco-specific attributes are not supported: Auth-Algo-Type and SSID.

Table 5-3 Authentication Attributes Honored in Access-Accept Packets (Standard)

Attribute ID	Description
6	Service-Type[1]
8	Framed-IP-Address
25	Class
26	Vendor-Specific
27	Timeout
29	Termination-Action
40	Acct-Status-Type
64	Tunnel-Type
79	EAP-Message
81	Tunnel-Group-ID

[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.

Note Message authenticator is not supported.

Table 5-4 Authentication Attributes Honored in Access-Accept Packets (Microsoft)

Attribute ID	Description
11	MS-CHAP-Challenge
16	MS-MPPE-Send-Key
17	MS-MPPE-Receive-Key
25	MS-MSCHAP2-Response
26	MS-MSCHAP2-Success

Table 5-5 Authentication Attributes Honored in Access-Accept Packets (Airespace)

Attribute ID	Description
1	VAP-ID
2	QoS-Level
3	DSCP
4	8021P-Type
5	VLAN-Interface-Name
6	ACL-Name
7	Data-Bandwidth-Average-Contract
8	Real-Time-Bandwidth-Average-Contract
9	Data-Bandwidth-Burst-Contract
10	Real-Time-Bandwidth-Burst-Contract
11	Guest-Role-Name

RADIUS Accounting Attributes

Table 5-6 identifies the RADIUS accounting attributes for accounting requests sent from a controller to the RADIUS server. Table 5-7 lists the different values for the Accounting-Status-Type attribute (40).

Table 5-6 Accounting Attributes for Accounting Requests

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
8	Framed-IP-Address
25	Class
30	Called-Station-ID (MAC address)
31	Calling-Station-ID (MAC address)
32	NAS-Identifier
40	Accounting-Status-Type
41	Accounting-Delay-Time (Stop and interim messages only)
42	Accounting-Input-Octets (Stop and interim messages only)
43	Accounting-Output-Octets (Stop and interim messages only)
44	Accounting-Session-ID
45	Accounting-Authentic
46	Accounting-Session-Time (Stop and interim messages only)
47	Accounting-Input-Packets (Stop and interim messages only)
48	Accounting-Output-Packets (Stop and interim messages only)
49	Accounting-Terminate-Cause (Stop messages only)

Table 5-6 Accounting Attributes for Accounting Requests (continued)

Attribute ID	Description
64	Tunnel-Type
65	Tunnel-Medium-Type
81	Tunnel-Group-ID

Table 5-7 Accounting-Status-Type Attribute Values

Attribute ID	Description
1	Start
2	Stop
3	Interim-Update
7	Accounting-On
8	Accounting-Off
9-14	Reserved for Tunneling Accounting
15	Reserved for Failed

Configuring 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+.

  Note 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.

Note If users attempt to make changes on a controller GUI page that are not permitted for their assigned role, a message appears indicating that they do not have sufficient privilege. If users enter a controller CLI command that is not permitted for their assigned role, a message may appear indicating that the command was successfully executed although it was not. In this case, the following additional message appears to inform users that they lack sufficient privileges to successfully execute the command: "Insufficient Privilege! Cannot execute command!"

- **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.

Note If multiple TACACS+ servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

You must configure TACACS+ on both your CiscoSecure Access Control Server (ACS) and your controller. You can configure the controller through either the GUI or the CLI.

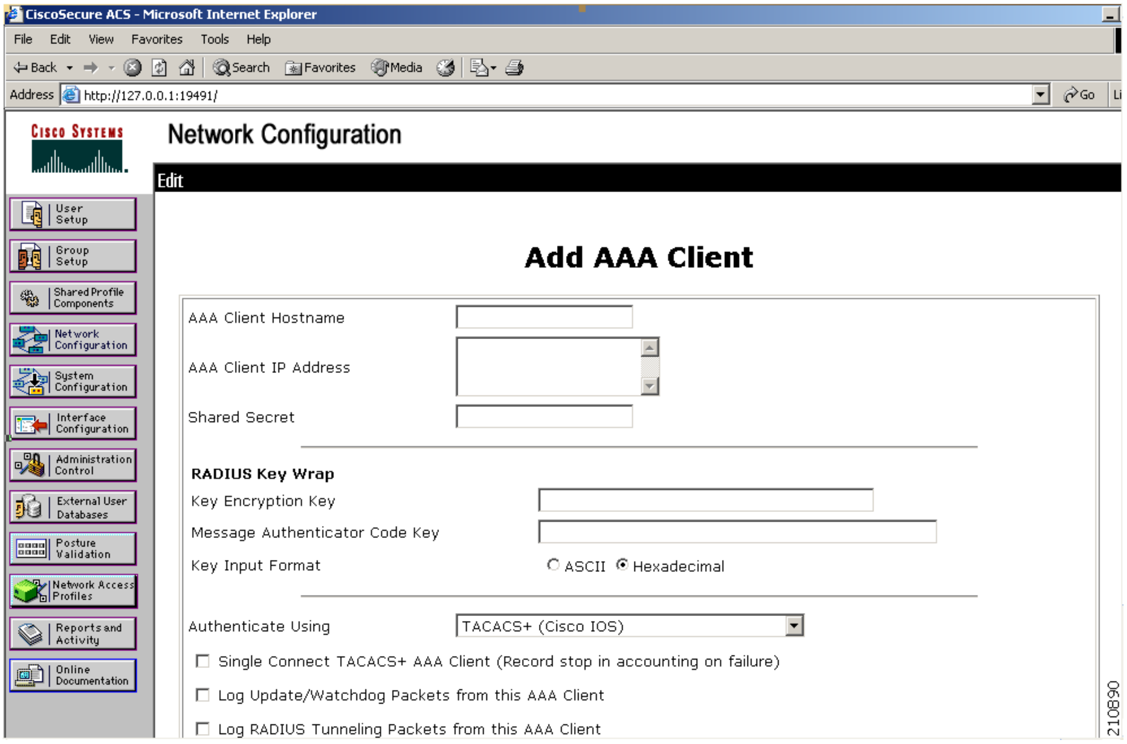
Configuring TACACS+ on the ACS

Follow these steps to configure TACACS+ on the ACS.

Note TACACS+ is supported on CiscoSecure ACS version 3.2 and greater. The instructions and illustrations in this section pertain to ACS version 4.1 and may vary for other versions. Refer to the CiscoSecure ACS documentation for the version you are running.

Step 1 Click **Network Configuration** on the ACS main page.

Step 2 Click **Add Entry** under AAA Clients to add your controller to the server. The Add AAA Client page appears (see Figure 5-6).



Add AAA Client

AAA Client Hostname

AAA Client IP Address

Shared Secret

RADIUS Key Wrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format ○ ASCII ● Hexadecimal

Authenticate Using TACACS+ (Cisco IOS)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

Figure 5-6 Add AAA Client Page on CiscoSecure ACS

Step 3 In the AAA Client Hostname field, enter the name of your controller.

Step 4 In the AAA Client IP Address field, enter the IP address of your controller.

Step 5 In the Shared Secret field, 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.

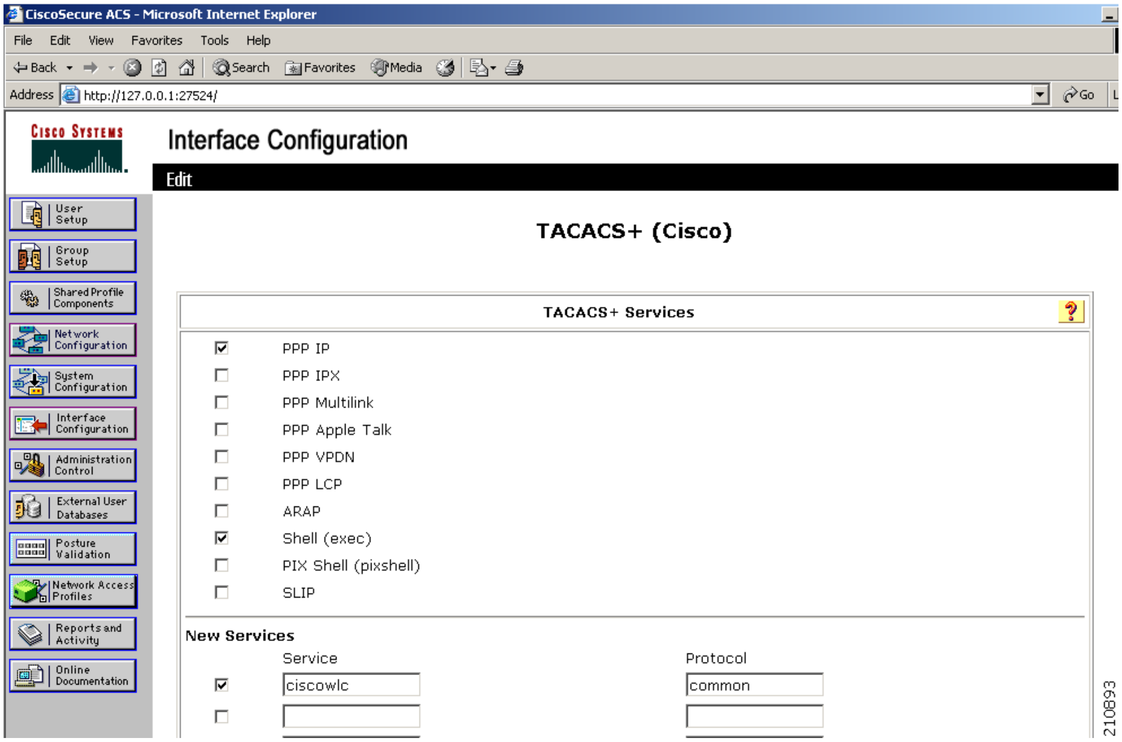
Step 6 Choose **TACACS+ (Cisco IOS)** from the Authenticate Using drop-down box.

Step 7 Click **Submit + Apply** to save your changes.

Step 8 Click **Interface Configuration** on the ACS main page.

Step 9 Click **TACACS+ (Cisco IOS)**. The TACACS+ (Cisco) page appears (see Figure 5-7).

Figure 5-7 TACACS+ (Cisco) Page on CiscoSecure ACS



Interface Configuration

Edit

TACACS+ (Cisco)

TACACS+ Services

☑ PPP IP
□ PPP IPX
□ PPP Multilink
□ PPP Apple Talk
□ PPP VPDN
□ PPP LCP
□ ARAP
☑ Shell (exec)
□ PIX Shell (pixshell)
□ SLIP

New Services

	Service	Protocol
☑	ciscowlc	common
□		

Step 10 Under TACACS+ Services, check the **Shell (exec)** check box.

Step 11 Under New Services, check the first check box and enter **ciscowlc** in the Service field and **common** in the Protocol field.

Step 12 Under Advanced Configuration Options, check the **Advanced TACACS+ Features** check box.

Step 13 Click **Submit** to save your changes.

Step 14 Click **System Configuration** on the ACS main page.

Step 15 Click **Logging**.

Step 16 When the Logging Configuration page appears, enable all of the events that you want to be logged and save your changes.

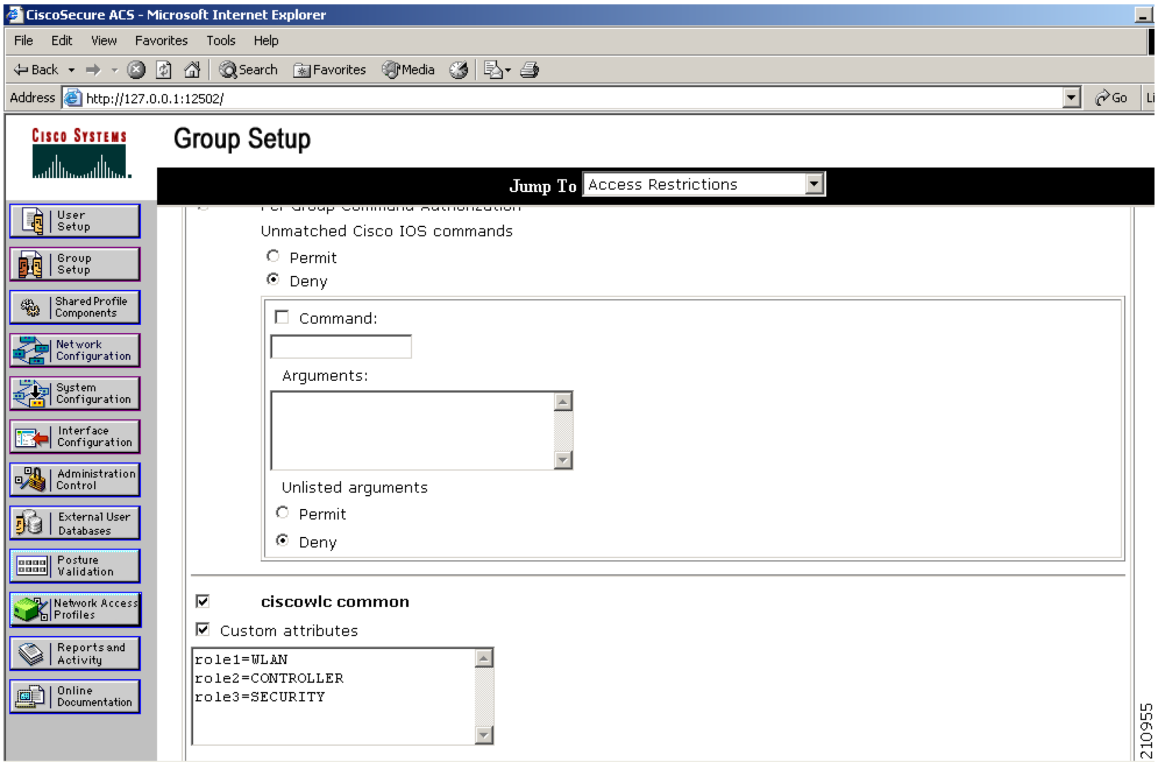
Step 17 Click **Group Setup** on the ACS main page.

Step 18 Choose a previously created group from the Group drop-down box.

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 (see Figure 5-8).

Figure 5-8 Group Setup Page on CiscoSecure ACS



Unmatched Cisco IOS commands
○ Permit
● Deny

□ Command:

Arguments:

Unlisted arguments
○ Permit
● Deny

☑ ciscowlc common
☑ Custom attributes

```
role1=WLAN
role2=CONTROLLER
role3=SECURITY
```

Step 20 Under **TACACS+ Settings**, check the **ciscowlc common** check box.

Step 21 Check 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. As mentioned previously, 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*x*=*ROLE*

For example, to specify the WLAN, CONTROLLER, and SECURITY roles for a particular user group, you would enter the following text:

```
role1=WLAN
role2=CONTROLLER
role3=SECURITY
```

To give a user group access to all seven roles, you would enter the following text:

```
role1=ALL
```

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.

Using the GUI to Configure TACACS+

Follow these steps to configure TACACS+ through the controller GUI.

Step 1 Click **Security** > **AAA** > **TACACS+**.

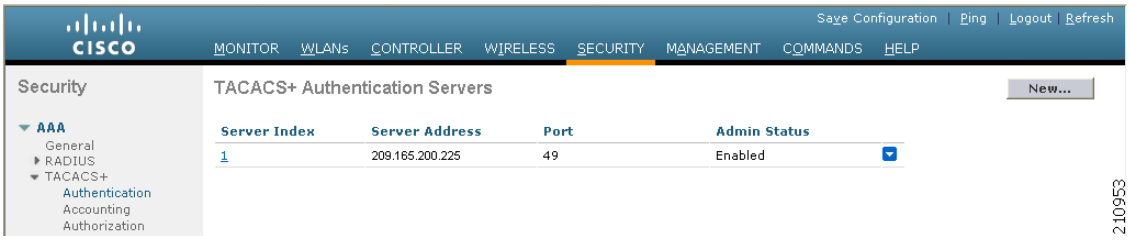
Step 2 Perform one of the following:

- If you want to configure a TACACS+ server for authentication, click **Authentication**.
- If you want to configure a TACACS+ server for authorization, click **Authorization**.
- If you want to configure a TACACS+ server for accounting, click **Accounting**.

Note The GUI pages used to configure authentication, authorization, and accounting all contain the same fields. 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 TACACS+ (Authentication, Authorization, or Accounting) Servers page appears (see Figure 5-9).

Figure 5-9 TACACS+ Authentication Servers Page



TACACS+ Authentication Servers

Server Index	Server Address	Port	Admin Status
1	209.165.200.225	49	Enabled

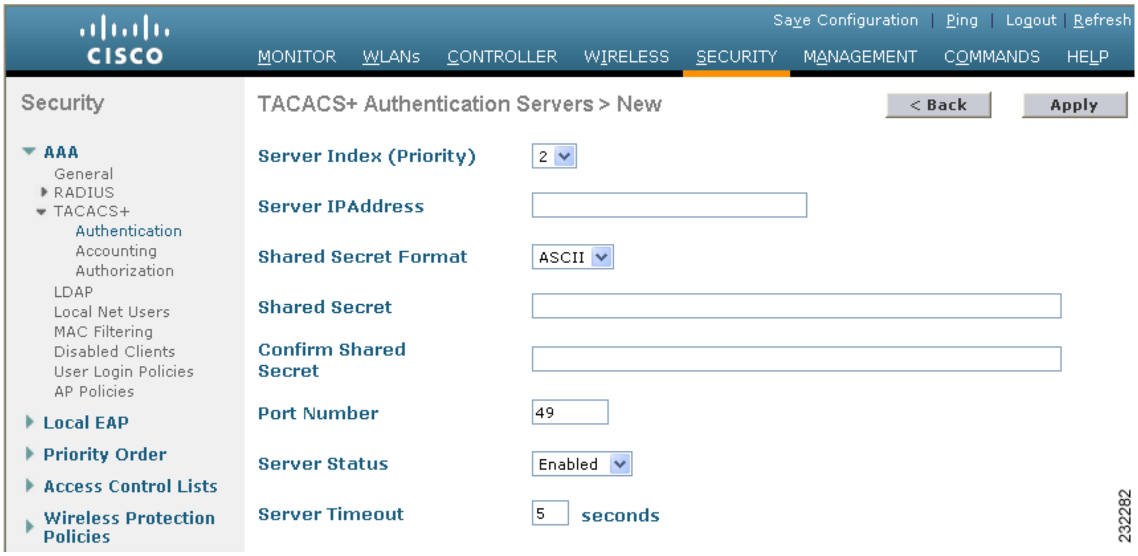
This page lists any TACACS+ servers that have already been configured.

- 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 (see Figure 5-10).

Figure 5-10 TACACS+ Authentication Servers > New Page



TACACS+ Authentication Servers > New

Server Index (Priority): 2

Server IPAddress:

Shared Secret Format: ASCII

Shared Secret:

Confirm Shared Secret:

Port Number: 49

Server Status: Enabled

Server Timeout: 5 seconds

Step 4 If you are adding a new server, choose a number from the Server Index (Priority) drop-down box 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 field.

Step 6 From the Shared Secret Format drop-down box, 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 fields, 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 field. The valid range is 1 to 65535, and the default value is 49.

Step 9 From the Server Status field, choose **Enabled** to enable this TACACS+ server or choose **Disabled** to disable it. The default value is Enabled.

Step 10 In the Server Timeout field, enter the number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

Note Cisco recommends 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.

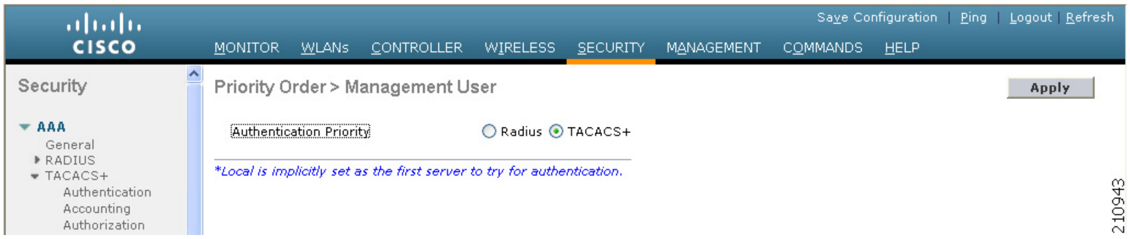
Step 11 Click **Apply** to commit your changes.

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 To specify the order of authentication when multiple databases are configured, click **Security** > **Priority Order** > **Management User**. The Priority Order > Management User page appears (see Figure 5-11).

Figure 5-11 Priority Order > Management User Page



Priority Order > Management User

Authentication Priority ○ Radius ● TACACS+

Local is implicitly set as the first server to try for authentication.

Step 15 For Authentication Priority, choose either **Radius** or **TACACS+** to specify which server has priority over the other when the controller attempts to authenticate management users. By default, the local database is always queried first. If the username is not found, the controller switches to the TACACS+ server if configured for TACACS+ or to the RADIUS server if configured for Radius. 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.

Using the CLI to Configure TACACS+

Use the commands in this section to configure TACACS+ through the controller CLI.

Note Refer to the "Using the GUI to Configure TACACS+" section on page 5-23 for the valid ranges and default values of the parameters used in the CLI commands.

1. Use these commands to configure a TACACS+ authentication server:
   - **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 retransmission timeout value for a TACACS+ authentication server.

2. Use these commands to configure a TACACS+ authorization server:
   - **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 retransmission timeout value for a TACACS+ authorization server.
3. Use these commands to configure a TACACS+ accounting server:
   - **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.
4. Use these commands to see TACACS+ statistics:
   - **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.

   For example, information similar to the following appears for the **show tacacs summary** command:

```
Authentication Servers

Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
1    11.11.12.2        49      Enabled   5
2    11.11.13.2        49      Enabled   5
3    11.11.14.2        49      Enabled   5

Authorization Servers

Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
1    11.11.12.2        49      Enabled   5
2    11.11.13.2        49      Enabled   5
3    11.11.14.2        49      Enabled   5

Accounting Servers

Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
1    11.11.12.2        49      Enabled   5
2    11.11.13.2        49      Enabled   5
3    11.11.14.2        49      Enabled   5
```

Information similar to the following appears for the **show tacacs auth stats** command:

```
Server Index................................... 1
Server Address................................. 10.10.10.10
Msg Round Trip Time............................ 0 (msec)
First Requests................................. 0
Retry Requests................................. 0
Accept Responses............................... 0
Reject Responses............................... 0
Error Responses................................ 0
Restart Responses.............................. 0
Follow Responses............................... 0
GetData Responses.............................. 0
Encrypt no secret Responses.................... 0
Challenge Responses............................ 0
Malformed Msgs................................. 0
Bad Authenticator Msgs......................... 0
Pending Requests............................... 0
Timeout Requests............................... 0
Unknowntype Msgs............................... 0
Other Drops....................................0
```

5. To clear the statistics for one or more TACACS+ servers, enter this command:

   clear stats tacacs [**auth** | **athr** | **acct**] {*index* | **all**}

6. To configure the order of authentication when multiple databases are configured, enter this command. The default setting is local and then radius.

   config aaa auth mgmt [**radius** | **tacacs**]

   To see the current management authentication server order, enter this command:

   show aaa auth

   Information similar to the following appears:

```
Management authentication server order:
   1.......................................... local
   2....................................... tacacs
```

7. To make sure the controller can reach the TACACS+ server, enter this command:

   ping *server_ip_address*

8. To enable or disable TACACS+ debugging, enter this command:

   debug aaa tacacs {**enable** | **disable**}

9. To save your changes, enter this command:

   save config

Viewing the TACACS+ Administration Server Logs

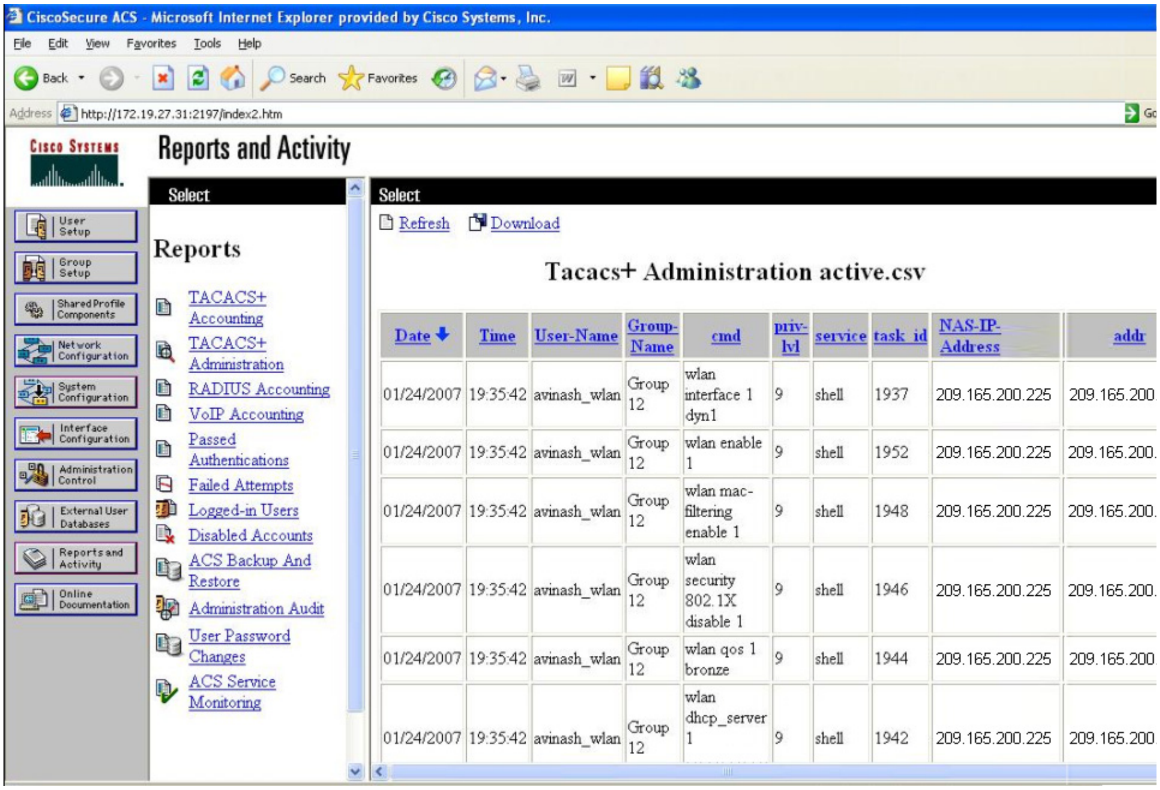
Follow these steps to view the TACACS+ administration server logs, if you have a TACACS+ accounting server configured on the controller.

Step 1 Click **Reports and Activity** on the ACS main page.

Step 2 Click **TACACS+ Administration**.

Step 3 Click the .csv file corresponding to the date of the logs you wish to view. The TACACS+ Administration .csv page appears (see Figure 5-12).

Figure 5-12 TACACS+ Administration .csv Page on CiscoSecure ACS



Tacacs+ Administration active.csv

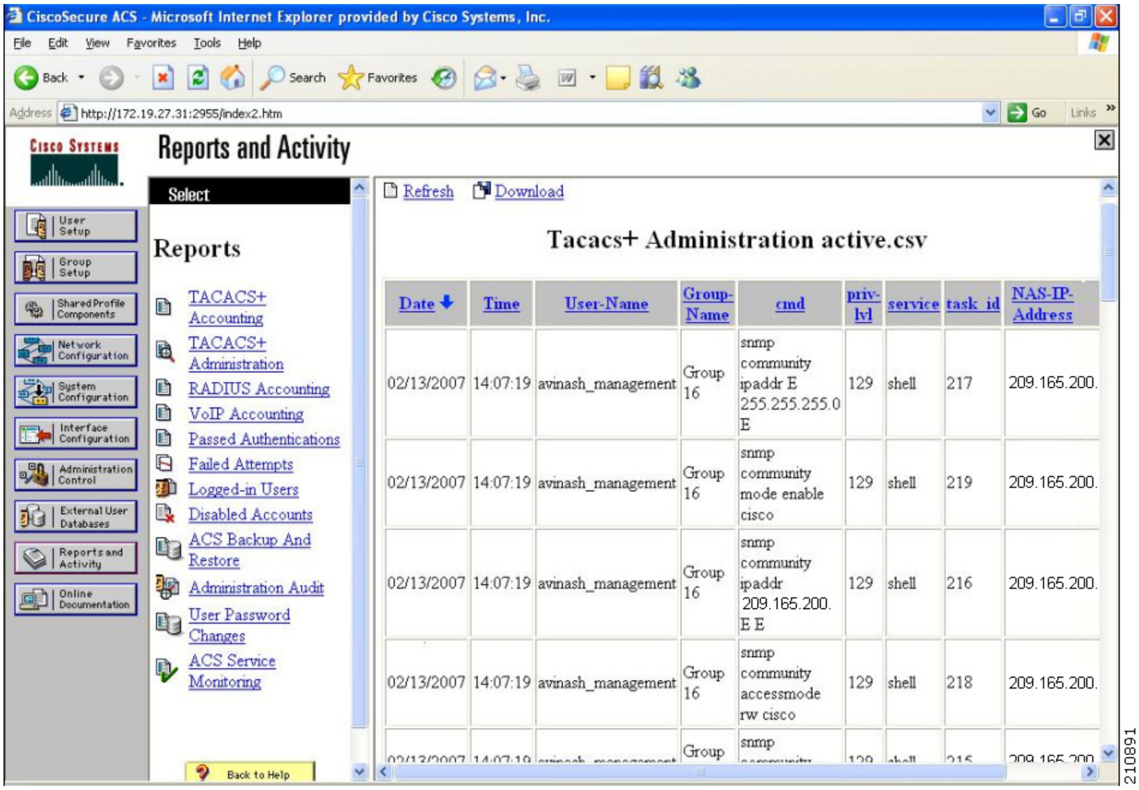
Date	Time	User-Name	Group-Name	cmd	priv-lvl	service	task_id	NAS-IP-Address	addr
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan interface 1 dyn1	9	shell	1937	209.165.200.225	209.165.200
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan enable 1	9	shell	1952	209.165.200.225	209.165.200.
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan mac-filtering enable 1	9	shell	1948	209.165.200.225	209.165.200.
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan security 802.1X disable 1	9	shell	1946	209.165.200.225	209.165.200.
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan qos 1 bronze	9	shell	1944	209.165.200.225	209.165.200
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan dhcp_server 1	9	shell	1942	209.165.200.225	209.165.200

This page provides the following information:

- The date and time the action was taken
- The name and assigned role of the user who took the action
- The group to which the user belongs
- The specific action that the user took
- The privilege level of the user who executed the action
- The IP address of the controller
- The 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 the user enters 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 maybe logged while the IP address and community name are logged as "E." See the first and third lines in the example in Figure 5-13.

Figure 5-13 TACACS+ Administration .csv Page on CiscoSecure ACS



Tacacs+ Administration active.csv

Date	Time	User-Name	Group-Name	cmd	priv-lvl	service	task_id	NAS-IP-Address
02/13/2007	14:07:19	avinash_management	Group 16	snmp community ipaddr E 255.255.255.0 E	129	shell	217	209.165.200.
02/13/2007	14:07:19	avinash_management	Group 16	snmp community mode enable cisco	129	shell	219	209.165.200.
02/13/2007	14:07:19	avinash_management	Group 16	snmp community ipaddr 209.165.200. E E	129	shell	216	209.165.200.
02/13/2007	14:07:19	avinash_management	Group 16	snmp community accessmode rw cisco	129	shell	218	209.165.200.
02/13/2007	14:07:19	avinash_management	Group	snmp	129	shell	215	209.165.200.

Note You can click **Refresh** at any time to refresh this page.

Configuring Local Network Users

This section explains how to 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. Refer to the "Configuring Local EAP" section on page 5-38 for more information.

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.

You can configure local network users through either the GUI or the CLI.

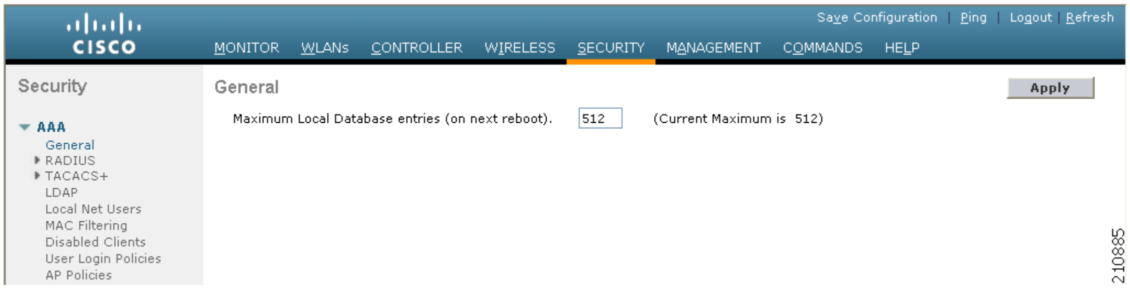
Using the GUI to Configure Local Network Users

Follow these steps to configure local network users using the controller GUI.

Step 1 Follow these steps to specify the maximum number of local network users that can exist on the local user database:

a. Click **Security** > **AAA** > **General** to open the General page (see Figure 5-14).

Figure 5-14 General Page



General

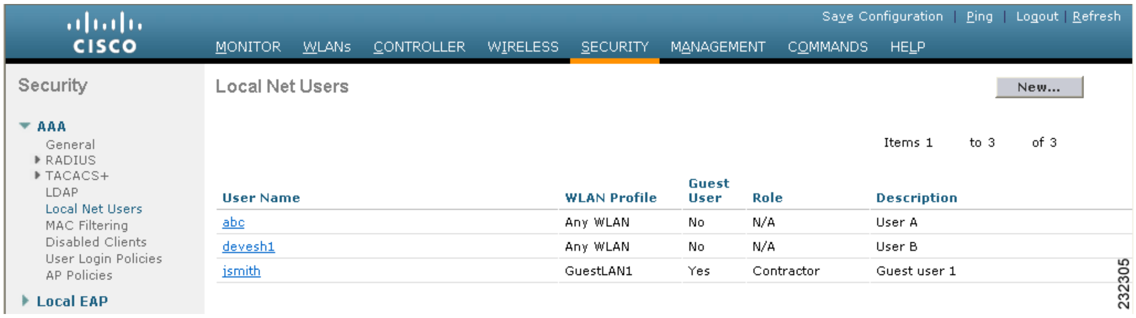
Maximum Local Database entries (on next reboot). 512 (Current Maximum is 512)

b. In the Maximum Local Database Entries field, enter a value for the maximum number of local network users that can be added to the local user database the next time the controller reboots. The currently configured value appears in parentheses to the right of the field. The valid range is 512 to 2048, and the default setting is 512.

c. Click **Apply** to commit your changes.

Step 2 Click **Security** > **AAA** > **Local Net Users** to open the Local Net Users page (see Figure 5-15).

Figure 5-15 Local Net Users Page



Local Net Users

Items 1 to 3 of 3

User Name	WLAN Profile	Guest User	Role	Description
abc	Any WLAN	No	N/A	User A
devesh1	Any WLAN	No	N/A	User B
jsmith	GuestLAN1	Yes	Contractor	Guest user 1

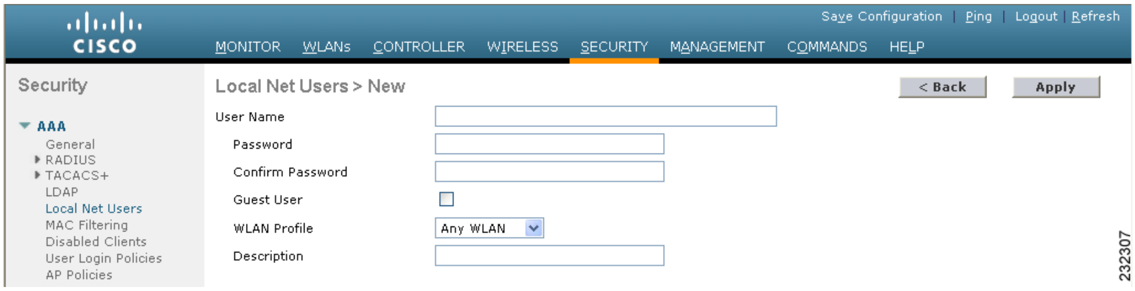
This page lists any local network users that have already been configured. It also specifies any guest users and the QoS role to which they are assigned (if applicable). See the "Configuring Quality of Service Roles" section on page 4-48 for information on configuring QoS roles.

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 3 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 (see Figure 5-16).

Figure 5-16 Local Net Users > New Page



Local Net Users > New

User Name	
Password	
Confirm Password	
Guest User	□
WLAN Profile	Any WLAN
Description	

Step 4 If you are adding a new user, enter a username for the local user in the User Name field. 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 5 In the Password and Confirm Password fields, enter a password for the local user. You can enter up to 24 alphanumeric characters.

Step 6 If you are adding a new user, check 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 unchecked.

Step 7 If you are adding a new user and you checked the Guest User check box, enter the amount of time (in seconds) that the guest user account is to remain active in the Lifetime field. The valid range is 60 to 2,592,000 seconds (30 days) inclusive, and the default setting is 86,400 seconds.

Step 8 If you are adding a new user, you checked the Guest User check box, and you want to assign a QoS role to this guest user, check the **Guest User Role** check box. The default setting is unchecked.

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 9 If you are adding a new user and you checked the Guest User Role check box, choose the QoS role that you want to assign to this guest user from the Role drop-down box.

Note If you want to create a new QoS role, see the "Configuring Quality of Service Roles" section on page 4-48 for instructions.

Step 10 From the WLAN Profile drop-down box, 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 11 In the Description field, enter a descriptive title for the local user (such as "User 1").

Step 12 Click **Apply** to commit your changes.

Step 13 Click **Save Configuration** to save your changes.

Using the CLI to Configure Local Network Users

Use the commands in this section to configure local network users using the controller CLI.

Note Refer to the "Using the GUI to Configure Local Network Users" section on page 5-30 for the valid ranges and default values of the parameters used in the CLI commands.

1. Use these commands to configure a local network user:

   - **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 guest lifetime** *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.

2. Use these commands to see information related to the local network users configured on the controller.

   - **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.

   For example, information similar to the following appears for the **show netuser detail** *username* command:

```
User Name............................... abc
WLAN Id................................. Any
Lifetime................................ Permanent
Description.......................... test user
```

3. To save your changes, enter this command:

   save config

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. 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. Refer to the "Configuring Local EAP" section on page 5-38 for more information.

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. For example, Microsoft Active Directory is not supported because it does not return a clear-text password. If the LDAP server cannot be configured to return a clear-text password, LEAP, EAP-FAST/MSCHAPv2, and PEAPv0/MSCHAPv2 are not supported.

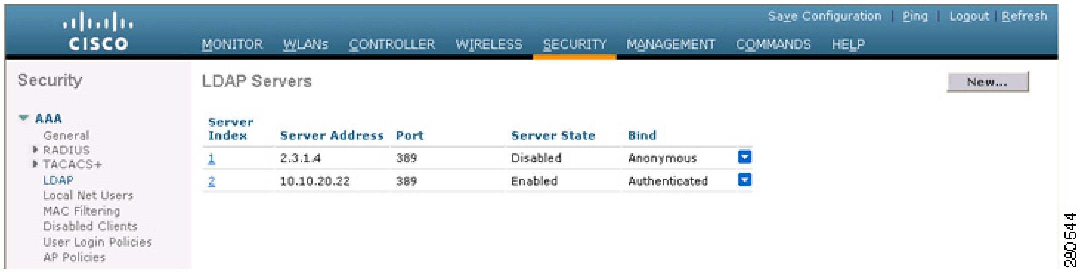
You can configure LDAP through either the GUI or the CLI.

Using the GUI to Configure LDAP

Follow these steps to configure LDAP using the controller GUI.

Step 1 Click **Security** > **AAA** > **LDAP** to open the LDAP Servers page (see Figure 5-17).

Figure 5-17 LDAP Servers Page



Server Index	Server Address	Port	Server State	Bind
1	2.3.1.4	389	Disabled	Anonymous
2	10.10.20.22	389	Enabled	Authenticated

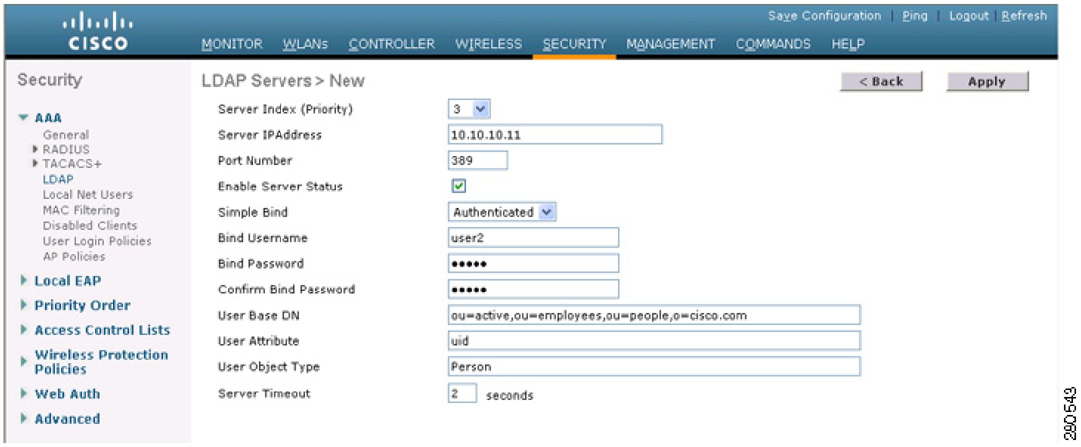
This page lists any LDAP servers that have already been configured.

- 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 (see Figure 5-18).

Figure 5-18 LDAP Servers > New Page



LDAP Servers > New

Server Index (Priority)	3
Server IPAddress	10.10.10.11
Port Number	389
Enable Server Status	☑
Simple Bind	Authenticated
Bind Username	user2
Bind Password	•••••
Confirm Bind Password	•••••
User Base DN	ou=active,ou=employees,ou=people,o=cisco.com
User Attribute	uid
User Object Type	Person
Server Timeout	2 seconds

Step 3 If you are adding a new server, choose a number from the Server Index (Priority) drop-down box to specify the priority order of this server in relation to any other configured LDAP servers. You can configure up to seventeen servers. If the controller cannot reach the first server, it tries the second one in the list and so on.

Step 4 If you are adding a new server, enter the IP address of the LDAP server in the Server IP Address field.

Step 5 If you are adding a new server, enter the LDAP server's TCP port number in the Port Number field. The valid range is 1 to 65535, and the default value is 389.

Step 6 Check the **Enable Server Status** check box to enable this LDAP server or uncheck it to disable it. The default value is disabled.

Step 7 From the Simple Bind drop-down box, 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 whereas the Authenticated method requires that a username and password be entered to secure access. The default value is Anonymous.

Step 8 If you chose Authenticated in Step 7, follow these steps:

a. In the Bind Username field, 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 therefore 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 fields, enter a password to be used for local authentication to the LDAP server. The password can contain up to 32 characters.

Step 9 In the User Base DN field, 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 10 In the User Attribute field, enter the name of the attribute in the user record that contains the username. You can obtain this attribute from your directory server.

Step 11 In the User Object Type field, 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 12 In the Server Timeout field, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

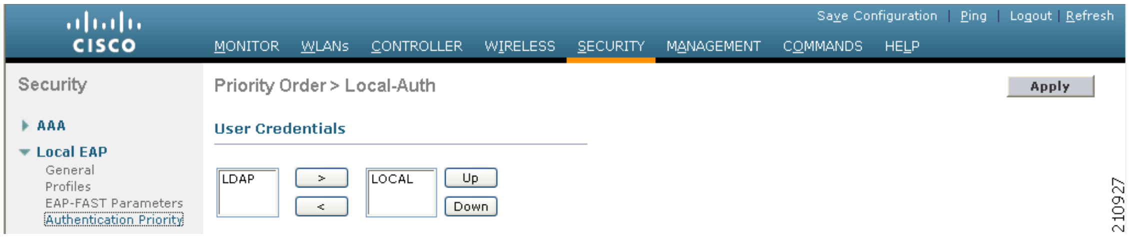
Step 13 Click **Apply** to commit your changes.

Step 14 Click **Save Configuration** to save your changes.

Step 15 Follow these steps to specify LDAP as the priority backend database server for local EAP authentication:

a. Click **Security** > **Local EAP** > **Authentication Priority** to open the Priority Order > Local-Auth page (see Figure 5-19).

Figure 5-19 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.

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.

e. Click **Save Configuration** to save your changes.

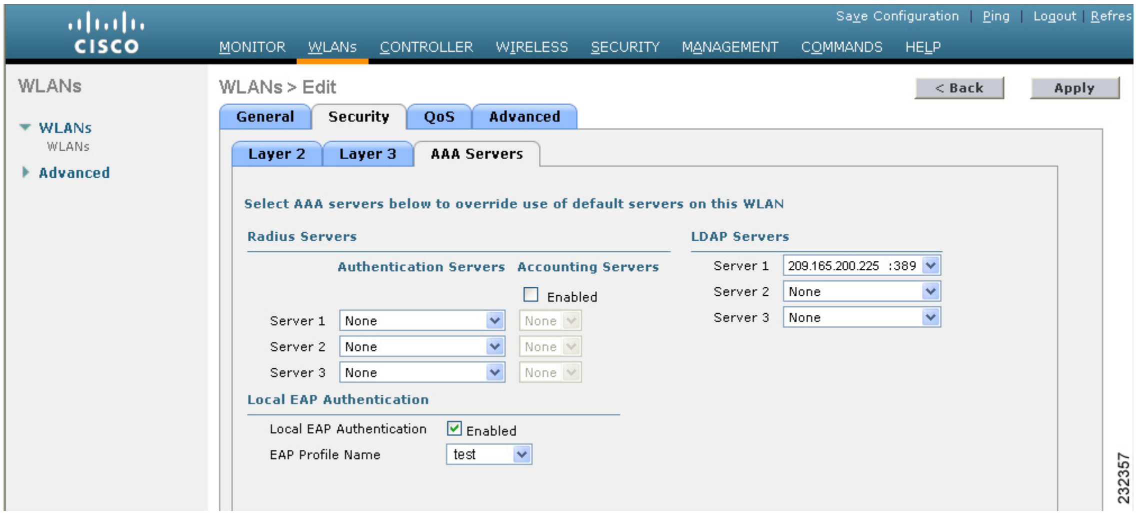
Step 16 (Optional) Follow these steps if you wish to assign specific LDAP servers to a WLAN.

a. Click **WLANs** to open the WLANs page.

b. Click the ID number of the desired WLAN.

c. When the WLANs > Edit page appears, click the **Security** > **AAA Servers** tabs to open the WLANs > Edit (Security > AAA Servers) page (see Figure 5-20).

Figure 5-20 WLANs > Edit (Security > AAA Servers) Page


Save Configuration | Ping | Logout | Refres
cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General Security QoS Advanced
Layer 2 Layer 3 AAA Servers
232357

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

	Authentication Servers	Accounting Servers
		□ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None

LDAP Servers

Server 1	209.165.200.225 :389
Server 2	None
Server 3	None

Local EAP Authentication

Local EAP Authentication ☑ Enabled

EAP Profile Name test

d. From the LDAP Servers drop-down boxes, 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.

Using the CLI to Configure LDAP

Use the commands in this section to configure LDAP using the controller CLI.

Note Refer to the "Using the GUI to Configure LDAP" section on page 5-33 for the valid ranges and default values of the parameters used in the CLI commands.

1. Use these commands to configure an LDAP server:
   - **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 therefore 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.

2. Use this command to specify LDAP as the priority backend database server:

   config local-auth user-credentials ldap

   Note If you enter **config local-auth user-credentials ldap local**, 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 **config local-auth user-credentials local ldap**, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.

3. (Optional) Use these commands if you wish to assign specific LDAP servers to a WLAN:

   - **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.

4. Use these commands to view information pertaining to configured LDAP servers:

   - **show ldap summary**—Shows a summary of the configured LDAP servers.
   - **show ldap** *index*—Shows detailed LDAP server information.
   - **show ldap statistics**—Shows LDAP server statistics.
   - **show wlan** *wlan_id*—Shows the LDAP servers that are applied to a WLAN.

   For example, information similar to the following appears for the **show ldap** *index* command:

```
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
```

Information similar to the following appears for the **show ldap summary** command:

```
Idx  Server Address   Port  Enabled
---  ---------------  ----  -------
1    2.3.1.4          389  No
2    10.10.20.22     389   Yes
```

Information similar to the following appears for the **show ldap statistics** command:

```
Server Index.................................... 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
...
```

5. To make sure the controller can reach the LDAP server, enter this command:

   ping *server_ip_address*

6. To save your changes, enter this command:

   save config

7. To enable or disable debugging for LDAP, enter this command:

   debug aaa ldap {**enable** | **disable**}

Configuring 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, thereby removing 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.

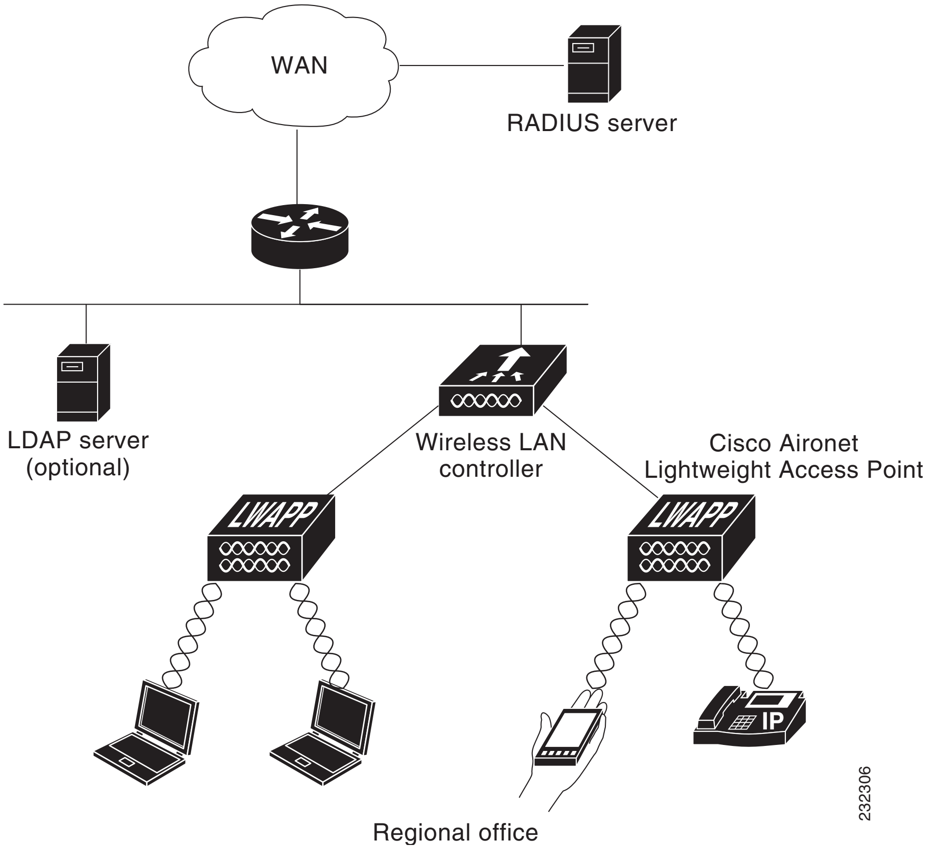
Note The LDAP backend database supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC. LEAP, EAP-FAST/MSCHAPv2, and PEAPv0/MSCHAPv2 are also supported but only if the LDAP server is set up to return a clear-text password. For example, Microsoft Active Directory is not supported because it does not return a clear-text password. If the LDAP server cannot be configured to return a clear-text password, LEAP, EAP-FAST/MSCHAPv2, and PEAPv0/MSCHAPv2 are not supported.

Note 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 then 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
```

Figure 5-21 provides an example of a remote office using local EAP.

Figure 5-21 Local EAP Example



You can configure local EAP through either the GUI or the CLI.

Using the GUI to Configure Local EAP

Follow these steps to configure local EAP using the controller GUI.

Step 1 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 wish to use your own vendor-specific certificates, they must be imported on the controller. If you are configuring local EAP to use one of these EAP types, make sure that the appropriate certificates and PACs (if you will use manual PAC provisioning) have been imported on the controller. Refer to Chapter 9 for instructions on importing certificates and PACs.

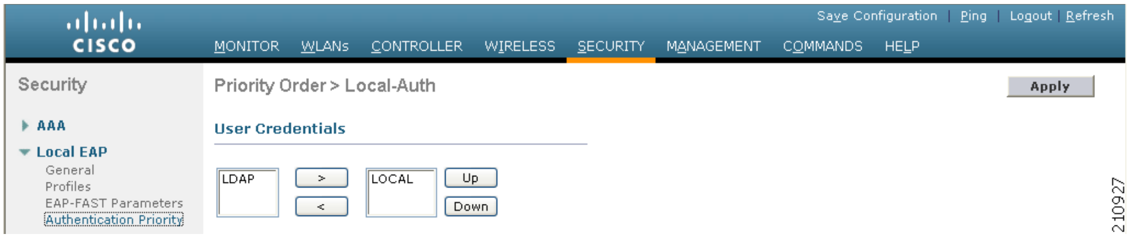
Step 2 If you want the controller to retrieve user credentials from the local user database, make sure that you have properly configured the local network users on the controller. See the "Configuring Local Network Users" section on page 5-29 for instructions.

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. See the "Configuring LDAP" section on page 5-33 for instructions.

Step 4 Follow these steps to specify the order in which user credentials are retrieved from the backend database servers:

a. Click **Security** > **Local EAP** > **Authentication Priority** to open the Priority Order > Local-Auth page (see Figure 5-22).

Figure 5-22 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.

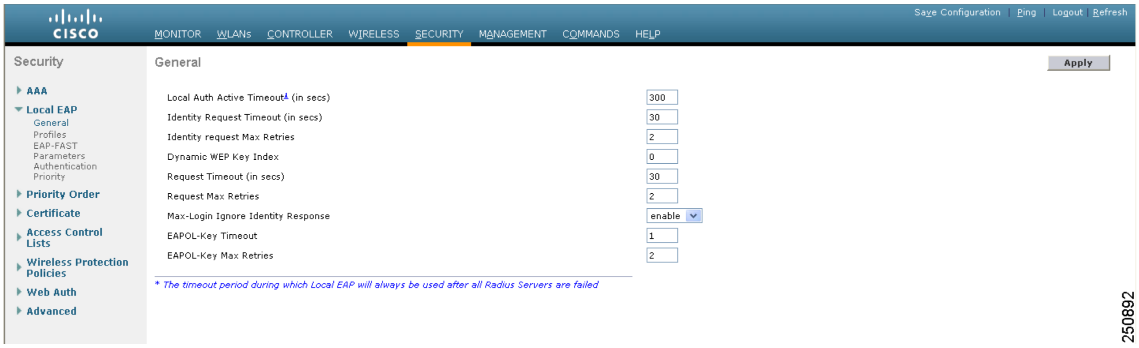
Note If both LDAP and LOCAL appear in the right User Credentials box with LDAP on the top and LOCAL on the bottom, local EAP attempts to authenticate clients using the LDAP backend database and fails over to the local user database if the LDAP servers are not reachable. If the user is not found, the 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 Follow these steps to specify values for the local EAP timers:

a. Click **Security** > **Local EAP** > **General** to open the General page (see Figure 5-23).

Figure 5-23 General Page



General

Local Auth Active Timeout[1] (in secs)	300
Identity Request Timeout (in secs)	30
Identity request Max Retries	2
Dynamic WEP Key Index	0
Request Timeout (in secs)	30
Request Max Retries	2
Max-Login Ignore Identity Response	enable
EAPOL-Key Timeout	1
EAPOL-Key Max Retries	2

* *The timeout period during which Local EAP will always be used after all Radius Servers are failed*

b. In the Local Auth Active Timeout field, 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 field, 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 field, 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 field, enter the key index used for dynamic wired equivalent privacy (WEP). The default setting is 0.

f. In the Request Timeout field, 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 field, 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 box, 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 field, 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.

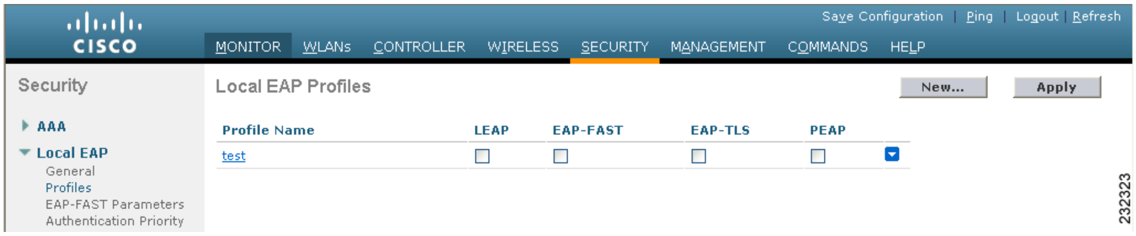
j. In the EAPOL-Key Max Retries field, enter the maximum number of times that the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 0 to 4 retries, and the default setting is 2 retries.

k. Click **Apply** to commit your changes.

Step 6 Follow these steps to create a local EAP profile, which specifies the EAP authentication types that are supported on the wireless clients:

a. Click **Security** > **Local EAP** > **Profiles** to open the Local EAP Profiles page (see Figure 5-24).

Figure 5-24 Local EAP Profiles Page



Local EAP Profiles

Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP	
test	□	□	□	□	▾

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**.

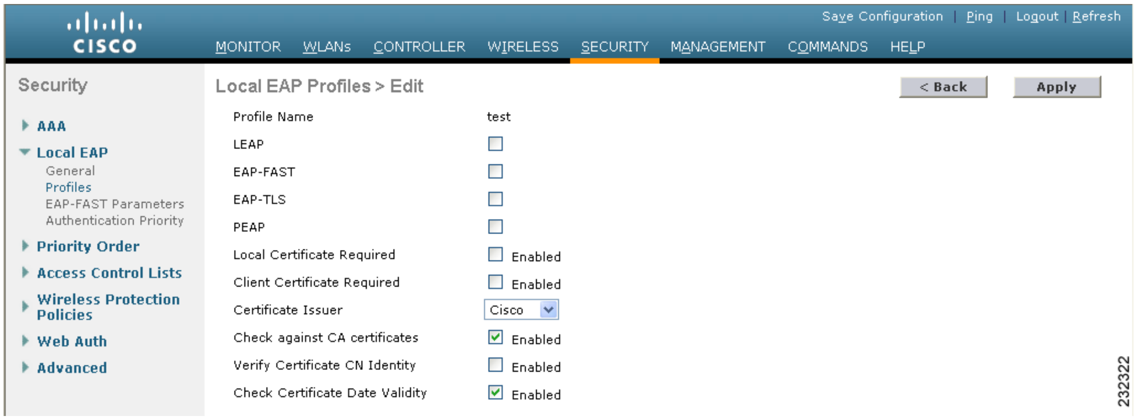
b. Click **New** to open the Local EAP Profiles > New page.

c. In the Profile Name field, enter a name 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 (see Figure 5-25).

Figure 5-25 Local EAP Profiles > Edit Page



Local EAP Profiles > Edit

Profile Name	test
LEAP	□
EAP-FAST	□
EAP-TLS	□
PEAP	□
Local Certificate Required	□ Enabled
Client Certificate Required	□ Enabled
Certificate Issuer	Cisco ▾
Check against CA certificates	☑ Enabled
Verify Certificate CN Identity	□ Enabled
Check Certificate Date Validity	☑ Enabled

e. Check the **LEAP**, **EAP-FAST**, **EAP-TLS**, and/or **PEAP** check boxes to specify the EAP type(s) 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 check 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, check the **Local Certificate Required** check box. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unchecked, 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.

g. If you chose EAP-FAST and want the wireless clients to send their device certificates to the controller in order to authenticate, check the **Client Certificate Required** check box. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unchecked, which is the default setting.

Note This option applies only to EAP-FAST because client certificates are not used with LEAP or PEAP and are mandatory for EAP-TLS.

h. If you chose EAP-FAST with certificates, EAP-TLS, or PEAP, choose which certificates will be sent to the client, the ones from **Cisco** or the ones from another **Vendor**, from the Certificate Issuer drop-down box. The default setting is Cisco.

i. If you chose EAP-FAST with certificates or EAP-TLS and want the incoming certificate from the client to be validated against the CA certificates on the controller, check the **Check Against CA Certificates** check box. The default setting is enabled.

j. If you chose EAP-FAST with certificates or EAP-TLS and want the common name (CN) in the incoming certificate to be validated against the CA certificates' CN on the controller, check the **Verify Certificate CN Identity** check box. The default setting is disabled.

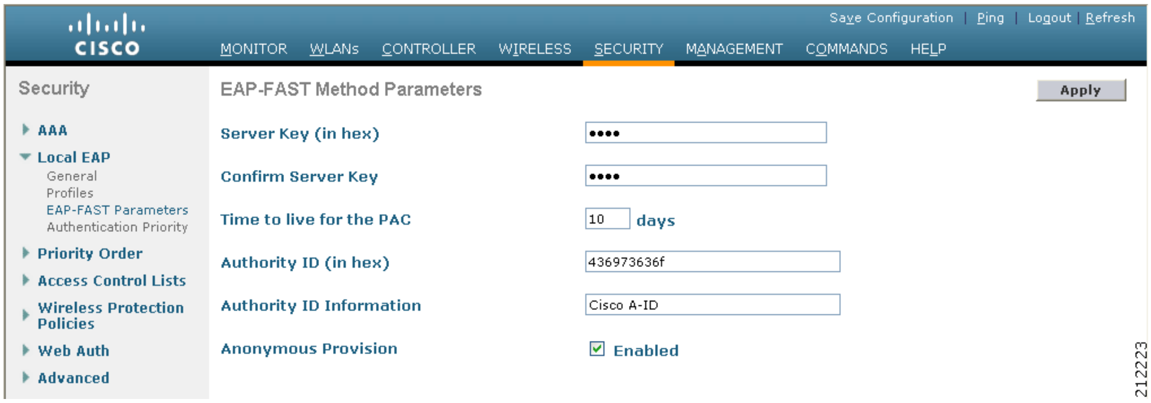
k. If you chose EAP-FAST with certificates or EAP-TLS and want the controller to verify that the incoming device certificate is still valid and has not expired, check the **Check Certificate Date Validity** check box. The default setting is enabled.

l. Click **Apply** to commit your changes.

Step 7 If you created an EAP-FAST profile, follow these steps to configure the EAP-FAST parameters:

a. Click **Security** > **Local EAP** > **EAP-FAST Parameters** to open the EAP-FAST Method Parameters page (see Figure 5-26).

Figure 5-26 EAP-FAST Method Parameters Page



EAP-FAST Method Parameters

Server Key (in hex) ••••

Confirm Server Key ••••

Time to live for the PAC 10 days

Authority ID (in hex) 436973636f

Authority ID Information Cisco A-ID

Anonymous Provision ☑ Enabled

b. In the Server Key and Confirm Server Key fields, enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.

c. In the Time to Live for the PAC field, 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 field, 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 field, enter the authority identifier of the local EAP-FAST server in text format.

f. If you want to enable anonymous provisioning, check 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, uncheck the **Anonymous Provision** check box.

g. Click **Apply** to commit your changes.

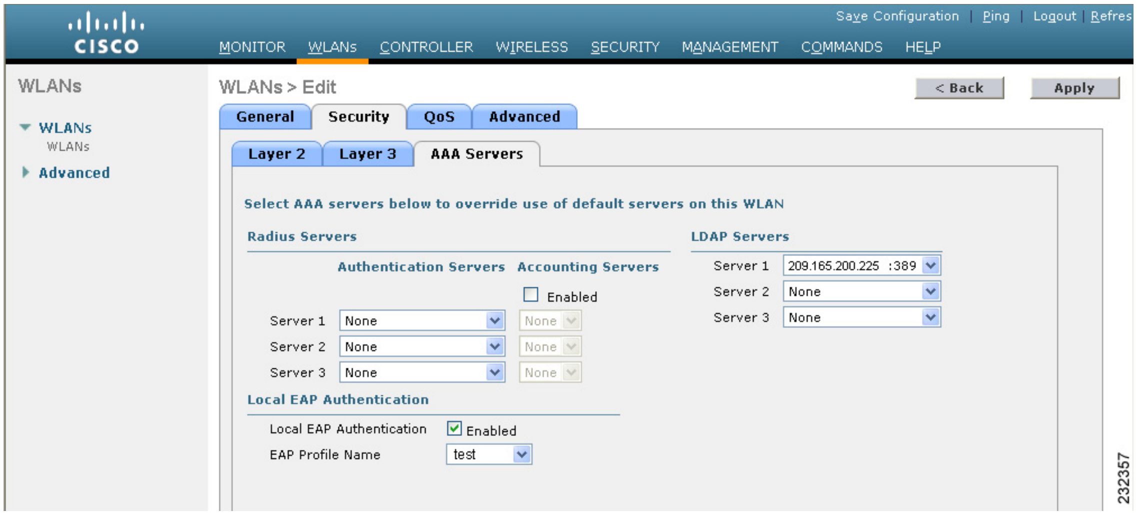
Step 8 Follow these steps to enable local EAP on a WLAN:

a. Click **WLANs** to open the WLANs page.

b. Click the ID number of the desired WLAN.

c. When the WLANs > Edit page appears, click the **Security** > **AAA Servers** tabs to open the WLANs > Edit (Security > AAA Servers) page (see Figure 5-27).

Figure 5-27 WLANs > Edit (Security > AAA Servers) Page


Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
232357

WLANs > Edit

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

	Authentication Servers	Accounting Servers
		□ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None

LDAP Servers

Server 1	209.165.200.225 :389
Server 2	None
Server 3	None

Local EAP Authentication

Local EAP Authentication ☑ Enabled

EAP Profile Name test

d. Check the **Local EAP Authentication** check box to enable local EAP for this WLAN.

e. From the EAP Profile Name drop-down box, choose the EAP profile that you want to use for this WLAN.

f. If desired, choose the LDAP server(s) that you want to use with local EAP on this WLAN from the LDAP Servers drop-down boxes.

g. Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your changes.

Using the CLI to Configure Local EAP

Follow these steps to configure local EAP using the controller CLI.

Note Refer to the "Using the GUI to Configure Local EAP" section on page 5-40 for the valid ranges and default values of the parameters used in the CLI commands.

Step 1 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 wish to use your own vendor-specific certificates, they must be imported on the controller. If you are configuring local EAP to use one of these EAP types, make sure that the appropriate certificates and PACs (if you will use manual PAC provisioning) have been imported on the controller. Refer to Chapter 9 for instructions on importing certificates and PACs.

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. See the "Configuring Local Network Users" section on page 5-29 for instructions.

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. See the "Configuring LDAP" section on page 5-33 for instructions.

Step 4 To specify the order in which user credentials are retrieved from the local and/or LDAP databases, enter this command:

config local-auth user-credentials {**local** | **ldap**}

Note If you enter **config local-auth user-credentials ldap local**, 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 **config local-auth user-credentials local ldap**, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.

Step 5 To specify values for the local EAP timers, enter 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 setting is 0.
- **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 To create a local EAP profile, enter 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 this command: **config local-auth eap-profile delete** *profile_name*.

Step 7 To add an EAP method to a local EAP profile, enter 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 this command: **config local-auth eap-profile method delete** *method profile_name*.

Step 8 To configure EAP-FAST parameters if you created an EAP-FAST profile, enter 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 To configure certificate parameters per profile, enter 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 To enable local EAP and attach an EAP profile to a WLAN, enter this command:

config wlan local-auth enable *profile_name wlan_id*

Note To disable local EAP for a WLAN, enter this command: **config wlan local-auth disable** *wlan_id.*

Step 11 To save your changes, enter this command:

save config

Step 12 To view information pertaining to local EAP, enter these commands:

- **show local-auth config—**Shows the local EAP configuration on the controller.

  Information similar to the following appears for the **show local-auth config** command:

```
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 .............................. 436973636f0000000000000000000000
     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.
- **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. Information similar to the following appears:

```
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. Information similar to the following appears:

```
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
   EAP Request Msg Timeouts Failures............. 0
   EAP Key Msg Timeouts.......................... 3
   EAP Key Msg Timeouts Failures.............. 1
```

- **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. Information similar to the following appears:

```
...
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 If necessary, you can use these commands to troubleshoot local EAP sessions:

- **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.

Configuring the System for SpectraLink NetLink Telephones

For 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.

Use one of these methods to enable long preambles:

- Using the GUI to Enable Long Preambles, page 5-50
- Using the CLI to Enable Long Preambles, page 5-51

Using the GUI to Enable Long Preambles

Use this procedure to use the GUI to enable long preambles to optimize the operation of SpectraLink NetLink phones on your wireless LAN.

Step 1 Click **Wireless** > **802.11b/g/n** > **Network** to open the 802.11b/g Global Parameters page.

Step 2 If the **Short Preamble** check box is checked, continue with this procedure. However, if the **Short Preamble** check box is unchecked (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 Uncheck the **Short Preamble** check box to enable long preambles.

Step 4 Click **Apply** to update the controller configuration.

Note If you do not already have an active CLI session to the controller, Cisco recommends that you start a CLI session to reboot the controller and watch the reboot process. A CLI session is also useful because the GUI loses its connection when the controller reboots.

Step 5 Click **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 Click **Wireless** > **802.11b/g/n** > **Network** to open the 802.11b/g Global Parameters page. If the **Short Preamble** check box is unchecked, the controller is optimized for SpectraLink NetLink phones.

Using the CLI to Enable Long Preambles

Use this procedure to use the CLI to enable long preambles to optimize the operation of SpectraLink NetLink phones on your wireless LAN.

Step 1 Log into the controller CLI.

Step 2 Enter **show 802.11b** and check 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. This example shows that short preambles are disabled:

```
Short Preamble mandatory....................... Disabled
```

Step 3 Enter **config 802.11b disable network** to disable the 802.11b/g network. (You cannot enable long preambles on the 802.11a network.)

Step 4 Enter **config 802.11b preamble long** to enable long preambles.

Step 5 Enter **config 802.11b enable network** to re-enable the 802.11b/g network.

Step 6 Enter **reset system** to reboot the controller. Enter **y** when this prompt appears:

```
The system has unsaved changes. Would you like to save them now? (y/n)
```

The controller reboots.

Step 7 To verify that the controller is properly configured, log back into the CLI and enter **show 802.11b** 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.

Using the CLI to Configure Enhanced Distributed Channel Access

Use this CLI command to configure 802.11 enhanced distributed channel access (EDCA) parameters to support SpectraLink phones:

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 re-enable the 802.11b/g network after entering this command.

Using Management over Wireless

The management over wireless feature allows operators 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.

Before you can use management over wireless, you must properly configure the controller using one of these sections:

- Using the GUI to Enable Management over Wireless, page 5-52
- Using the CLI to Enable Management over Wireless, page 5-52

Using the GUI to Enable Management over Wireless

Step 1 Click **Management** > **Mgmt Via Wireless** to open the Management Via Wireless page.

Step 2 Check the **Enable Controller Management to be accessible from Wireless Clients** check box to enable management over wireless for the WLAN or uncheck it to disable this feature. The default value is unchecked.

Step 3 Click **Apply** to commit your changes.

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

Step 5 Use a wireless client web browser to connect to the controller management port or distribution system port IP address, and log into the controller GUI to verify that you can manage the WLAN using a wireless client.

Using the CLI to Enable Management over Wireless

Step 1 In the CLI, use the **show network** command to verify whether the management over wireless interface is enabled or disabled. If it is disabled, continue with Step 2. Otherwise, continue with Step 3.

Step 2 To enable management over wireless, enter **config network mgmt-via-wireless enable**.

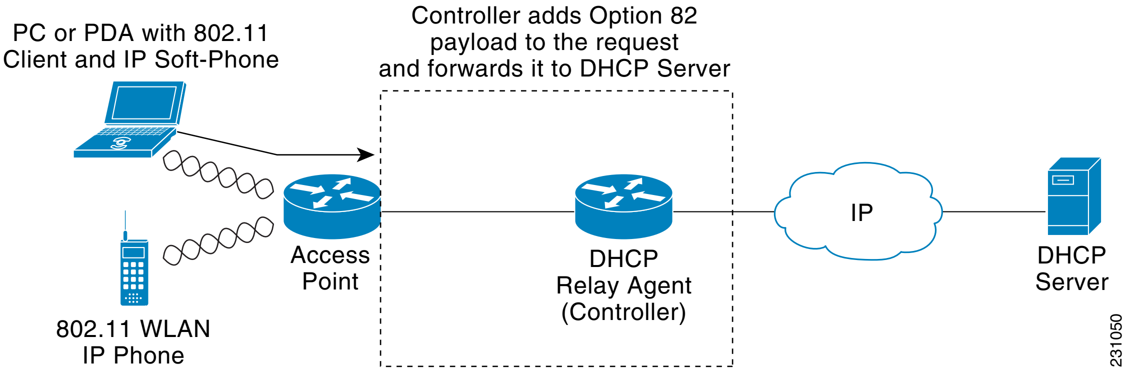
Step 3 Use a wireless client to associate with an access point connected to the controller that you want to manage.

Step 4 Enter **telnet controller-ip-address** and log into the CLI to verify that you can manage the WLAN using a wireless client.

Configuring 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. See Figure 5-28 for an illustration of this process.

Figure 5-28 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.

Note In order for DHCP option 82 to operate correctly, you must enable DHCP proxy, which is disabled by default. Refer to the "Configuring DHCP Proxy" section on page 4-22 for instructions on configuring DHCP proxy.

Note Any DHCP packets that already include a relay agent option are dropped at the controller.

Note DHCP option 82 is not supported for use with auto-anchor mobility, which is described in Chapter 12.

Use these commands to configure DHCP option 82 on the controller.

1. To configure the format of the DHCP option 82 payload, enter 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.
2. To enable or disable DHCP option 82 on the controller, enter this command:

   config interface dhcp ap-manager opt-82 {**enable** | **disable**}
3. To see the status of DHCP option 82 on the controller, enter this command:

   show interface detailed ap-manager

   Information similar to the following appears:

```
Interface Name................................. ap-manager
IP Address..................................... 10.30.16.13
IP Netmask..................................... 255.255.248.0
IP Gateway..................................... 10.30.16.1
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
```

Configuring and Applying 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.

Note If you are using an external web server with a 2100 series controller or the controller network module within a Cisco 28/37/38xx Series Integrated Services Router, you must configure a preauthentication ACL on the WLAN for the external web server.

You can define up to 64 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.

Note 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.

Note ACLs in your network might need to be modified if CAPWAP uses different ports than LWAPP.

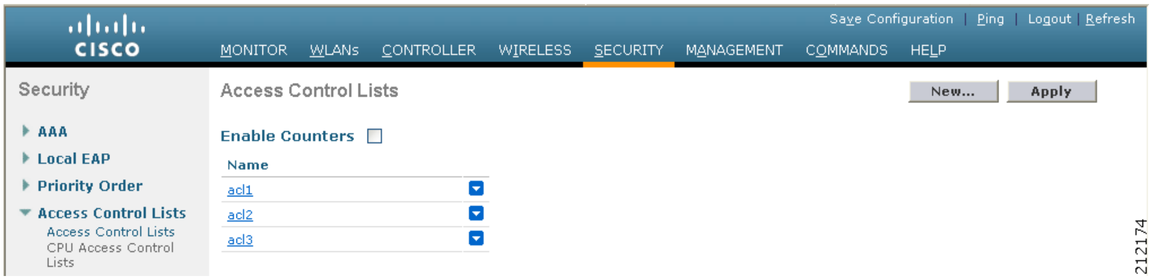
You can configure and apply ACLs through either the GUI or the CLI.

Using the GUI to Configure Access Control Lists

Follow these steps to configure ACLs using the controller GUI.

Step 1 Click **Security** > **Access Control Lists** > **Access Control Lists** to open the Access Control Lists page (see Figure 5-29).

Figure 5-29 Access Control Lists Page



This page lists all of the ACLs 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**.

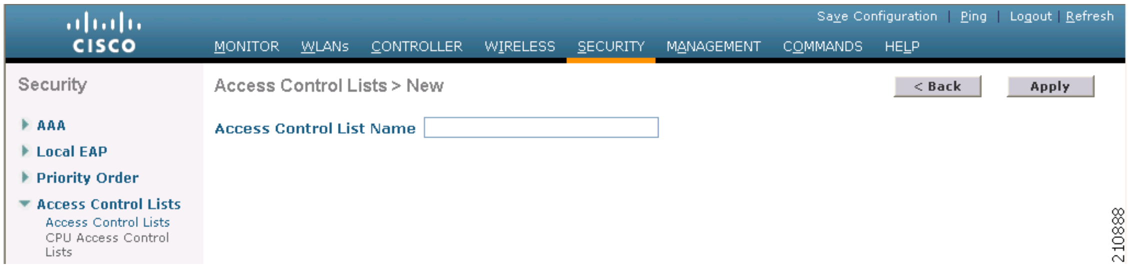
Step 2 If you want to see if packets are hitting any of the ACLs configured on your controller, check the **Enable Counters** check box and click **Apply**. Otherwise, leave the check box unchecked, which is the default value. This feature is useful when troubleshooting your system.

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**.

Note ACL counters are available only on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

Step 3 To add a new ACL, click **New**. The Access Control Lists > New page appears (see Figure 5-30).

Figure 5-30 Access Control Lists > New Page



Access Control Lists > New

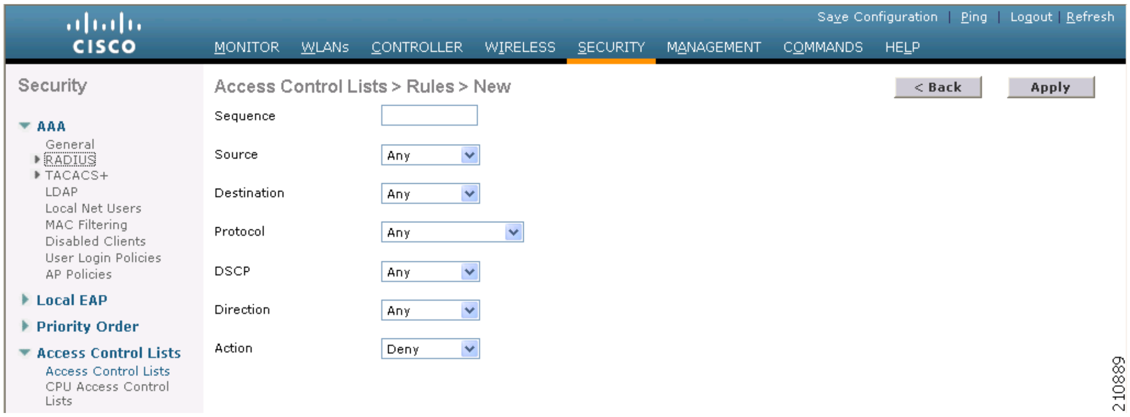
Access Control List Name

Step 4 In the Access Control List Name field, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 5 Click **Apply**. When the Access Control Lists page reappears, click the name of the new ACL.

Step 6 When the Access Control Lists > Edit page appears, click **Add New Rule**. The Access Control Lists > Rules > New page appears (see Figure 5-31).

Figure 5-31 Access Control Lists > Rules > New Page



Access Control Lists > Rules > New

Sequence

Source Any

Destination Any

Protocol Any

DSCP Any

Direction Any

Action Deny

Step 7 Follow these steps to configure a rule for this ACL:

a. The controller supports up to 64 rules for each ACL. These rules are listed in order from 1 to 64. In the Sequence field, 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 contiguous 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 box, 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 edit boxes.

c. From the Destination drop-down box, 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 edit boxes.

d. From the Protocol drop-down box, 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**—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

Note If you choose **Other**, enter the number of the desired protocol in the Protocol edit box. You can find the list of available protocols and their corresponding numbers here: http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml

Note 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.

f. From the DSCP drop-down box, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header field 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 box, choose one of these options to specify the direction of the traffic to which this ACL applies:

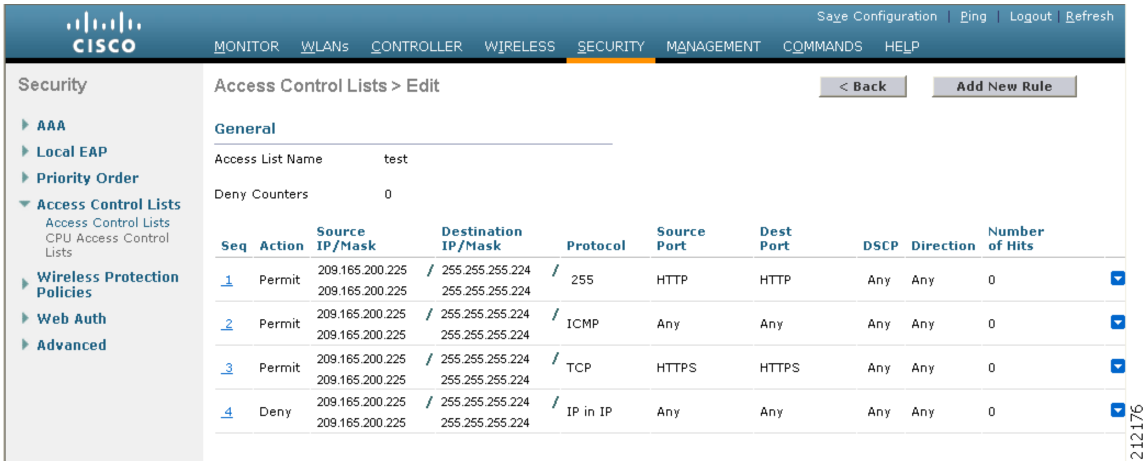
- **Any**—Any direction (This is the default value.)
- **Inbound**—From the client
- **Outbound**—To the client

Note If you are planning to apply this ACL to the controller CPU, choose **Any** or **Inbound** because a CPU ACL applies only to packets that are sent to the CPU, not packets from the CPU.

h. From the Action drop-down box, 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. See Figure 5-32.

Figure 5-32 Access Control Lists > Edit Page



Access Control Lists > Edit

General

Access List Name test

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	209.165.200.225 / 209.165.200.225	255.255.255.224 / 255.255.255.224	255	HTTP	HTTP	Any	Any	0
2	Permit	209.165.200.225 / 209.165.200.225	255.255.255.224 / 255.255.255.224	ICMP	Any	Any	Any	Any	0
3	Permit	209.165.200.225 / 209.165.200.225	255.255.255.224 / 255.255.255.224	TCP	HTTPS	HTTPS	Any	Any	0
4	Deny	209.165.200.225 / 209.165.200.225	255.255.255.224 / 255.255.255.224	IP in IP	Any	Any	Any	Any	0

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

Step 9 Repeat this procedure to add any additional ACLs.

Using the GUI to Apply Access Control Lists

Follow the instructions in these sections to apply ACLs using the controller GUI:

- Applying an Access Control List to an Interface, page 5-59
- Applying an Access Control List to the Controller CPU, page 5-60
- Applying an Access Control List to a WLAN, page 5-61
- Applying a Preauthentication Access Control List to a WLAN, page 5-62

Note 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.

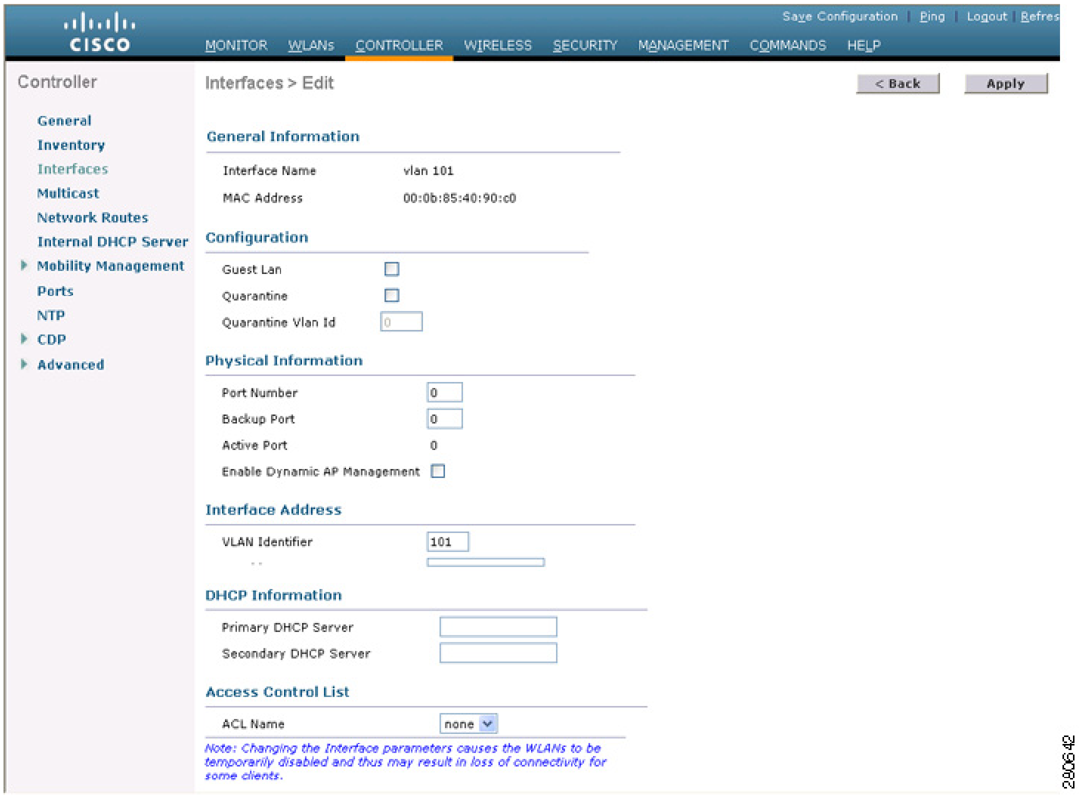
Applying an Access Control List to an Interface

Follow these steps to apply an ACL to a management, AP-manager, or dynamic interface using the controller GUI.

Step 1 Click **Controller** > **Interfaces**.

Step 2 Click the name of the desired interface. The Interfaces > Edit page for that interface appears (see Figure 5-33).

Figure 5-33 Interfaces > Edit Page



Interfaces > Edit

General Information

Interface Name vlan 101

MAC Address 00:0b:85:40:90:c0

Configuration

Guest Lan □

Quarantine □

Quarantine Vlan Id 0

Physical Information

Port Number 0

Backup Port 0

Active Port 0

Enable Dynamic AP Management □

Interface Address

VLAN Identifier 101

DHCP Information

Primary DHCP Server

Secondary DHCP Server

Access Control List

ACL Name none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

Step 3 Choose the desired ACL from the ACL Name drop-down box and click **Apply**. None is the default value.

> **Note** See Chapter 3 for more information on configuring controller interfaces.

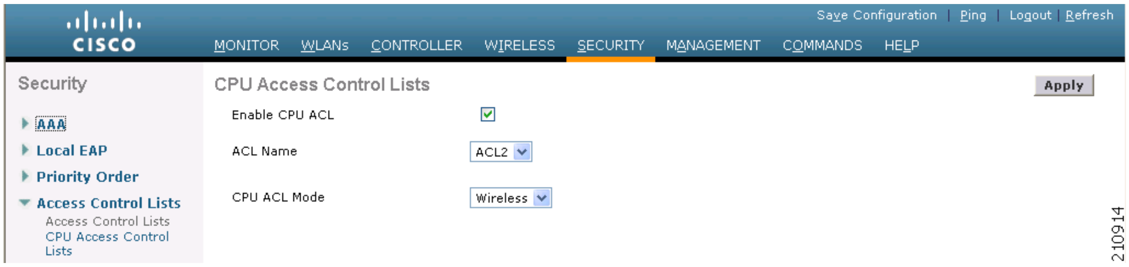
Step 4 Click **Save Configuration** to save your changes.

Applying an Access Control List to the Controller CPU

Follow these steps to apply an ACL to the controller CPU to control traffic to the CPU using the controller GUI.

Step 1 Choose **Security** > **Access Control Lists** > **CPU Access Control Lists**. The CPU Access Control Lists page appears (see Figure 5-34).

Figure 5-34 CPU Access Control Lists Page



CPU Access Control Lists

Enable CPU ACL ☑

ACL Name ACL2

CPU ACL Mode Wireless

Step 2 Check the **Enable CPU ACL** check box to enable a designated ACL to control the traffic to the controller CPU or uncheck the check box to disable the CPU ACL feature and remove any ACL that had been applied to the CPU. The default value is unchecked.

Step 3 From the ACL Name drop-down box, 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 checked, an error message appears indicating that you must choose an ACL.

Note This parameter is available only if you checked the CPU ACL Enable check box.

Step 4 From the CPU ACL Mode drop-down box, choose the type of traffic (wired, wireless, or both) that will be restricted from reaching the controller CPU. Wired is the default value.

Note This parameter is available only if you checked the CPU ACL Enable check box.

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

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

Applying an Access Control List to a WLAN

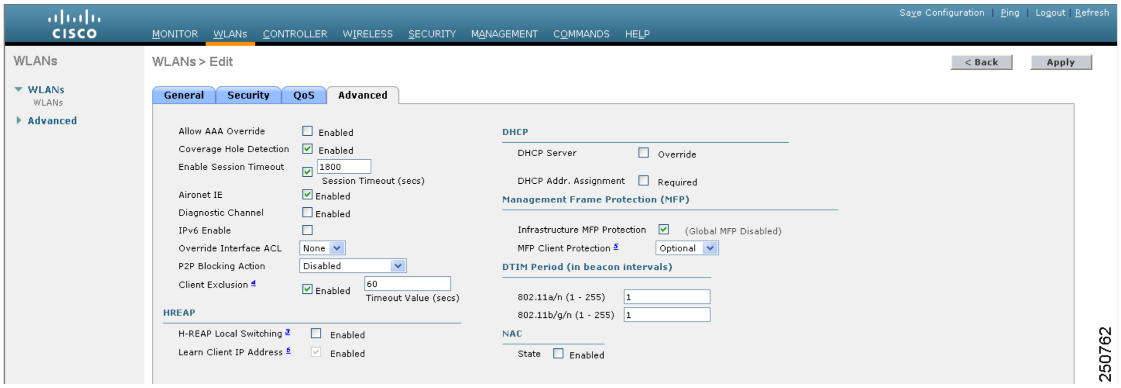
Follow these steps to apply an ACL to a WLAN using the controller GUI.

Step 1 Click **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Click the **Advanced** tab to open the WLANs > Edit (Advanced) page (see Figure 5-35).

Figure 5-35 WLANs > Edit (Advanced) Page


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
250762

WLANs > Edit

Allow AAA Override ☐ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel ☐ Enabled
IPv6 Enable ☐
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion 4 ☑ Enabled 60 Timeout Value (secs)

HREAP
H-REAP Local Switching 3 ☐ Enabled
Learn Client IP Address 6 ☑ Enabled

DHCP
DHCP Server ☐ Override
DHCP Addr. Assignment ☐ Required

Management Frame Protection (MFP)
Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection 5 Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
State ☐ Enabled

Step 4 From the Override Interface ACL drop-down box, choose the 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 See Chapter 6 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

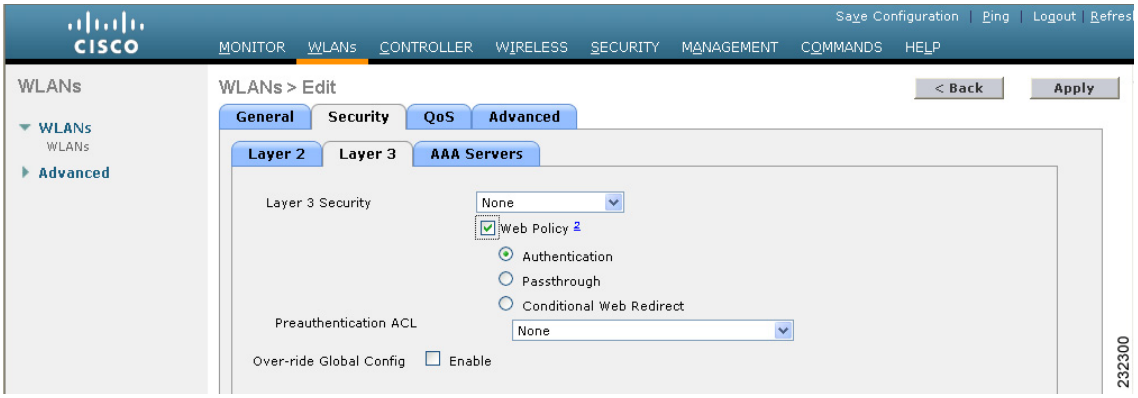
Follow these steps to apply a preauthentication ACL to a WLAN using the controller GUI.

Step 1 Click **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Click the **Security** and **Layer 3** tabs to open the WLANs > Edit (Security > Layer 3) page (see Figure 5-36).

Figure 5-36 WLANs > Edit (Security > Layer 3) Page


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
232300

WLANs > Edit

Layer 3 Security None
☑ Web Policy 2
● Authentication
○ Passthrough
○ Conditional Web Redirect
Preauthentication ACL None
Over-ride Global Config ☐ Enable

Step 4 Check the **Web Policy** check box.

Step 5 From the Preauthentication ACL drop-down box, choose the desired ACL and click **Apply**. None is the default value.

Note See Chapter 6 for more information on configuring WLANs.

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

Using the CLI to Configure Access Control Lists

Follow these steps to configure ACLs using the controller CLI.

Step 1 To see all of the ACLs that are configured on the controller, enter this command:

show acl summary

Information similar to the following appears:

```
ACL Counter Status        Enabled
-------------------------------------
ACL Name                   Applied
------------------------ -----------
acl1                         Yes
acl2                         Yes
acl3                       Yes
```

Step 2 To see detailed information for a particular ACL, enter this command:

show acl detailed *acl_name*

Information similar to the following appears:

```
            Source         Destination        Source Port Dest Port
I Dir IP Address/Netmask IP Address/Netmask Prot    Range Range   DSCP Action Counter
- --- ------------------ ------------------ ---- ----------- -------- ----- ------ -------
1 Any 0.0.0.0/0.0.0.0   0.0.0.0/0.0.0.0   Any    0-65535  0-65535  0    Deny    0
2 In  0.0.0.0/0.0.0.0   200.200.200.0/     6     80-80    0-65535  Any  Permit  0
                       255.255.255.0

DenyCounter :     0
```

The Counter field increments each time a packet matches an ACL rule, and the DenyCounter field increments each time a packet does not match any of the rules.

Step 3 To enable or disable ACL counters for your controller, enter this command:

config acl counter {**start** | **stop**}

Note If you want to clear the current counters for an ACL, enter this command:
clear acl counters *acl_name*

Note ACL counters are available only on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

Step 4 To add a new ACL, enter this command:

config acl create *acl_name*

You can enter up to 32 alphanumeric characters for the *acl_name* parameter.

Step 5 To add a rule for an ACL, enter this command:

config acl rule add *acl_name rule_index*

Step 6 To configure an ACL rule, enter this command:

config 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 port range *acl_name rule_index start_port end_port* |

swap index *acl_name index_1 index_2*}

Refer to Step 7 of the "Using the GUI to Configure Access Control Lists" section on page 5-55 for explanations of the rule parameters.

Step 7 To save your settings, enter this command:

save config

Note To delete an ACL, enter **config acl delete** *acl_name*. To delete an ACL rule, enter **config acl rule delete** *acl_name rule_index*.

Using the CLI to Apply Access Control Lists

Follow these steps to apply ACLs using the controller CLI.

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 **show interface detailed** {**management** | **ap-manager** | *dynamic_interface_name*}. To remove an ACL that is applied to an interface, enter **config interface acl** {**management** | **ap-manager** | *dynamic_interface_name*} **none**.

  See Chapter 3 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 **show acl cpu**. To remove the ACL that is applied to the controller CPU, enter **config acl cpu none**.

- 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 **show wlan** *wlan_id*. To remove the ACL that is applied to a WLAN, enter **config wlan acl** *wlan_id* **none**.

- To apply a preauthentication ACL to a WLAN, enter this command:

  config wlan security web-auth acl *wlan_id acl_name*

  See Chapter 6 for more information on configuring WLANs.

Step 2 To save your settings, enter this command:

save config

Configuring 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. Controller software release 4.1 or later supports both infrastructure and client MFP while controller software release 4.0 supports only infrastructure MFP.

- **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 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 Error reports generated on a hybrid-REAP access point in stand-alone mode cannot be forwarded to the controller and are dropped.

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.

You can configure MFP through either the GUI or the CLI.

Guidelines for Using MFP

Follow these guidelines for using MFP:

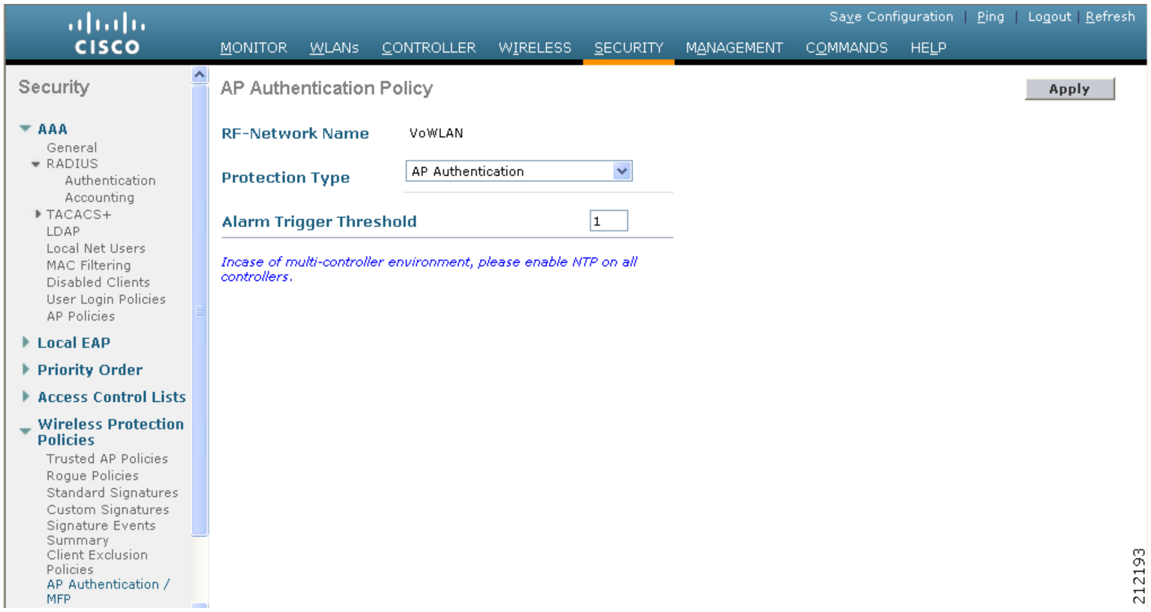
- MFP is supported for use with Cisco Aironet lightweight access points.
- Lightweight access points support infrastructure MFP in local and monitor modes and in hybrid-REAP mode when the access point is connected to a controller. They support Client MFP in local, hybrid-REAP, and bridge modes.
- Client 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.

Using the GUI to Configure MFP

Follow these steps to configure MFP using the controller GUI.

Step 1 Click **Security** > **Wireless Protection Policies** > **AP Authentication/MFP**. The AP Authentication Policy page appears (see Figure 5-37).

Figure 5-37 AP Authentication Policy Page



AP Authentication Policy

RF-Network Name VoWLAN

Protection Type AP Authentication

Alarm Trigger Threshold 1

Incase of multi-controller environment, please enable NTP on all controllers.

Step 2 To enable infrastructure MFP globally for the controller, choose **Management Frame Protection** from the Protection Type drop-down box.

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.

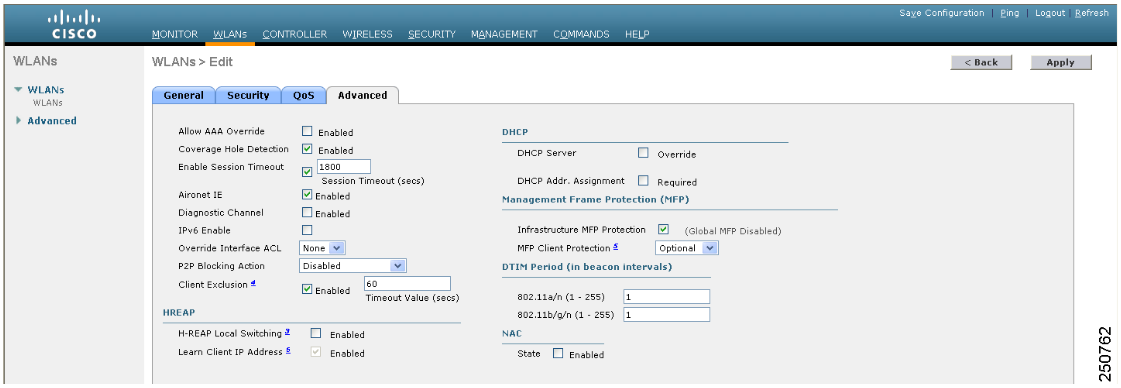
Step 4 Follow these steps if you want to disable or re-enable infrastructure MFP for a particular WLAN after MFP has been enabled globally for the controller:

a. Click **WLANs**.

b. Click the profile name of the desired WLAN. The WLANs > Edit page appears.

c. Click **Advanced**. The WLANs > Edit (Advanced) page appears (see Figure 5-38).

Figure 5-38 WLANs > Edit (Advanced) Page



WLANs > Edit

Allow AAA Override ☐ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel ☐ Enabled
IPv6 Enable ☐
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] ☑ Enabled 60 Timeout Value (secs)

HREAP

H-REAP Local Switching [3] ☐ Enabled
Learn Client IP Address [6] ☑ Enabled

DHCP

DHCP Server ☐ Override
DHCP Addr. Assignment ☐ Required

Management Frame Protection (MFP)

Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC

State ☐ Enabled

d. Uncheck the **Infrastructure MFP Protection** check box to disable MFP for this WLAN or check this check box to enable infrastructure MFP for this WLAN. The default value is enabled. If global MFP is disabled, a note appears in parentheses to the right of the check box.

e. Choose **Disabled**, **Optional**, or **Required** from the MFP Client Protection drop-down box. 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).

f. Click **Apply** to commit your changes.

Step 5 Follow these steps if you want to disable or re-enable infrastructure MFP validation for a particular access point after infrastructure MFP has been enabled globally for the controller:

a. Click **Wireless** > **Access Points** > **All APs** to open the All APs page.

b. Click the name of the desired access point.

c. Click the **Advanced** tab. The All APs > Details for (Advanced) page appears.

d. Uncheck the **MFP Frame Validation** check box to disable MFP for this access point or check this check box to enable MFP for this access point. The default value is enabled. If global MFP is disabled, a note appears in parentheses to the right of the check box.

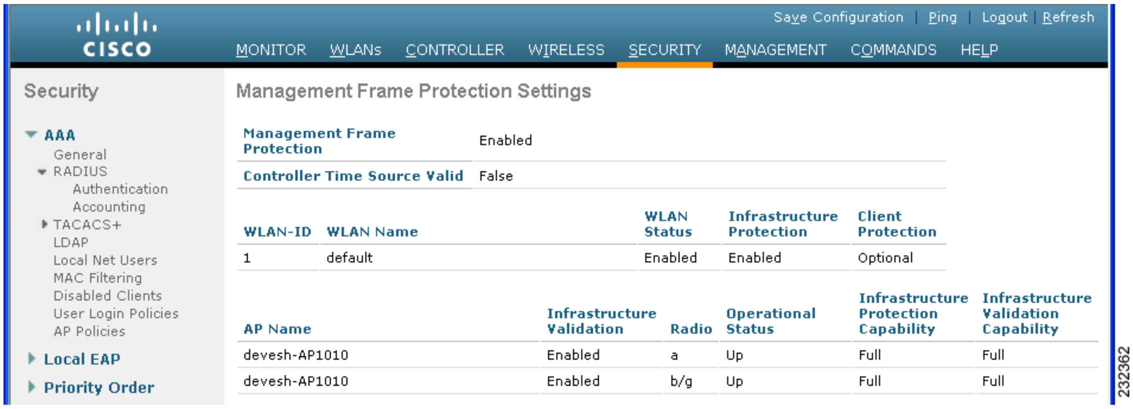
e. Click **Apply** to commit your changes.

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

Using the GUI to View MFP Settings

To see the controller’s current global MFP settings, click **Security** > **Wireless Protection Policies** > **Management Frame Protection**. The Management Frame Protection Settings page appears (see Figure 5-39).

Figure 5-39 Management Frame Protection Settings Page



Management Frame Protection Settings

Management Frame Protection	Enabled
Controller Time Source Valid	False

WLAN-ID	WLAN Name	WLAN Status	Infrastructure Protection	Client Protection
1	default	Enabled	Enabled	Optional

AP Name	Infrastructure Validation	Radio	Operational Status	Infrastructure Protection Capability	Infrastructure Validation Capability
devesh-AP1010	Enabled	a	Up	Full	Full
devesh-AP1010	Enabled	b/g	Up	Full	Full

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 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.
- The Infrastructure Validation field shows if infrastructure MFP is enabled for individual access points.

Using the CLI to Configure MFP

Use these commands to configure MFP using the controller CLI.

1. To enable or disable infrastructure MFP globally for the controller, enter this command:

   config wps mfp infrastructure {**enable** | **disable**}

2. To enable or disable infrastructure MFP signature generation on a WLAN, enter this command:

   config wlan mfp infrastructure protection {**enable** | **disable}** *wlan_id*

   Note Signature generation is activated only if infrastructure MFP is globally enabled.

3. To enable or disable infrastructure MFP validation on an access point, enter this command:

   config ap mfp infrastructure validation {**enable** | **disable**} *Cisco_AP*

   Note MFP validation is activated only if infrastructure MFP is globally enabled.

4. To enable or disable client MFP on a specific WLAN, enter 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.

Using the CLI to View MFP Settings

Use these commands to view MFP settings using the controller CLI.

1. To see the controller's current MFP settings, enter this command:

   show wps mfp summary

   Information similar to the following appears:

```
Global Infrastructure MFP state.... Enabled
Controller Time Source Valid....... False

                    WLAN      Infra.      Client
WLAN ID  WLAN Name Status     Protection  Protection
-------  ---------- -------- ----------  -----------
1        test1      Enabled   Disabled    Disabled
2        open       Enabled   Enabled     Required
3        testpsk    Enabled   *Enabled    Optional but inactive (WPA2 not configured)

         Infra.             Operational     --Infra. Capability--
AP Name  Validation  Radio  State           Protection  Validation
-------- ----------- -----  -----------  ----------- -----------
mapAP    Disabled    a      Up              Full        Full
                    b/g     Up              Full        Full
rootAP2  Enabled    a       Up              Full        Full
                    b/g     Up              Full        Full
HReap    *Enabled   b/g     Up             Full        Full
                    a      Down            Full        Full
```

2. To see the current MFP configuration for a particular WLAN, enter 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
    H-REAP Local Switching................ Disabled
   Infrastructure MFP protection.......... Enabled
   Client MFP............................ Required
...
```

3. To see the current MFP configuration for a particular access point, enter this command:

   show ap config general *AP_name*

   Information similar to the following appears:

```
Cisco AP Identifier............................. 0
Cisco AP Name................................... ap:52:c5:c0
AP Regulatory Domain............................ 80211bg: -N 80211a: -N
Switch Port Number ............................. 1
MAC Address..................................... 00:0b:85:52:c5:c0
IP Address Configuration........................ Static IP assigned
IP Address...................................... 10.67.73.33
IP NetMask...................................... 255.255.255.192
...
AP Mode ........................................ Local
Remote AP Debug ................................ Disabled
S/W  Version ................................... 4.0.2.0
Boot  Version .................................. 2.1.78.0
Mini IOS Version ..............................      --
Stats Reporting Period ......................... 180
LED State....................................... Enabled
ILP Pre Standard Switch......................... Disabled
ILP Power Injector.............................. Disabled
Number Of Slots................................. 2
AP Model........................................ AP1020
AP Serial Number................................ WCN09260057
AP Certificate Type............................. Manufacture Installed
Management Frame Protection Validation .......... Enabled
```

4. To see whether client MFP is enabled for a specific client, enter this command:

   show client detail *client_mac*

```
Client MAC Address.............................. 00:14:1c:ed:34:72
...
Policy Type..................................... WPA2
Authentication Key Management................... PSK
Encryption Cipher............................... CCMP (AES)
Management Frame Protection..................... Yes
...
```

5. To see MFP statistics for the controller, enter 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.

```
BSSID             Radio Validator AP Last Source Addr  Found  Error Type Count Frame Types
----------------- ----- ------------- ----------------- ------ ------------ ----- -------
00:0b:85:56:c1:a0  a    jatwo-1000b 00:01:02:03:04:05 Infra  Invalid MIC 183  Assoc Req
                                                                               Probe Req
                                                                               Beacon
                                                     Infra  Out of seq     4  Assoc Req
                                                     Infra  Unexpected MIC 85 Reassoc Req
                                                     Client Decrypt err  1974 Reassoc Req
                                                                               Disassoc
                                                     Client Replay err     74 Assoc Req
                                                                               Probe Req
                                                                               Beacon
                                                     Client Invalid ICV   174 Reassoc Req
                                                                               Disassoc
                                                     Client Invalid header174 Assoc Req
                                                                               Probe Req
                                                                               Beacon
                                                     Client Brdcst disass 174 Reassoc Req
                                                                               Disassoc
00:0b:85:56:c1:a0  b/g  jatwo-1000b 00:01:02:03:04:05 Infra  Out of seq  185 Reassoc Resp
                                                     Client Not encrypted 174 Assoc Resp
                                                                               Probe Resp
```

Using the CLI to Debug MFP Issues

Use these commands 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

Follow these steps to configure the controller to exclude clients under certain conditions using the controller GUI.

Step 1 Click **Security** > **Wireless Protection Policies** > **Client Exclusion Policies** to open the Client Exclusion Policies page.

Step 2 Check 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 Identity Networking

These sections explain the identity networking feature, how it is configured, and the expected behavior for various security policies:

- Identity Networking Overview, page 5-74
- RADIUS Attributes Used in Identity Networking, page 5-75
- Configuring AAA Override, page 5-78

Identity Networking Overview

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 since 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 include:

- 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. This 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.

QoS-Level

This attribute indicates the Quality of Service 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 fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     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 fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     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 fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          |  Vendor type  | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    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 fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |    Length     |      Tag      |   String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type – 81 for Tunnel-Private-Group-ID.
- Length – >= 3

- Tag – The Tag field 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 field 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 field is greater than 0x1F, it should be interpreted as the first byte of the following String field.
- String – This field must be present. The group is represented by the String field. There is no restriction on the format of group IDs.

Tunnel Attributes

Note 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.

Reference RFC2868 defines RADIUS tunnel attributes used for authentication and authorization, and RFC2867 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 Virtual LAN (VLAN), defined in IEEE8021Q, based on the result of the authentication. This 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 Access- Request.

For use in VLAN assignment, the following tunnel attributes are used:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

Note that the VLANID is 12-bits, taking a value between 1 and 4094, inclusive. Since the Tunnel-Private-Group-ID is of type String as defined in RFC2868, 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 field. As noted in RFC2868, section 3.1:

- The Tag field 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. Valid values for this field are 0x01 through 0x1F, inclusive. If the Tag field 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 field of greater than 0x1F is interpreted as the first octet of the following field.
- 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 field 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

The Allow AAA Override option of a WLAN allows you to configure the WLAN for identity networking. It allows you to apply VLAN tagging, QoS, and ACLs to individual clients based on the returned RADIUS attributes from the AAA server.

Note 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 already configured on the interface, or disable and then re-enable the WLAN after you apply the interface so that the clients can reauthenticate.

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, simply 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 = 0, Gold = 1, Platinum = 2, and Bronze = 3. Follow the steps below to do so.

Note This issue does not apply to the Cisco Secure Access Control Server (ACS).

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:

```
################################################################################
# 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
#
@radius.dct
#
# Standard attributes supported by Airespace
#
# Define additional vendor specific attributes (VSAs)
#

MACRO Airespace-VSA(t,s) 26 [vid=14179 type1=%t% len1=+2 data=%s%]

ATTRIBUTE   WLAN-Id                 Airespace-VSA(1, integer)     cr
ATTRIBUTE   Aire-QoS-Level         Airespace-VSA(2, integer)     r
VALUE Aire-QoS-Level Bronze  3
VALUE Aire-QoS-Level Silver   0
VALUE Aire-QoS-Level Gold     1
VALUE Aire-QoS-Level Platinum 2

ATTRIBUTE   DSCP                        Airespace-VSA(3, integer)     r
ATTRIBUTE   802.1P-Tag                  Airespace-VSA(4, integer)     r
ATTRIBUTE   Interface-Name              Airespace-VSA(5, string)      r
ATTRIBUTE   ACL-Name                    Airespace-VSA(6, string)      r

# This should be last.

################################################################################
# CiscoWLAN.dct - Cisco WLC dictionary
##############################################################################
```

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 box.

Using the GUI to Configure AAA Override

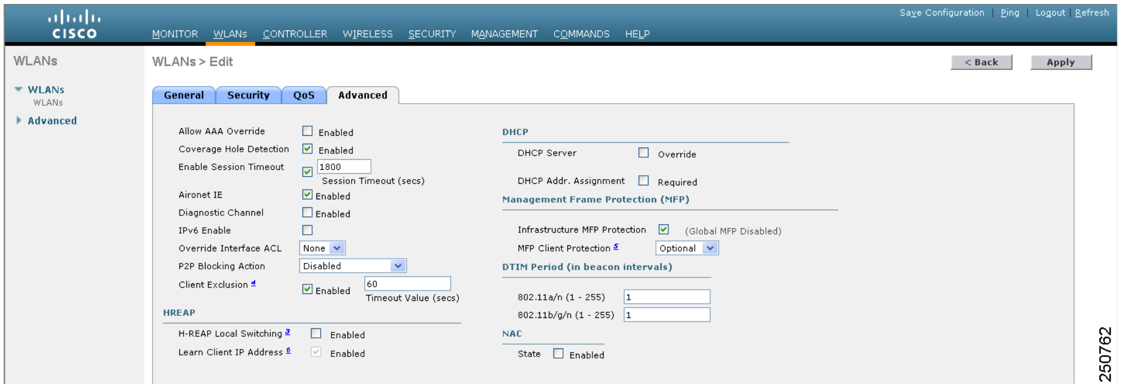
Follow these steps to configure AAA override using the controller GUI.

Step 1 Click **WLAN**s 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 Click the **Advanced** tab to open the WLANs > Edit (Advanced) page (see Figure 5-40).

Figure 5-40 WLANs > Edit (Advanced) Page



WLANs > Edit

Allow AAA Override ☐ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel ☐ Enabled
IPv6 Enable ☐
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] ☑ Enabled 60 Timeout Value (secs)

HREAP
H-REAP Local Switching [2] ☐ Enabled
Learn Client IP Address [5] ☑ Enabled

DHCP
DHCP Server ☐ Override
DHCP Addr. Assignment ☐ Required

Management Frame Protection (MFP)
Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
State ☐ Enabled

Step 4 Check the **Allow AAA Override** check box to enable AAA override or uncheck it to disable this feature. The default value is disabled.

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

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

Using the CLI to Configure AAA Override

Use this command to enable or disable AAA override using the controller CLI:

config wlan aaa-override {**enable** | **disable**} *wlan_id*

For *wlan_id*, enter an ID from 1 to 16.

Managing Rogue Devices

This section describes security solutions for rogue devices. A rogue device is an unknown access point or client that is detected by managed access points in your network as not belonging to your system.

Challenges

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. Therefore, 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 as 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.

Classifying Rogue Access Points

Controller software release 5.0 or later improves 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. Now you can create rules that enable the controller to 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 The 4400 series controllers, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch support up to 625 rogues, and the 2100 series controllers and Controller Network Module for Integrated Services Routers support up to 125 rogues. Each controller limits the number of rogue containments to three per radio (or six per radio for access points in monitor mode).

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 5-8 shows the rogue states that can be adopted by a rogue access point in a particular classification type.

Table 5-8 Classification Mapping

Rule-Based Classification Type	Rogue States
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. For example, 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. For example, the access points belonging 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.

Table 5-8 Classification Mapping (continued)

Rule-Based Classification Type	Rogue States
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, 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 5-9 shows the allowable classification types and rogue states from and to which an unknown access point can be configured.

Table 5-9 Allowable Classification Type and Rogue State Transitions

From	To
Friendly (Internal, External, Alert)	Malicious (Alert)
Friendly (Internal, External, Alert)	Unclassified (Alert)
Friendly (Alert)	Friendly (Internal, External)
Malicious (Alert, Threat)	Friendly (Internal, External)
Malicious (Contained, Contained Pending)	Malicious (Alert)
Unclassified (Alert, Threat)	Friendly (Internal, External)
Unclassified (Contained, Contained Pending)	Unclassified (Alert)
Unclassified (Alert)	Malicious (Alert)

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.

WCS Interaction

WCS software release 5.0 or later also supports 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 RLDP

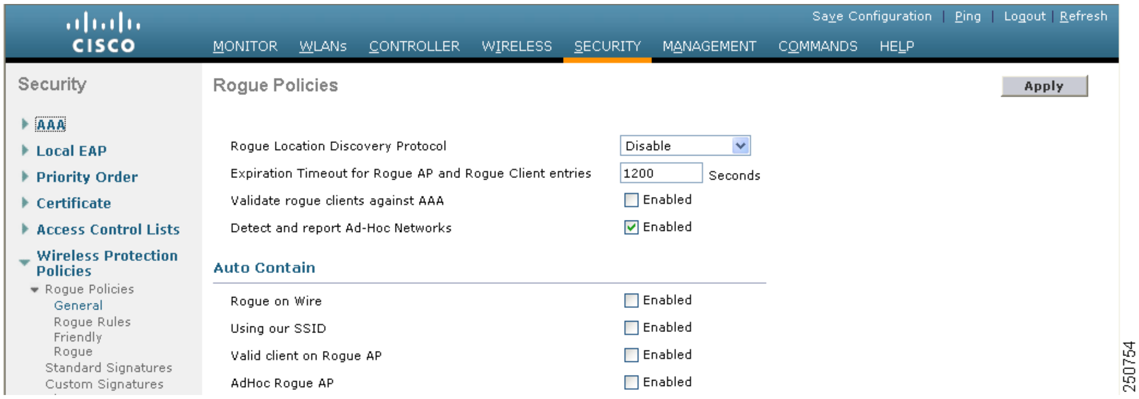
You can configure RLDP to detect and automatically contain rogue devices using the controller GUI or CLI.

Using the GUI to Configure RLDP

Using the controller GUI, follow these steps to configure RLDP.

Step 1 Click **Security** > **Wireless Protection Policies** > **Rogue Policies** > **General** to open the Rogue Policies page (see Figure 5-41).

Figure 5-41 Rogue Policies Page



Rogue Policies

Rogue Location Discovery Protocol: Disable
Expiration Timeout for Rogue AP and Rogue Client entries: 1200 Seconds
Validate rogue clients against AAA: ☐ Enabled
Detect and report Ad-Hoc Networks: ☑ Enabled

Auto Contain

Rogue on Wire: ☐ Enabled
Using our SSID: ☐ Enabled
Valid client on Rogue AP: ☐ Enabled
AdHoc Rogue AP: ☐ Enabled

Step 2 Choose one of the following options from the Rogue Location Discovery Protocol drop-down box:

- **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 3 In the Expiration Timeout for Rogue AP and Rogue Client Entries field, 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 4 If desired, check 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 unchecked.

Step 5 If desired, check the **Detect and Report Ad-Hoc Networks** check box to enable ad-hoc rogue detection and reporting. The default value is checked.

Step 6 If you want the controller to automatically contain certain rogue devices, check the following check boxes. Otherwise, leave the check boxes unchecked, 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.

- **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 unchecked, 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 unchecked, the controller only generates an alarm when such a rogue is detected.
- **AdHoc Rogue AP**—Automatically contains adhoc networks detected by the controller. If you leave this parameter unchecked, the controller only generates an alarm when such a network is detected.

Step 7 Click **Apply** to commit your changes.

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

Using the CLI to Configure RLDP

Using the controller CLI, follow these steps to configure RLDP.

Step 1 To enable, disable, or initiate RLDP, enter 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 2 To specify the number of seconds after which the rogue access point and client entries expire and are removed from the list, enter this command:

config rogue 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 3 To enable or disable ad-hoc rogue detection and reporting, enter this command:

config rogue adhoc {**enable** | **disable**}

Step 4 To enable or disable the AAA server or local database to validate if rogue clients are valid clients, enter this command:

config rogue client aaa {**enable** | **disable**}

Step 5 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 this command: **config rogue ap ssid alarm**.

- **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 this command: **config rogue ap valid-client alarm**.

- **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 this command: **config rogue adhoc alert**.

Step 6 To save your changes, enter this command:

save config

Configuring Rogue Classification Rules

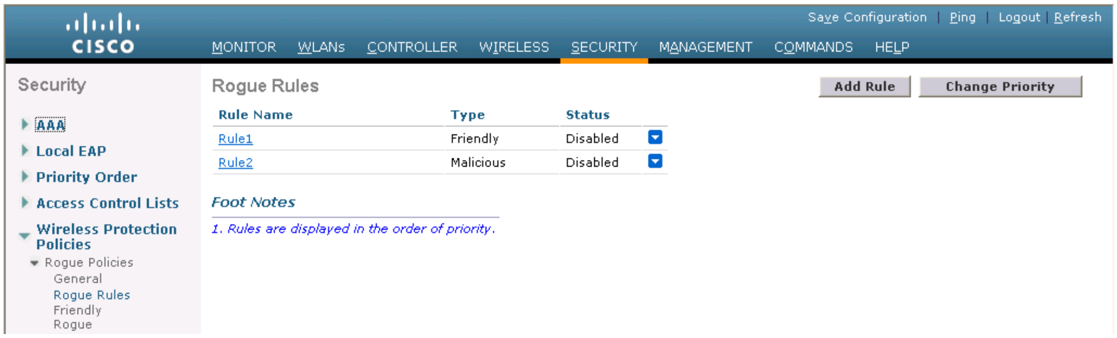
You can configure up to 64 rogue classification rules per controller using the controller GUI or CLI.

Using the GUI to Configure Rogue Classification Rules

Using the controller GUI, follow these steps to configure rogue classification rules.

Step 1 Click **Security** > **Wireless Protection Policies** > **Rogue Policies** > **Rogue Rules** to open the Rogue Rules page (see Figure 5-42).

Figure 5-42 Rogue Rules Page



Rule Name	Type	Status
Rule1	Friendly	Disabled
Rule2	Malicious	Disabled

Foot Notes

1. Rules are displayed in the order of priority.

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 To create a new rule, follow these steps:

a. Click **Add Rule**. An Add Rule section appears at the top of the page.

b. In the Rule Name field, enter a name for the new rule. Make sure that the name does not contain any spaces.

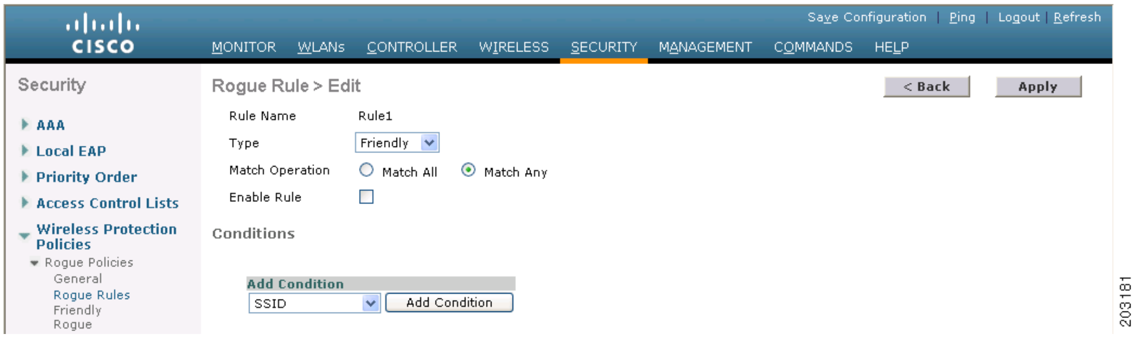
c. From the Rule Type drop-down box, choose **Friendly** or **Malicious** to classify rogue access points matching this rule as friendly or malicious.

d. Click **Add** to add this rule to the list of existing rules, or click **Cancel** to discard this new rule.

Step 3 To edit a rule, follow these steps:

a. Click the name of the rule that you want to edit. The Rogue Rule > Edit page appears (see Figure 5-43).

Figure 5-43 Rogue Rule > Edit Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
Local EAP
Priority Order
Access Control Lists
Wireless Protection Policies
Rogue Policies
General
Rogue Rules
Friendly
Rogue
< Back
Apply
203181

Rogue Rule > Edit

Rule Name: Rule1
Type: Friendly
Match Operation: ○ Match All ● Match Any
Enable Rule: □

Conditions

Add Condition: SSID [Add Condition]

b. From the Type drop-down box, choose **Friendly** or **Malicious** to classify rogue access points matching this rule as friendly or malicious.

c. From the Match Operation field, 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, check the **Enable Rule** check box. The default value is unchecked.

e. From the Add Condition drop-down box, 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 field, 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 field. 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 in the Time Duration field. 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 field. 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.

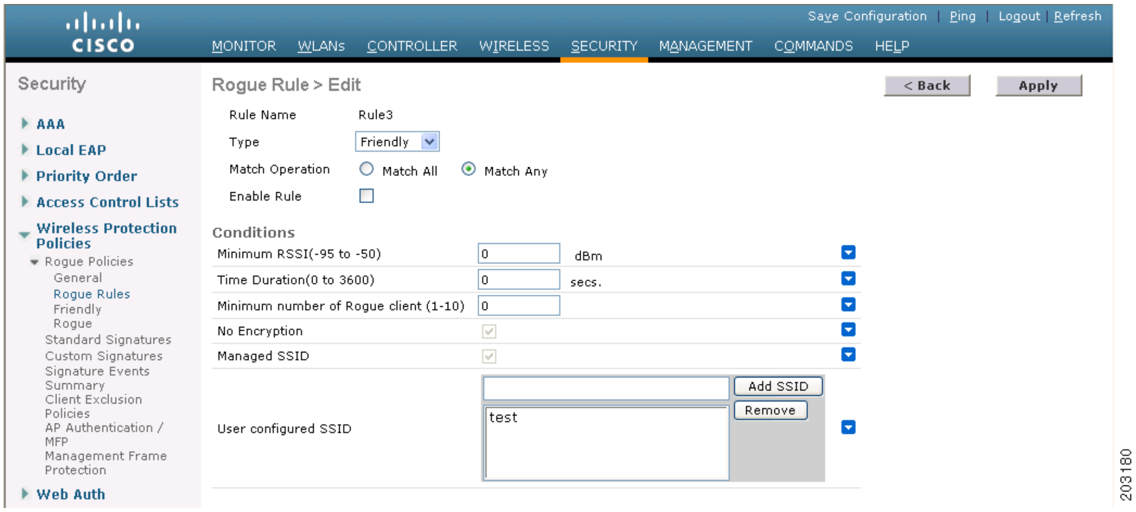
Note WCS refers to this option as “Open Authentication.”

- **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 as 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 (see Figure 5-44).

Figure 5-44 Rogue Rule > Edit Page



Rogue Rule > Edit

Rule Name: Rule3
Type: Friendly
Match Operation: ○ Match All ● Match Any
Enable Rule: □

Conditions

Minimum RSSI(-95 to -50)	0	dBm
Time Duration(0 to 3600)	0	secs.
Minimum number of Rogue client (1-10)	0	
No Encryption	✓	
Managed SSID	✓	
User configured SSID	test	

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.

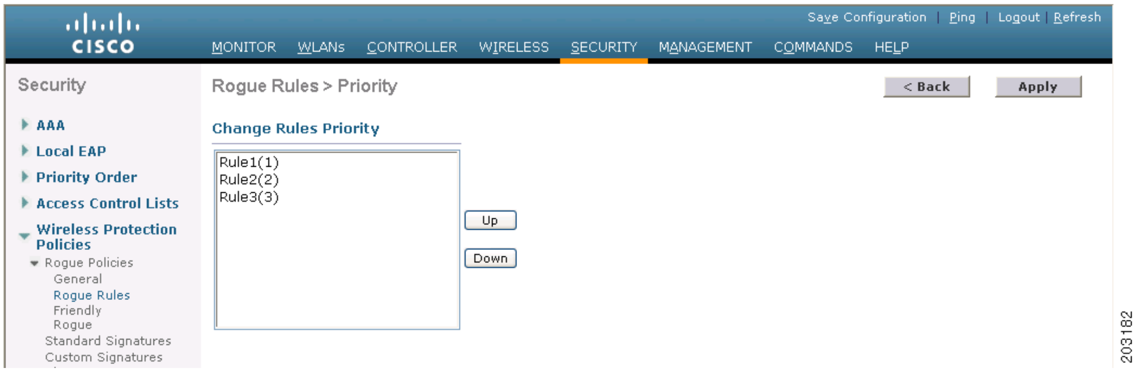
Step 4 Click **Save Configuration** to save your changes.

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 (see Figure 5-45).

Figure 5-45 Rogue Rules > Priority Page



Rule1(1)
Rule2(2)
Rule3(3)

The rogue rules are listed in priority order in the Change Rules Priority edit 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.

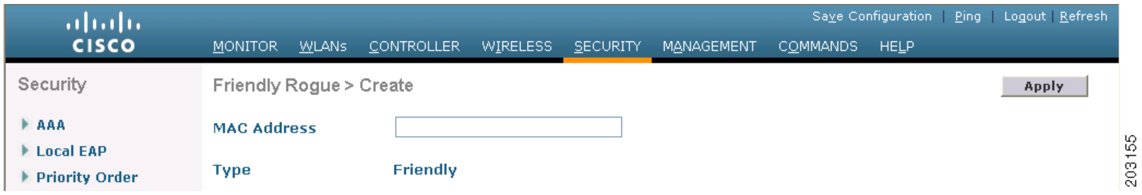
d. Continue to move the rules up or down until the rules are in the desired order.

e. Click **Apply** to commit your changes.

Step 6 If you want to classify any rogue access points as friendly and add them to the friendly MAC address list, follow these steps:

a. Click **Security** > **Wireless Protection Policies** > **Rogue Policies** > **Friendly Rogue** to access the Friendly Rogue > Create page (see Figure 5-46).

Figure 5-46 Friendly Rogue > Create Page


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
Local EAP
Priority Order
Friendly Rogue > Create
Apply
MAC Address
203155

Type Friendly

b. In the MAC Address field, 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.

Using the CLI to Configure Rogue Classification Rules

Using the controller CLI, follow these steps to configure rogue classification rules.

Step 1 To create a rule, enter 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 this command: **config rogue rule priority** *priority rule_name*. If you later want to change the classification of this rule, enter this command: **config rogue rule classify** {**friendly** | **malicious**} *rule_name*.

Note If you ever want to delete all of the rogue classification rules or a specific rule, enter this command: **config rogue rule delete** {**all** | *rule_name*}.

Step 2 To disable all rules or a specific rule, enter this command:

config rogue rule disable {**all** | *rule_name*}

Note A rule must be disabled before you can modify its attributes.

Step 3 To add conditions to a rule that the rogue access point must meet, enter 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.

  Note If you ever want to delete all of the SSIDs or a specific SSID from the user-configured SSID list, enter this command: **config rogue rule condition ap delete ssid** {**all** | *ssid*} *rule_name*.

- **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 this command: **config rogue rule condition ap delete** {**all** | *condition_type*} *condition_value rule_name*.

Step 4 To 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, enter this command:

config rogue rule match {**all** | **any**} *rule_name*

Step 5 To enable all rules or a specific rule, enter this command:

config rogue rule enable {**all** | *rule_name*}

Note For your changes to become effective, you must enable the rule.

Step 6 To add a new friendly access point entry to the friendly MAC address list or delete an existing friendly access point entry from the list, enter this command:

config rogue ap friendly {**add** | **delete**} *ap_mac_address*

Step 7 To save your changes, enter this command:

save config

Step 8 To view the rogue classification rules that are configured on the controller, enter this command:

show rogue rule summary

Information similar to the following appears:

```
Priority Rule Name  State      Type       Match  Hit Count
-------- ----------- -------- ------------ ------ ---------
1        Rule1      Disabled   Friendly      Any   0
2        Rule2      Enabled    Malicious     Any  339
3       Rule3      Disabled   Friendly     Any   0
```

Step 9 To view detailed information for a specific rogue classification rule, enter 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 Classifying Rogue Devices

Using the controller GUI or CLI, you can view rogue devices and determine the action that the controller should take.

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.

Using the GUI to View and Classify Rogue Devices

Using the controller GUI, follow these steps to view and classify rogue devices.

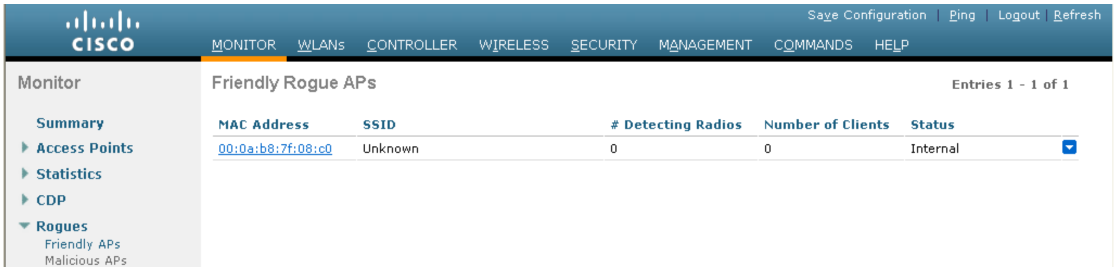
Step 1 Click **Monitor** > **Rogues**.

Step 2 Click the following options to view the different types of rogue access points detected by the controller:

- **Friendly APs**
- **Malicious APs**
- **Unclassified APs**

A page similar to the following appears (see Figure 5-47).

Figure 5-47 Friendly Rogue APs Page



Friendly Rogue APs

Entries 1 - 1 of 1

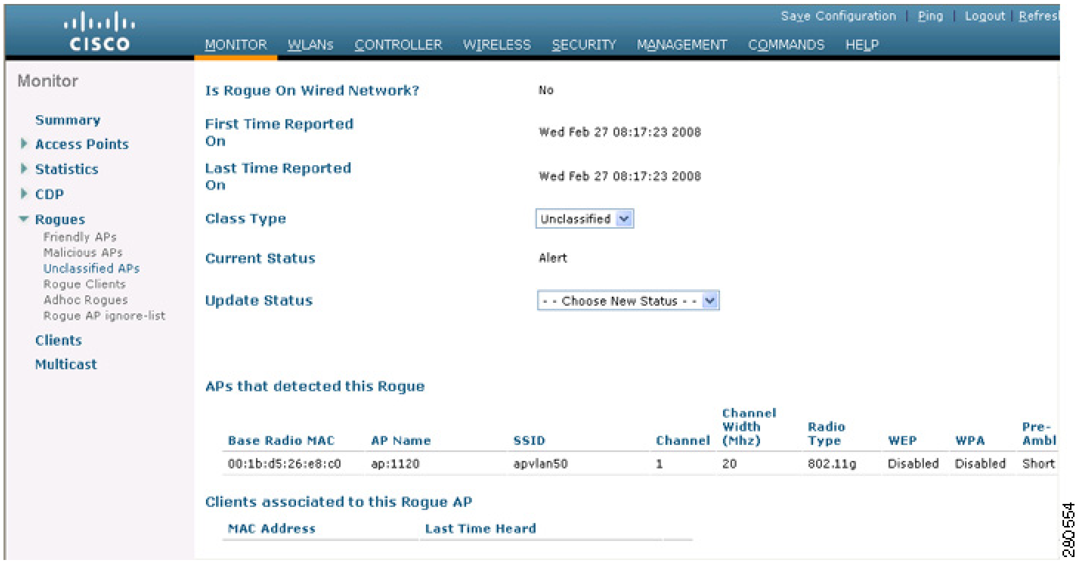
MAC Address	SSID	# Detecting Radios	Number of Clients	Status
00:0a:b8:7f:08:c0	Unknown	0	0	Internal

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, 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** 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**.

Step 3 To obtain more details about a rogue access point, click the MAC address of the access point. The Rogue AP Detail page appears (see Figure 5-48).

Figure 5-48 Rogue AP Detail Page



Is Rogue On Wired Network? No

First Time Reported On Wed Feb 27 08:17:23 2008

Last Time Reported On Wed Feb 27 08:17:23 2008

Class Type Unclassified

Current Status Alert

Update Status - - Choose New Status - -

APs that detected this Rogue

Base Radio MAC	AP Name	SSID	Channel	Channel Width (Mhz)	Radio Type	WEP	WPA	Pre-Ambl
00:1b:d5:26:e8:c0	ap:1120	apvlan50	1	20	802.11g	Disabled	Disabled	Short

Clients associated to this Rogue AP

MAC Address	Last Time Heard

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.

Step 4 The Class Type field 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.

If you want to change the classification of this device, choose a different classification from the Class Type drop-down box.

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 box, 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.

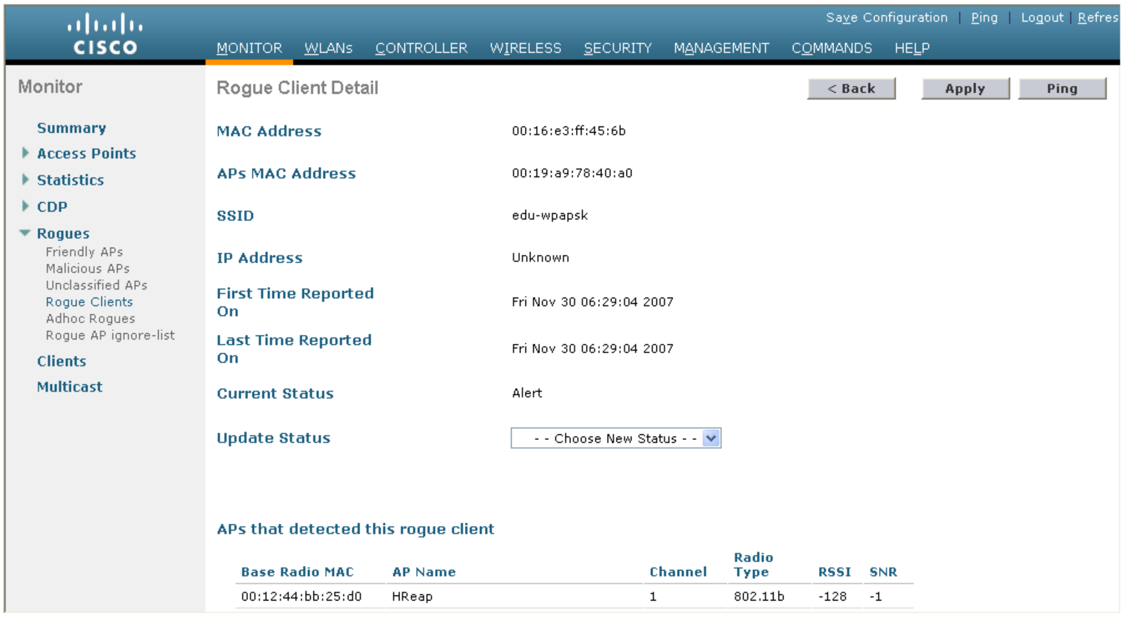
Step 6 Click **Apply** to commit your changes.

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

Step 8 To view any rogue clients that are connected to the controller, click **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 To obtain more details about a rogue client, click the MAC address of the client. The Rogue Client Detail page appears (see Figure 5-49).

Figure 5-49 Rogue Client Detail Page



Rogue Client Detail

MAC Address	00:16:e3:ff:45:6b
APs MAC Address	00:19:a9:78:40:a0
SSID	edu-wpapsk
IP Address	Unknown
First Time Reported On	Fri Nov 30 06:29:04 2007
Last Time Reported On	Fri Nov 30 06:29:04 2007
Current Status	Alert
Update Status	- - Choose New Status - -

APs that detected this rogue client

Base Radio MAC	AP Name	Channel	Radio Type	RSSI	SNR
00:12:44:bb:25:d0	HReap	1	802.11b	-128	-1

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 box, 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.

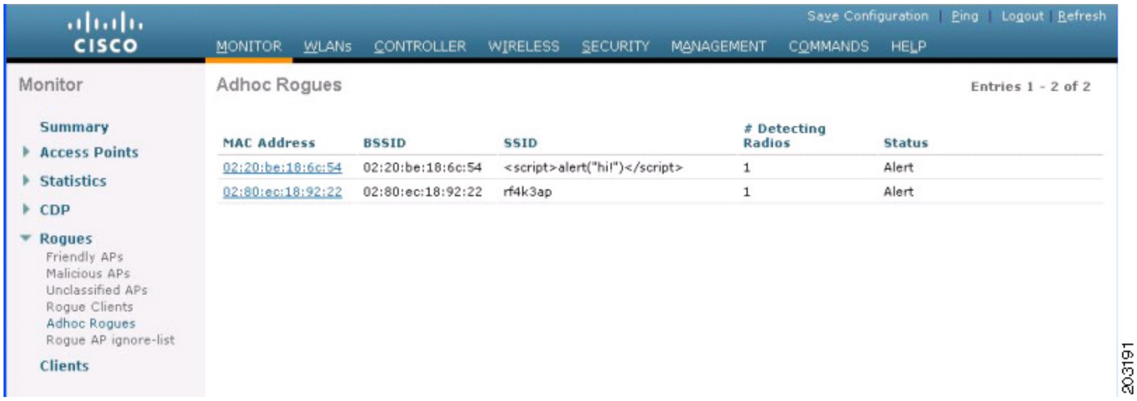
Step 11 Click **Apply** to commit your changes.

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 To view any ad-hoc rogues detected by the controller, click **Adhoc Rogues**. The Adhoc Rogues page appears (see Figure 5-50).

Figure 5-50 Adhoc Rogues Page



Adhoc Rogues

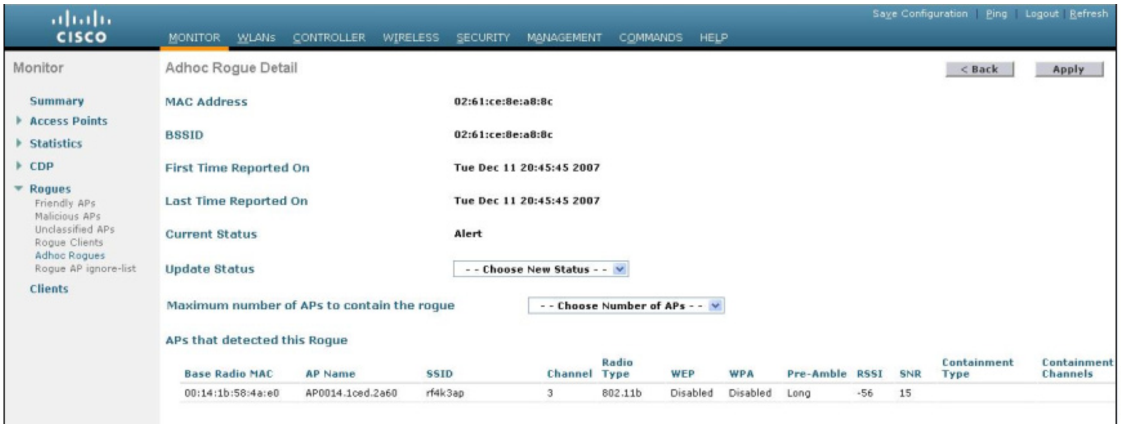
Entries 1 - 2 of 2

MAC Address	BSSID	SSID	# Detecting Radios	Status
02:20:be:18:6c:54	02:20:be:18:6c:54	<script>alert("hi!")</script>	1	Alert
02:80:ec:18:92:22	02:80:ec:18:92:22	rf4k3ap	1	Alert

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 To obtain more details about an ad-hoc rogue, click the MAC address of the rogue. The Adhoc Rogue Detail page appears (see Figure 5-51).

Figure 5-51 Adhoc Rogue Detail Page



Adhoc Rogue Detail

MAC Address 02:61:ce:8e:a8:8c

BSSID 02:61:ce:8e:a8:8c

First Time Reported On Tue Dec 11 20:45:45 2007

Last Time Reported On Tue Dec 11 20:45:45 2007

Current Status Alert

Update Status - - Choose New Status - -

Maximum number of APs to contain the rogue - - Choose Number of APs - -

APs that detected this Rogue

Base Radio MAC	AP Name	SSID	Channel	Radio Type	WEP	WPA	Pre-Amble	RSSI	SNR	Containment Type	Containment Channels
00:14:1b:58:4a:e0	AP0014.1ced.2a60	rf4k3ap	3	802.11b	Disabled	Disabled	Long	-56	15		

This page provides the following information: the MAC address and BSSID of the adhoc 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 box, 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 box, 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.**

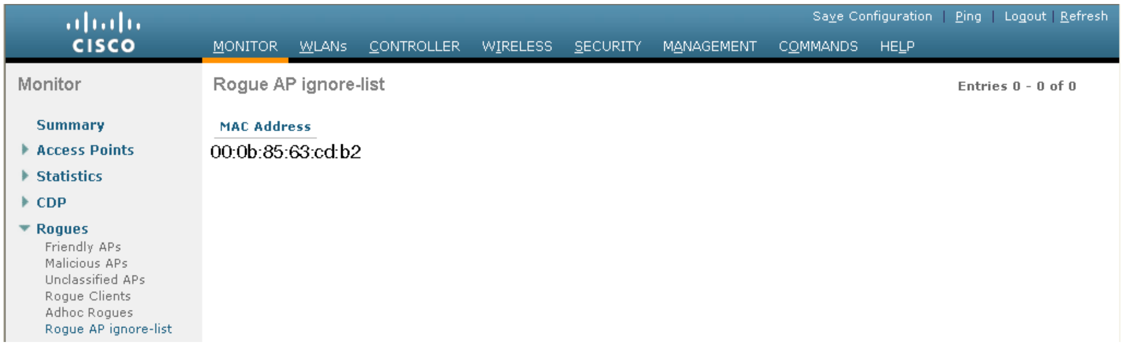
The bottom of the page provides information on the access points that detected this ad-hoc rogue.

Step 18 Click **Apply** to commit your changes.

Step 19 Click **Save Configuration** to save your changes.

Step 20 To view any access points that have been configured to be ignored, click **Rogue AP Ignore-List**. The Rogue AP Ignore-List page appears (see Figure 5-52).

Figure 5-52 Rogue AP Ignore-List Page



Rogue AP ignore-list

Entries 0 - 0 of 0

MAC Address
00:0b:85:63:cd:b2

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.

Using the CLI to View and Classify Rogue Devices

Using the controller CLI, enter these commands to view and classify rogue devices.

1. To view a list of all rogue access points detected by the controller, enter 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
00:0b:85:63:cd:bf Malicious         1        0       Fri Nov 30 11:23:12 2007
...
```

2. To view a list of the friendly rogue access points detected by the controller, enter this command:

   show rogue ap friendly summary

   Information similar to the following appears:

```
Number of APs.................................. 1

MAC Address        State              # APs # Clients Last Heard
-----------------  ------------------ ----- --------- ---------------------------
00:0a:b8:7f:08:c0  Internal           1   0        Tue Nov 27 13:52:04 2007
```

3. To view a list of the malicious rogue access points detected by the controller, enter this command:

   show rogue ap malicious summary

   Information similar to the following appears:

```
Number of APs.................................... 264

MAC Address        State              # APs # Clients Last Heard
-----------------  ------------------ ----- --------- -----------------------
00:0b:85:01:30:3f  Alert              1     0         Fri Nov 30 11:20:01 2007
00:0b:85:63:70:6f  Alert              1     0         Fri Nov 30 11:20:14 2007
00:0b:85:63:cd:bf  Alert              1     0         Fri Nov 30 11:23:12 2007
00:0b:85:63:cd:dd  Alert              1     0         Fri Nov 30 11:27:03 2007
00:0b:85:63:cd:de  Alert              1     0         Fri Nov 30 11:26:23 2007
00:0b:85:63:cd:df Alert            1      0        Fri Nov 30 11:26:50 2007
...
```

4. To view a list of the unclassified rogue access points detected by the controller, enter this command:

   show rogue ap unclassified summary

   Information similar to the following appears:

```
Number of APs.................................... 164

MAC Address        State              # APs # Clients Last Heard
-----------------  ------------------ ----- --------- -----------------------
00:0b:85:63:cd:bd  Alert              1     0         Fri Nov 30 11:12:52 2007
00:0b:85:63:cd:e7  Alert              1     0         Fri Nov 30 11:29:01 2007
00:0b:85:63:ce:05  Alert              1     0         Fri Nov 30 11:26:23 2007
00:0b:85:63:ce:07  Alert               1     0         Fri Nov 30 11:26:23 2007
...
```

5. To view detailed information for a specific rogue access point, enter this command:

   show rogue ap detailed *ap_mac_address*

   Information similar to the following appears:

```
Rogue BSSID...................................... 00:0b:85:63:d1:94
Is Rogue on Wired Network........................ No
Classification................................... Unclassified
State............................................ Alert
First Time Rogue was Reported.................... Fri Nov 30 11:24:56 2007
Last Time Rogue was Reported..................... Fri Nov 30 11:24:56 2007
Reported By
    AP 1
        MAC Address.............................. 00:12:44:bb:25:d0
        Name..................................... HReap
        Radio Type............................... 802.11g
        SSID..................................... edu-eap
        Channel.................................. 6
        RSSI..................................... -61 dBm
        SNR...................................... -1 dB
        Encryption............................... Enabled
        ShortPreamble............................ Enabled
        WPA Support.............................. Disabled
        Last reported by this AP.............. Fri Nov 30 11:24:56 2007
```

6. To see the rogue report (which shows the number of rogue devices detected on different channel widths) for a specific 802.11a/n radio, enter 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
    ...
```

7. To view a list of all rogue clients that are associated to a rogue access point, enter this command:

   show rogue ap clients *ap_mac_address*

   Information similar to the following appears:

```
MAC Address        State              # APs  Last Heard
-----------------  ------------------ ----- -------------------------
00:bb:cd:12:ab:ff  Alert              1      Fri Nov 30 11:26:23 2007
```

8. To view a list of all rogue clients detected by the controller, enter this command:

   show rogue client summary

   Information similar to the following appears:

```
Validate rogue clients against AAA............... Disabled

MAC Address        State              # APs Last Heard
-----------------  ------------------ ----- -----------------------
00:0a:8a:7d:f5:f5  Alert              1     Mon Dec  3 21:56:36 2007
00:18:ba:78:c4:44  Alert              1     Mon Dec  3 21:59:36 2007
00:18:ba:78:c4:d1  Alert              1     Mon Dec  3 21:47:36 2007
00:18:ba:78:ca:f8 Alert            1     Mon Dec  3 22:02:36 2007
...
```

9. To view detailed information for a specific rogue client, enter 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:b6:b0
        Name..................................... AP0016.47b2.31ea
        Radio Type............................... 802.11a
        RSSI..................................... -71 dBm
        SNR...................................... 23 dB
        Channel.................................. 149
        Last reported by this AP.............. Mon Dec  3 21:50:36 2007
```

10. To view a list of all ad-hoc rogues detected by the controller, enter this command:

    show rogue adhoc summary

    Information similar to the following appears:

```
Detect and report Ad-Hoc Networks................ Enabled

Client MAC Address  Adhoc BSSID         State     # APs   Last Heard
------------------  ------------------  ----------- -------  ------------------------
00:bb:cd:12:ab:ff  super              Alert       1       Fri Nov 30 11:26:23 2007
```

11. To view detailed information for a specific ad-hoc rogue, enter 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
```

12. To view a list of rogue access points that are configured to be ignored, enter this command:

    show rogue ignore-list

    Information similar to the following appears:

```
MAC Address
------------------
10:bb:17:cc:01:ef
```

Note Refer to Step 20 of the "Using the GUI to View and Classify Rogue Devices" section on page 5-93 for more information on the rogue-ignore access point list.

13. To classify a rogue access point as friendly, enter 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.

14. To mark a rogue access point as malicious, enter this command:

    config rogue ap classify malicious state {**alert** | **contain**} *ap_mac_address*

    where

    - **contain** means that the controller contains the offending device so that its signals no longer interfere with authorized clients.
    - **alert** means that the controller forwards an immediate alert to the system administrator for further action.

    Note A rogue access point cannot be moved to the Malicious class if its current state is Contain.

15. To mark a rogue access point as unclassified, enter 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.

16. To specify how the controller should respond to a rogue client, enter 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.

17. To specify how the controller should respond to an adhoc rogue, enter 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.

18. To save your changes, enter this command:

    save config

Configuring IDS

The Cisco intrusion detection system/intrusion prevention system (CIDS/IPS) 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, see below
- IDS signatures, see page 5-107

Note The Cisco wireless intrusion prevention system (wIPS) is also supported on the controller through WCS. Refer to the "Configuring wIPS" section on page 5-119 for more information.

Configuring IDS Sensors

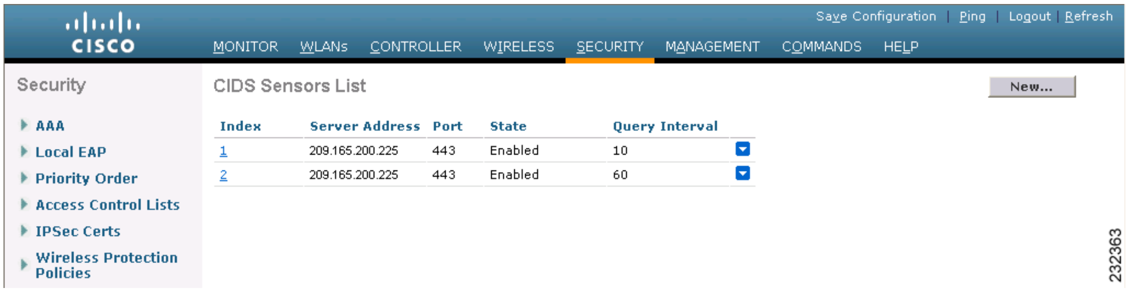
You can configure IDS sensors to detect various types of IP-level attacks in your network. When the sensors identify an attack, they can alert the controller to shun the offending client. When you add a new IDS sensor, you register the controller with that IDS sensor so that the controller can query the sensor to get the list of shunned clients. You can configure IDS sensor registration through either the GUI or the CLI.

Using the GUI to Configure IDS Sensors

Follow these steps to configure IDS sensors using the controller GUI.

Step 1 Click **Security** > **Advanced** > **CIDs** > **Sensors** to open the CIDS Sensors List page appears (see Figure 5-53).

Figure 5-53 CIDS Sensors List Page



CIDS Sensors List

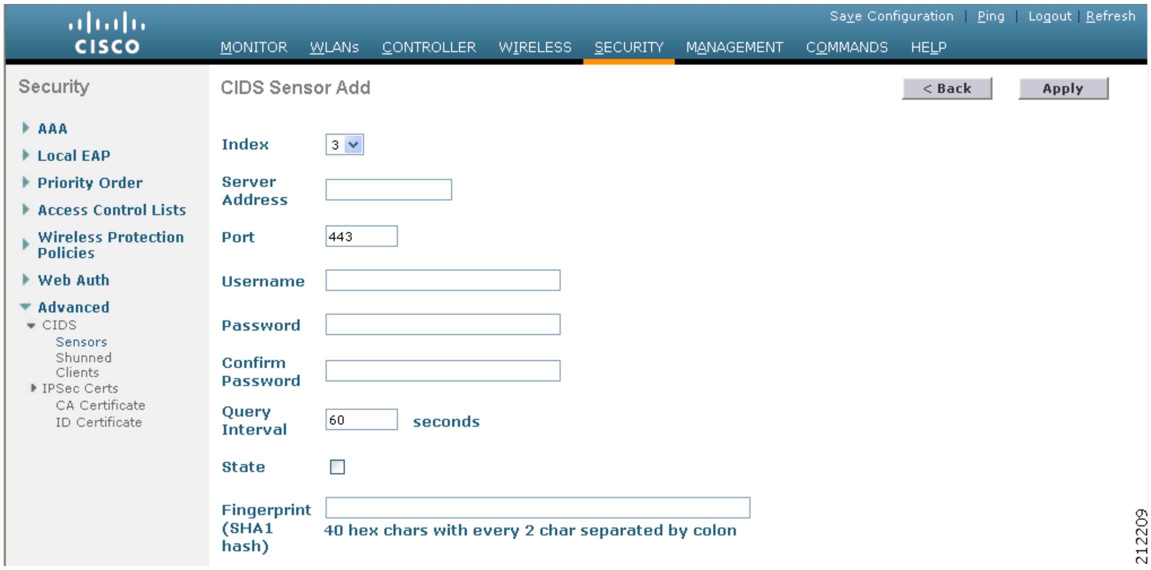
Index	Server Address	Port	State	Query Interval
1	209.165.200.225	443	Enabled	10
2	209.165.200.225	443	Enabled	60

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 To add an IDS sensor to the list, click **New**. The CIDS Sensor Add page appears (see Figure 5-54).

Figure 5-54 CIDS Sensor Add Page



CIDS Sensor Add

Index 3

Server Address

Port 443

Username

Password

Confirm Password

Query Interval 60 seconds

State ☐

Fingerprint (SHA1 hash)
40 hex chars with every 2 char separated by colon

Step 3 The controller supports up to five IDS sensors. From the Index drop-down box, 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 field, enter the IP address of your IDS server.

Step 5 The Port field contains the number of the HTTPS port through which the controller is to communicate with the IDS sensor. Cisco recommends that you set this parameter to 443 because the sensor uses this value to communicate by default.

Default: 443

Range: 1 to 65535

Step 6 In the Username field, 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 fields, enter the password that the controller uses to authenticate to the IDS sensor.

Step 8 In the Query Interval field, enter the time (in seconds) for how often the controller should query the IDS server for IDS events.

Default: 60 seconds

Range: 10 to 3600 seconds

Step 9 Check the **State** check box to register the controller with this IDS sensor or uncheck this check box to disable registration. The default value is disabled.

Step 10 Enter a 40-hexadecimal-character security key in the Fingerprint field. This key is used to verify the validity of the sensor and is used to prevent security attacks.

Note Do not include the colons that appear between every two bytes within the key. For example, enter AABBCCDD instead of 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.

Using the CLI to Configure IDS Sensors

Follow these steps to configure IDS sensors using the controller CLI.

Step 1 To add an IDS sensor, enter 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.

Note The username must be configured on the IDS sensor and have at least a read-only privilege.

Step 2 (Optional) To specify the number of the HTTPS port through which the controller is to communicate with the IDS sensor, enter 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 Cisco recommends that you use the default value of 443. The sensor uses this value to communicate by default.

Step 3 To specify how often the controller should query the IDS server for IDS events, enter 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 To enter a 40-hexadecimal-character security key used to verify the validity of the sensor, enter 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 To enable or disable this controller's registration with an IDS sensor, enter this command:

config wps cids-sensor {**enable** | **disable**} *index*

Step 6 To save your settings, enter this command:

save config

Step 7 To view the IDS sensor configuration, enter 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 8 To obtain debug information regarding IDS sensor configuration, enter this command:

debug wps cids enable

Note If you ever want to delete or change the configuration of a sensor, you must first disable it by entering **config wps cids-sensor disable** *index*. To then delete the sensor, enter **config wps cids-sensor delete** *index*.

Viewing 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 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. See Chapter 12 for more information on mobility groups.

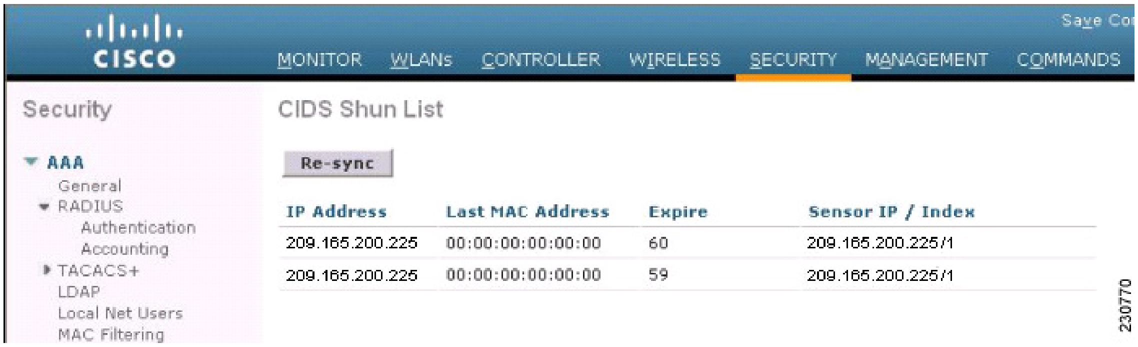
You can view the list of clients that the IDS sensors have identified to be shunned through either the GUI or the CLI.

Using the GUI to View Shunned Clients

Follow these steps to view the list of clients that the IDS sensors have identified to be shunned using the controller GUI.

Step 1 Click **Security** > **Advanced** > **CIDS** > **Shunned Clients**. The CIDS Shun List page appears (see Figure 5-55).

Figure 5-55 CIDS Shun List Page



CIDS Shun List

IP Address	Last MAC Address	Expire	Sensor IP / Index
209.165.200.225	00:00:00:00:00:00	60	209.165.200.225/1
209.165.200.225	00:00:00:00:00:00	59	209.165.200.225/1

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.

Using the CLI to View Shunned Clients

Follow these steps to view the list of clients that the IDS sensors have identified to be shunned using the controller CLI.

Step 1 To view the list of clients to be shunned, enter this command:

```
show wps shun-list
```

Step 2 To force the controller to sync up with other controllers in the mobility group for the shun list, enter this command:

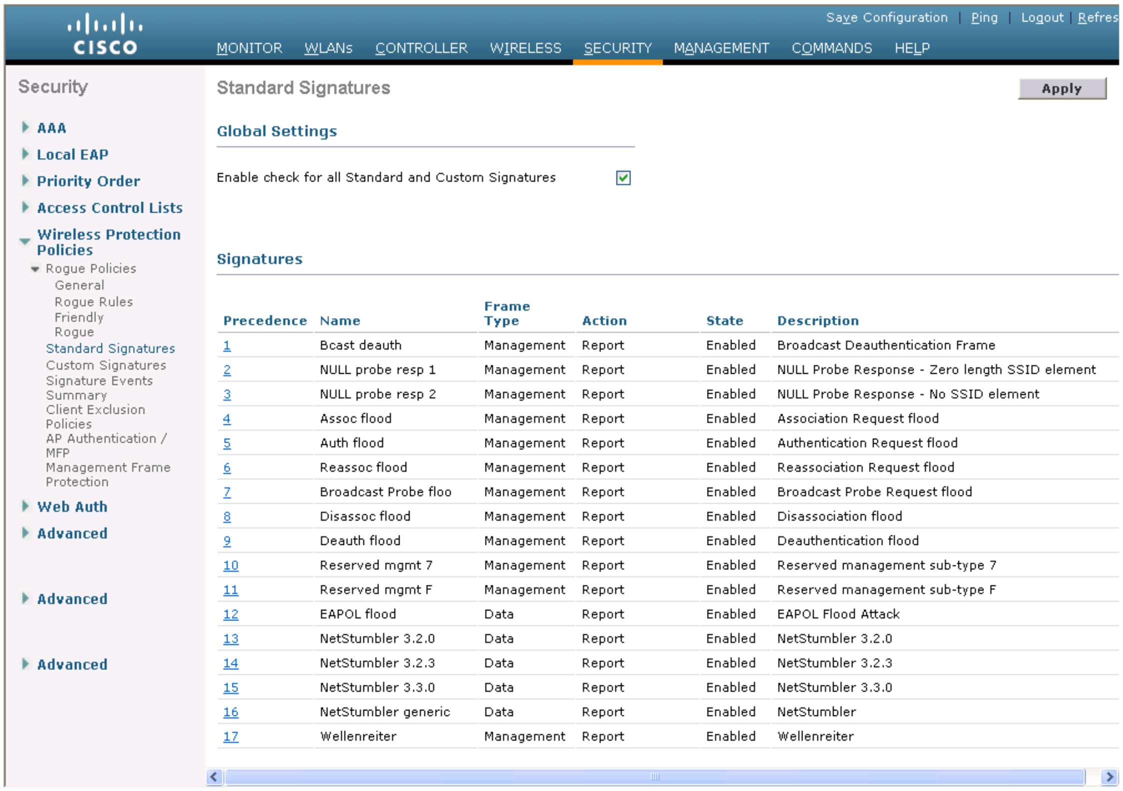
```
config wps shun-list re-sync
```

Configuring 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 (see Figure 5-56).

Figure 5-56 Standard Signatures Page



Standard Signatures

Global Settings

Enable check for all Standard and Custom Signatures ☑

Signatures

Precedence	Name	Frame Type	Action	State	Description
1	Bcast deauth	Management	Report	Enabled	Broadcast Deauthentication Frame
2	NULL probe resp 1	Management	Report	Enabled	NULL Probe Response - Zero length SSID element
3	NULL probe resp 2	Management	Report	Enabled	NULL Probe Response - No SSID element
4	Assoc flood	Management	Report	Enabled	Association Request flood
5	Auth flood	Management	Report	Enabled	Authentication Request flood
6	Reassoc flood	Management	Report	Enabled	Reassociation Request flood
7	Broadcast Probe floo	Management	Report	Enabled	Broadcast Probe Request flood
8	Disassoc flood	Management	Report	Enabled	Disassociation flood
9	Deauth flood	Management	Report	Enabled	Deauthentication flood
10	Reserved mgmt 7	Management	Report	Enabled	Reserved management sub-type 7
11	Reserved mgmt F	Management	Report	Enabled	Reserved management sub-type F
12	EAPOL flood	Data	Report	Enabled	EAPOL Flood Attack
13	NetStumbler 3.2.0	Data	Report	Enabled	NetStumbler 3.2.0
14	NetStumbler 3.2.3	Data	Report	Enabled	NetStumbler 3.2.3
15	NetStumbler 3.3.0	Data	Report	Enabled	NetStumbler 3.3.0
16	NetStumbler generic	Data	Report	Enabled	NetStumbler
17	Wellenreiter	Management	Report	Enabled	Wellenreiter

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 include:
  - 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 include:
  - 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 containing 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:

Version	String
3.2.0	“Flurble gronk bloopit, bnip Frundletrune”
3.2.3	“All your 802.11b are belong to us”
3.3.0	Sends white spaces

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 include:

  - 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. You can configure signatures through either the GUI or the CLI.

Using the GUI to Configure IDS Signatures

You must follow these instructions to configure signatures using the controller GUI:

- Uploading or downloading IDS signatures, page 5-110
- Enabling or disabling IDS signatures, page 5-111
- Viewing IDS signature events, page 5-114

Using the GUI to Upload or Download IDS Signatures

Follow these steps to upload or download IDS signatures using the controller GUI.

Step 1 If desired, create your own custom signature file.

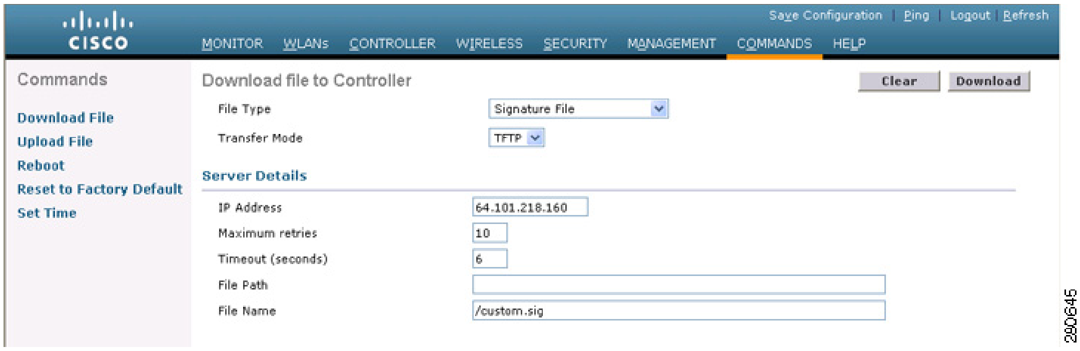
Step 2 Make sure that you have a Trivial File Transfer Protocol (TFTP) server available. Keep these guidelines in mind when setting up a TFTP server:

- 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 Click **Commands** to open the Download File to Controller page (see Figure 5-57).

Figure 5-57 Download File to Controller Page



Download file to Controller

File Type: Signature File

Transfer Mode: TFTP

Server Details

IP Address: 64.101.218.160

Maximum retries: 10

Timeout (seconds): 6

File Path:

File Name: /custom.sig

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 box on the Download File to Controller page.
- If you want to upload a standard signature file from the controller, click **Upload File** and then choose **Signature File** from the File Type drop-down box on the Upload File from Controller page.

Step 6 From the Transfer Mode drop-down box, choose **TFTP** or **FTP**.

Step 7 In the IP Address field, 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 the controller should attempt to download the signature file in the Maximum Retries field.

Range: 1 to 254

Default: 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 field.

Range: 1 to 254 seconds

Default: 6 seconds

Step 10 In the File Path field, enter the path of the signature file to be downloaded or uploaded. The default value is "/."

Step 11 In the File Name field, enter the name of the signature file to be downloaded or uploaded.

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 12 If you are using an FTP server, follow these steps:

a. In the Server Login Username field, enter the username to log into the FTP server.

b. In the Server Login Password field, enter the password to log into the FTP server.

c. In the Server Port Number field, enter the port number on the FTP server through which the download occurs. The default value is 21.

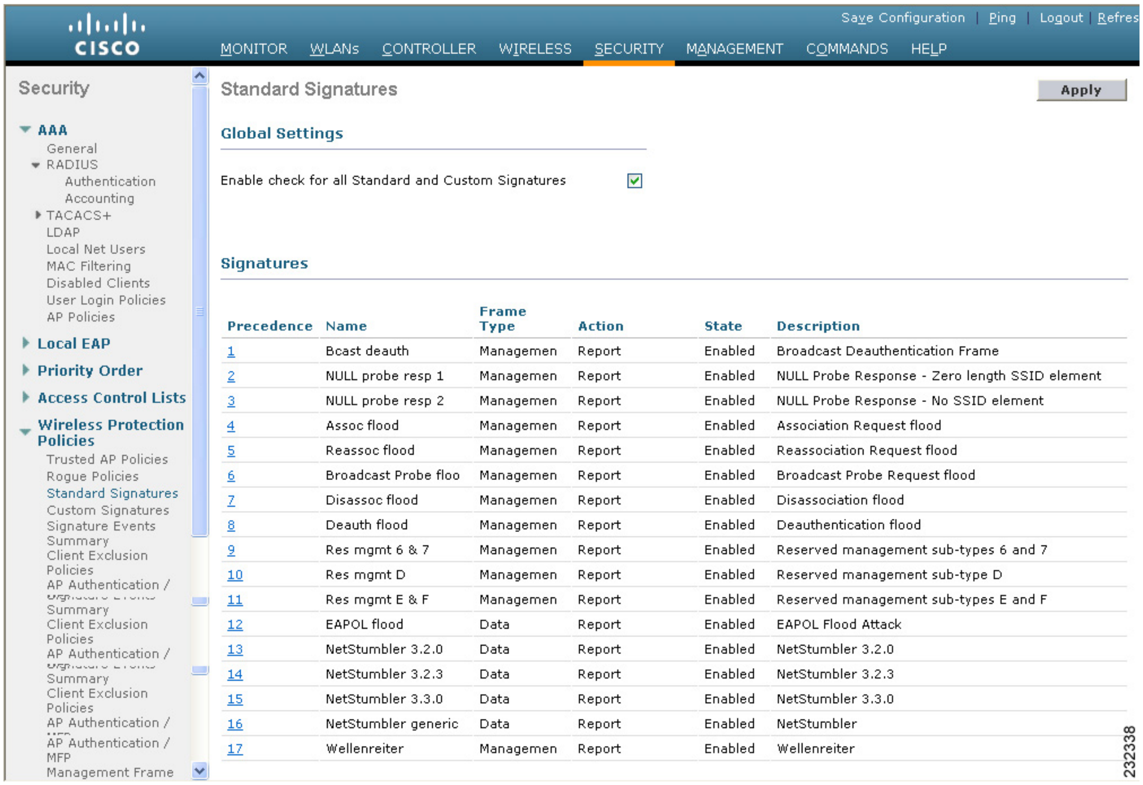
Step 13 Click **Download** to download the signature file to the controller or **Upload** to upload the signature file from the controller.

Using the GUI to Enable or Disable IDS Signatures

Follow these steps to enable or disable IDS signatures using the controller GUI.

Step 1 Click **Security** > **Wireless Protection Policies** > **Standard Signatures** or **Custom Signatures**. The Standard Signatures page (see Figure 5-58) or the Custom Signatures page appears.

Figure 5-58 Standard Signatures Page



Standard Signatures

Global Settings

Enable check for all Standard and Custom Signatures ☑

Signatures

Precedence	Name	Frame Type	Action	State	Description
1	Bcast deauth	Managemen	Report	Enabled	Broadcast Deauthentication Frame
2	NULL probe resp 1	Managemen	Report	Enabled	NULL Probe Response - Zero length SSID element
3	NULL probe resp 2	Managemen	Report	Enabled	NULL Probe Response - No SSID element
4	Assoc flood	Managemen	Report	Enabled	Association Request flood
5	Reassoc flood	Managemen	Report	Enabled	Reassociation Request flood
6	Broadcast Probe floo	Managemen	Report	Enabled	Broadcast Probe Request flood
7	Disassoc flood	Managemen	Report	Enabled	Disassociation flood
8	Deauth flood	Managemen	Report	Enabled	Deauthentication flood
9	Res mgmt 6 & 7	Managemen	Report	Enabled	Reserved management sub-types 6 and 7
10	Res mgmt D	Managemen	Report	Enabled	Reserved management sub-type D
11	Res mgmt E & F	Managemen	Report	Enabled	Reserved management sub-types E and F
12	EAPOL flood	Data	Report	Enabled	EAPOL Flood Attack
13	NetStumbler 3.2.0	Data	Report	Enabled	NetStumbler 3.2.0
14	NetStumbler 3.2.3	Data	Report	Enabled	NetStumbler 3.2.3
15	NetStumbler 3.3.0	Data	Report	Enabled	NetStumbler 3.3.0
16	NetStumbler generic	Data	Report	Enabled	NetStumbler
17	Wellenreiter	Managemen	Report	Enabled	Wellenreiter

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 action 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.

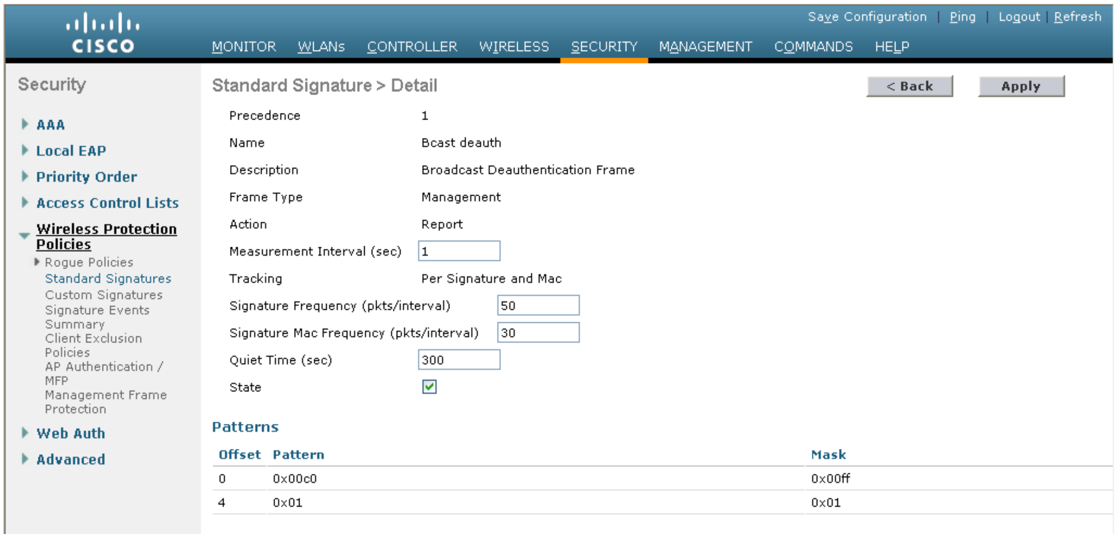
Step 2 Perform one of the following:

- If you want to allow all signatures (both standard and custom) whose individual states are set to Enabled to remain enabled, check 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. The default value is enabled (or checked). 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, uncheck the **Enable Check for All Standard and Custom Signatures** check box. If you uncheck 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 To enable or disable an individual signature, click the precedence number of the desired signature. The Standard Signature (or Custom Signature) > Detail page appears (see Figure 5-59).

Figure 5-59 Standard Signature > Detail Page



Standard Signature > Detail

Precedence	1
Name	Bcast deauth
Description	Broadcast Deauthentication Frame
Frame Type	Management
Action	Report
Measurement Interval (sec)	1
Tracking	Per Signature and Mac
Signature Frequency (pkts/interval)	50
Signature Mac Frequency (pkts/interval)	30
Quiet Time (sec)	300
State	☑

Patterns

Offset	Pattern	Mask
0	0x00c0	0x00ff
4	0x01	0x01

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:
  - 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 field, 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 field, 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 field, 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 field, 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 Check the **State** check box to enable this signature to detect security attacks or uncheck it to disable this signature. The default value is enabled (or checked).

Step 10 Click **Apply** to commit your changes. The Standard Signatures or Custom Signatures page reflects the signature's updated state.

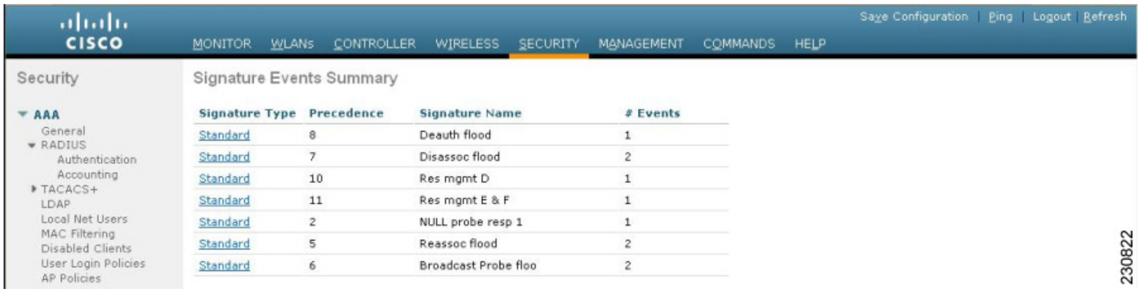
Step 11 Click **Save Configuration** to save your changes.

Using the GUI to View IDS Signature Events

Follow these steps to view signature events using the controller GUI.

Step 1 Click **Security** > **Wireless Protection Policies** > **Signature Events Summary**. The Signature Events Summary page appears (see Figure 5-60).

Figure 5-60 Signature Events Summary Page



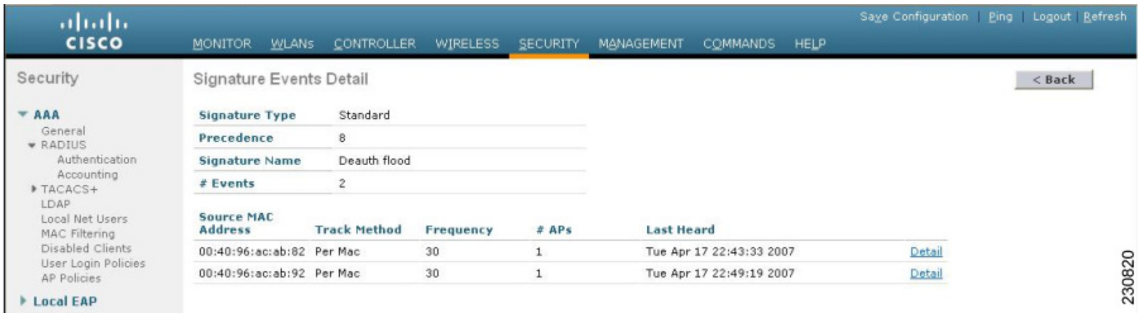
Signature Events Summary

Signature Type	Precedence	Signature Name	# Events
Standard	8	Deauth flood	1
Standard	7	Disassoc flood	2
Standard	10	Res mgmt D	1
Standard	11	Res mgmt E & F	1
Standard	2	NULL probe resp 1	1
Standard	5	Reassoc flood	2
Standard	6	Broadcast Probe floo	2

This page shows the number of attacks detected by the enabled signatures.

Step 2 To see more information on the attacks detected by a particular signature, click the signature type link for that signature. The Signature Events Detail page appears (see Figure 5-61).

Figure 5-61 Signature Events Detail Page



Signature Events Detail

Signature Type	Standard
Precedence	8
Signature Name	Deauth flood
# Events	2

Source MAC Address	Track Method	Frequency	# APs	Last Heard	
00:40:96:ac:ab:82	Per Mac	30	1	Tue Apr 17 22:43:33 2007	Detail
00:40:96:ac:ab:92	Per Mac	30	1	Tue Apr 17 22:49:19 2007	Detail

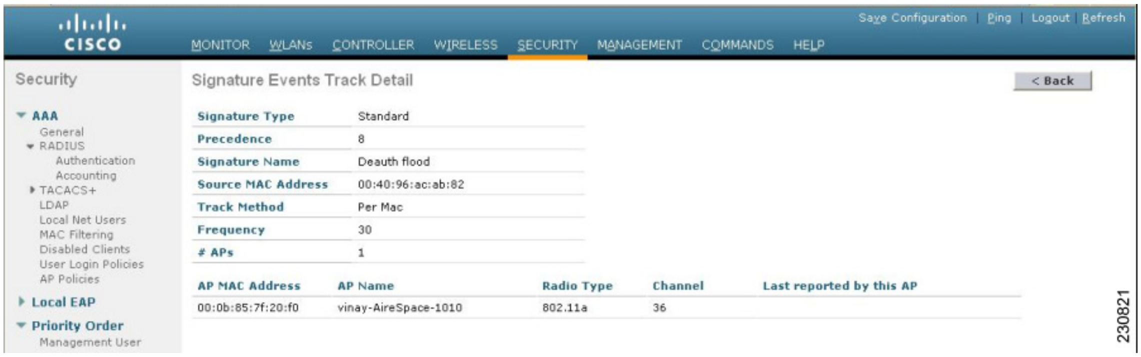
This page shows the following information:

- 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 To see more information for a particular attack, click the **Detail** link for that attack. The Signature Events Track Detail page appears (see Figure 5-62).

Figure 5-62 Signature Events Track Detail Page



Signature Events Track Detail

Signature Type	Standard
Precedence	8
Signature Name	Deauth flood
Source MAC Address	00:40:96:ac:ab:82
Track Method	Per Mac
Frequency	30
# APs	1

AP MAC Address	AP Name	Radio Type	Channel	Last reported by this AP
00:0b:85:7f:20:f0	vinay-AireSpace-1010	802.11a	36	

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

Using the CLI to Configure IDS Signatures

Follow these steps to configure IDS signatures using the controller 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 "Using the GUI to Upload or Download IDS Signatures" section on page 5-110.

Step 3 Copy the custom signature file (*.sig) to the default directory on your TFTP server.

Step 4 To specify the download or upload mode, enter **transfer** {**download** | **upload**} **mode tftp**.

Step 5 To specify the type of file to be downloaded or uploaded, enter **transfer** {**download** | **upload**} **datatype signature**.

Step 6 To specify the IP address of the TFTP server, enter **transfer** {**download** | **upload**} **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 7 To specify the download or upload path, enter **transfer** {**download | upload**} **path** *absolute-tftp-server-path-to-file*.

Step 8 To specify the file to be downloaded or uploaded, enter **transfer** {**download | upload**} **filename** *filename.sig*.

> **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 **transfer** {**download | upload**} **start** and answer **y** to the prompt to confirm the current settings and start the download or upload.

Step 10 To specify the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval, enter 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 To specify the number of matching packets per interval that must be identified at the individual access point level before an attack is detected, enter 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 To specify the number of matching packets per interval that must be identified per client per access point before an attack is detected, enter 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 To 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, enter this command:

config 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 To enable or disable IDS signatures, perform one of the following:

- To enable or disable an individual IDS signature, enter this command:

  config 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:

  config 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 To save your changes, enter 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:

config wps signature reset {*signature_id* | **all**}

Note You can reset signatures to default values only through the controller CLI.

Using the CLI to View IDS Signature Events

Use these commands to view signature events using the controller CLI.

1. To see whether IDS signature processing is enabled or disabled on the controller, enter this command:

   show wps summary

   Information similar to the following appears:

```
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.

2. To see individual summaries of all of the standard and custom signatures installed on the controller, enter 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
```

3. To see the number of attacks detected by the enabled signatures, enter 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
```

4. To see more information on the attacks detected by a particular standard or custom signature, enter 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
```

5. To see information on attacks that are tracked by access points on a per-signature and per-channel basis, enter this command:

   show wps signature events {**standard** | **custom**} *precedence#* **detailed per-signature** *source_mac*

6. To see information on attacks that are tracked by access points on an individual-client basis (by MAC address), enter 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

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 is an appliance-based solution that 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.

The Cisco Adaptive wIPS is not configured on the controller. Instead, WCS forwards the profile configuration to the wIPS service, which in turn 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.

Access points in monitor mode 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.

Note In all of the above cases, the controller functions solely as a forwarding device.

Note For more information on the Cisco Adaptive wIPS, refer to the *Cisco Wireless Control System Configuration Guide, Release 5.2* and the *Cisco 3300 Series Mobility Services Engine Configuration Guide, Release 5.2*.

Configuring wIPS on an Access Point

Using the controller CLI, follow these steps to configure wIPS on an access point. These steps are required in order to enable wIPS.

Step 1 To configure an access point for monitor mode, enter 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 To save your changes, enter this command:

save config

Step 4 To disable the access point radio, enter this command:

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

Step 5 To configure the wIPS submode on the access point, enter this command:

config ap mode monitor submode wips *Cisco_AP*

Note To disable wIPS on the access point, enter this command: **config ap mode monitor submode none** *Cisco_AP*.

Step 6 To enable wIPS optimized channel scanning for the access point, enter 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. Three channel sets are available:

- **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 non-overlapping channels allowed in the access point's country of operation

The 802.11a or 802.11b Monitor Channels field 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 To re-enable the access point radio, enter this command:

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

Step 8 To save your changes, enter this command:

save config

Viewing wIPS Information

Using the controller CLI, enter these commands to view wIPS information.

Note You can also view the access point submode from the controller GUI. To do so, click **Wireless** > **Access Points** > **All APs** > the access point name > the **Advanced** tab. The AP Sub Mode field shows *wIPS* if the access point in is 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.

1. To view the wIPS submode on the access point, enter 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
...
```

2. To see the wIPS optimized channel scanning configuration on the access point, enter 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
```

3. To view the wIPS configuration forwarded by WCS to the controller, enter this command:

   show wps wips summary

   Information similar to the following appears:

```
Policy Name.............. Default
Policy Version.......... 3
```

4. To view the current state of wIPS operation on the controller, enter 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
NMSP Transmit Packets Dropped......... 0
NMSP Largest Packet................... 1377
```

5. To clear the wIPS statistics on the controller, enter this command:

   clear stats wps wips

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.

Configuring Maximum Local Database Entries

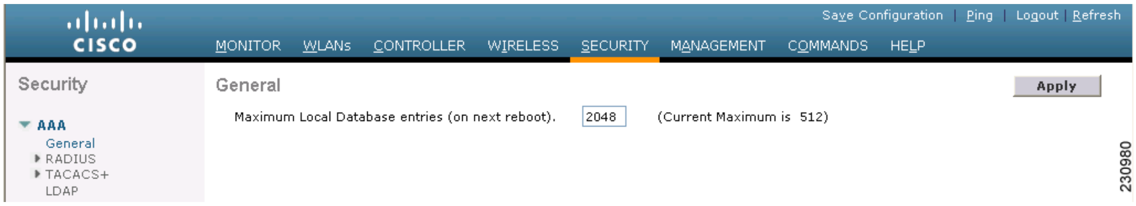
You can use the controller GUI or CLI to specify the maximum local database entries used for storing user authentication information. The information in the database is used in conjunction with the controller's web authentication feature.

Using the GUI to Configure Maximum Local Database Entries

Follow these steps to configure a controller to use the maximum local database entries using the GUI.

Step 1 Click **Security** > **AAA** > **General** to open the General page (see Figure 5-63).

Figure 5-63 General Page


cisco
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
General
RADIUS
TACACS+
LDAP
Apply
230980

General

Maximum Local Database entries (on next reboot). 2048 (Current Maximum is 512)

Step 2 Enter the desired maximum value (on the next controller reboot) in the Maximum Local Database Entries field. The range of possible values is 512 to 2048 (which also includes any configured MAC filter entries). The default value is 2048. The current value appears in parentheses to the right of the field.

Step 3 Click **Apply** to commit your changes.

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

Using the CLI to Specify the Maximum Number of Local Database Entries

To configure the maximum number of local database entries using the CLI, enter this command:

config database size *max_entries*

CHAPTER 6

Configuring WLANsWireless Device Access

This chapter describes how to configure up to 512 WLANs for your Cisco UWN Solution. It contains these sections:

- WLAN Overview, page 6-2
- Configuring WLANs, page 6-2

WLAN Overview

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 unique security policies. The controller publishes up to 16 WLANs to each connected access point, but you can create up to 512 WLANs on the controller and then selectively publish these WLANs (using access point groups) to different access points to better manage your wireless network.

Note Cisco 2106, 2112, and 2125 controllers support only up to 16 WLANs.

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. Refer to the "Creating Access Point Groups" section on page 6-44 for more information on access point groups.

Note Controller software releases prior to 5.2 support up to only 16 WLANs. Cisco does not support downgrading the controller from software release 5.2 to a previous release as inconsistencies might occur for WLANs and wired guest LANs. As a result, you would need to reconfigure your WLAN, mobility anchor, and wired LAN configurations.

Note Cisco recommends 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 WLANs

These sections describe how to configure WLANs:

- Creating WLANs, page 6-3
- Searching WLANs, page 6-7
- Configuring DHCP, page 6-8
- Configuring MAC Filtering for WLANs, page 6-14
- Assigning WLANs to Interfaces, page 6-15
- Configuring the DTIM Period, page 6-16
- Configuring Peer-to-Peer Blocking, page 6-18
- Configuring Layer 2 Security, page 6-20
- Configuring a Session Timeout, page 6-27
- Configuring Layer 3 Security, page 6-28
- Assigning a QoS Profile to a WLAN, page 6-30
- Configuring QoS Enhanced BSS, page 6-32
- Configuring IPv6 Bridging, page 6-36
- Configuring Cisco Client Extensions, page 6-39

- Configuring Access Point Groups, page 6-42
- Configuring Web Redirect with 802.1X Authentication, page 6-49
- Disabling Accounting Servers per WLAN, page 6-53
- Disabling Coverage Hole Detection per WLAN, page 6-54
- Configuring NAC Out-of-Band Integration, page 6-55

Creating WLANs

This section provides instructions for creating up to 512 WLANs using either the controller GUI or CLI.

Note Each AP can broadcast only up to 16 WLANs.

WLANs with ID that is higher than 16 are not applied to the default AP group, regardless of the number of WLANs configured. For WLANs with ID that is higher than 16, you need to configure a separate AP group.

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. Creating WLANs with the same SSID enables you to assign different Layer 2 security policies within the same wireless LAN. To distinguish among WLANs with the same SSID, you must create a unique profile name for each WLAN.

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. These are the available Layer 2 security policies:

- 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

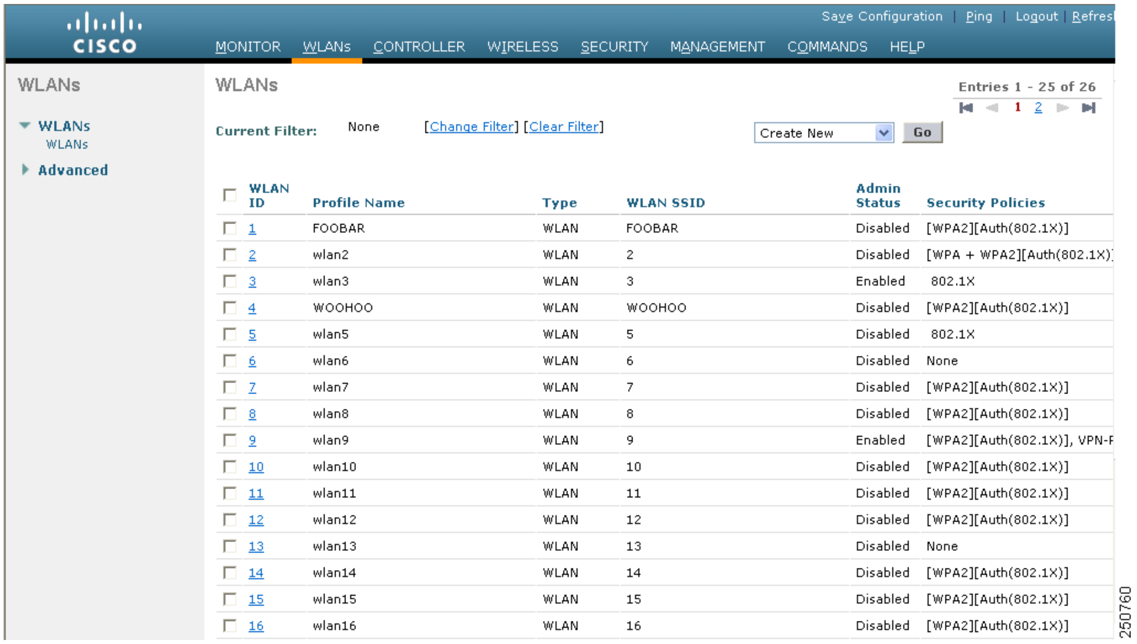
  Note Although WPA and WPA2 cannot both be used by multiple WLANs with the same SSID, two WLANs with the same SSID could be configured with WPA/TKIP with PSK and WPA/TKIP with 802.1X, respectively, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X, respectively.

Using the GUI to Create WLANs

Follow these steps to create WLANs using the GUI.

Step 1 Click **WLANs** to open the WLANs page (see Figure 6-1).

Figure 6-1 WLANs Page


Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
Entries 1 - 25 of 26
1 2
Create New
Go
250760

WLANs

Current Filter: None [Change Filter] [Clear Filter]

□	WLAN ID	Profile Name	Type	WLAN SSID	Admin Status	Security Policies
□	1	FOOBAR	WLAN	FOOBAR	Disabled	[WPA2][Auth(802.1X)]
□	2	wlan2	WLAN	2	Disabled	[WPA + WPA2][Auth(802.1X)
□	3	wlan3	WLAN	3	Enabled	802.1X
□	4	WOOHOO	WLAN	WOOHOO	Disabled	[WPA2][Auth(802.1X)]
□	5	wlan5	WLAN	5	Disabled	802.1X
□	6	wlan6	WLAN	6	Disabled	None
□	7	wlan7	WLAN	7	Disabled	[WPA2][Auth(802.1X)]
□	8	wlan8	WLAN	8	Disabled	[WPA2][Auth(802.1X)]
□	9	wlan9	WLAN	9	Enabled	[WPA2][Auth(802.1X)], VPN-F
□	10	wlan10	WLAN	10	Disabled	[WPA2][Auth(802.1X)]
□	11	wlan11	WLAN	11	Disabled	[WPA2][Auth(802.1X)]
□	12	wlan12	WLAN	12	Disabled	[WPA2][Auth(802.1X)]
□	13	wlan13	WLAN	13	Disabled	None
□	14	wlan14	WLAN	14	Disabled	[WPA2][Auth(802.1X)]
□	15	wlan15	WLAN	15	Disabled	[WPA2][Auth(802.1X)]
□	16	wlan16	WLAN	16	Disabled	[WPA2][Auth(802.1X)]

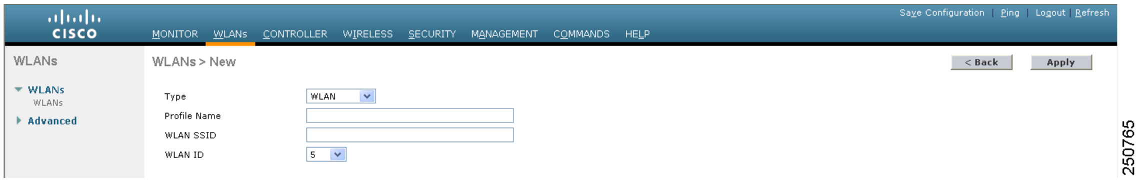
This page lists all of the WLANs currently configured on the controller. For each WLAN, you can see its WLAN ID, profile name, type, SSID, status, and security policies.

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 check the check box to the left of the WLAN, choose **Remove Selected** from the drop-down box, 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 To create a new WLAN, choose **Create New** from the drop-down box and click **Go**. The WLANs > New page appears (see Figure 6-2).

Figure 6-2 WLANs > New Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
250765

WLANs > New

Type: WLAN

Profile Name:

WLAN SSID:

WLAN ID: 5

Step 3 From the Type drop-down box, choose **WLAN** to create a WLAN.

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 10-23.

Step 4 In the Profile Name field, enter up to 32 alphanumeric characters for the profile name to be assigned to this WLAN. The profile name must be unique.

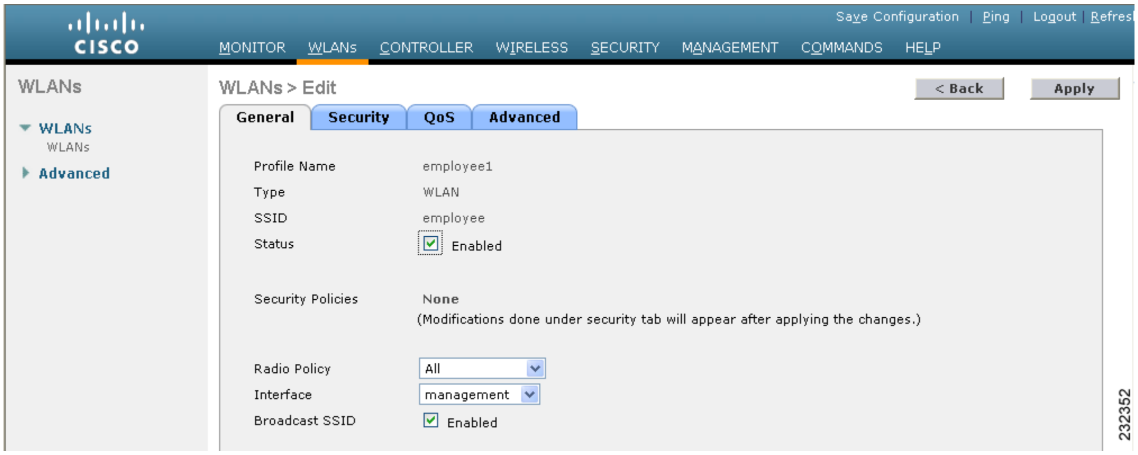
Step 5 In the WLAN SSID field, enter up to 32 alphanumeric characters for the SSID to be assigned to this WLAN.

Step 6 From the WLAN ID drop-down box, choose the ID number for this WLAN.

Step 7 Click **Apply** to commit your changes. The WLANs > Edit page appears (see Figure 6-3).

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.

Figure 6-3 WLANs > Edit Page



Profile Name employee1
Type WLAN
SSID employee
Status ☑ Enabled

Security Policies None
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All
Interface management
Broadcast SSID ☑ Enabled

Step 8 Use the parameters on the General, Security, QoS, and Advanced tabs to configure this WLAN. Refer to the sections in the rest of this chapter for instructions on configuring specific features for WLANs.

Step 9 On the General tab, check the **Status** check box to enable this WLAN. Be sure to leave it unchecked until you have finished making configuration changes to the WLAN.

Note You can also enable or disable WLANs from the WLANs page by checking 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 box, and clicking **Go**.

Step 10 Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Using the CLI to Create WLANs

Use these commands to create WLANs using the CLI.

1. To view the list of existing WLANs and to see whether they are enabled or disabled, enter this command:

   show wlan summary

2. To create a new WLAN, enter this command:

   config wlan create *wlan_id* {*profile_name* | *foreign_ap*} *ssid*

   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 10-23.

3. To disable a WLAN (for example, before making any modifications to a WLAN), enter this command:

   config wlan disable {*wlan_id* | *foreign_ap* | **all**}

   where

   - *wlan_id* is a WLAN ID between 1 and 512 (inclusive),
   - *foreign_ap* is a third-party access point, and
   - **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.

4. To enable a WLAN (for example, after you have finished making configuration changes to the WLAN), enter 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").

5. To delete a WLAN, enter 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.

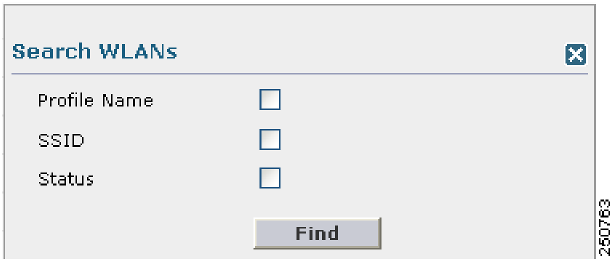
Searching WLANs

You can search for specific WLANs in the list of up to 512 WLANs on the WLANs page. This feature is especially useful if your WLANs span multiple pages, preventing you from viewing them all at once.

Follow these steps to search for WLANs using the controller GUI.

Step 1 On the WLANs page, click **Change Filter**. The Search WLANs window appears (see Figure 6-4).

Figure 6-4 Search WLANs Window



Step 2 Perform one of the following:

- To search for WLANs based on profile name, check the **Profile Name** check box and enter the desired profile name in the edit box.
- To search for WLANs based on SSID, check the **SSID** check box and enter the desired SSID in the edit box.
- To search for WLANs based on their status, check the **Status** check box and choose **Enabled** or **Disabled** from the drop-down box.
- To close the Search WLANs window without making any changes, click the **X** in the upper right-hand corner.

Step 3 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**.

Configuring DHCP

WLANs can be configured 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.

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, appliance-mode access points on the management interface, 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, priming, or over-the-air discovery.

Note Refer to Chapter 7 or the *Controller Deployment Guide* at this URL for more information on how access points find controllers:

http://www.cisco.com/en/US/products/ps6366/prod_technical_reference_list.html

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. This means that each controller appears as a DHCP Relay agent to the DHCP server. This also means that the controller appears 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.

Per-Interface Assignment

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 Refer to Chapter 3 for information on configuring the controller’s interfaces.

Per-WLAN Assignment

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, Cisco recommends 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 be 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 5-52 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.

You are also allowed to create separate WLANs with DHCP Addr. Assignment Required disabled; then define the primary / secondary DHCP server as 0.0.0.0 on the interface assigned to the WLAN. These WLANs drop all DHCP requests and force clients to use a static IP address. Note that these WLANs do not support management over wireless connections.

Note Refer to Chapter 4 for instructions on globally configuring DHCP proxy.

This section provides both GUI and CLI instructions for configuring DHCP.

Using the GUI to Configure DHCP

Follow these steps to configure DHCP using the GUI.

Step 1 Follow the instructions in the "Using the GUI to Configure the Management, AP-Manager, Virtual, and Service-Port Interfaces" section on page 3-11 or "Using the GUI to Configure Dynamic Interfaces" section on page 3-16 to configure a primary DHCP server for a management, AP-manager, or dynamic interface that will be assigned to the WLAN.

> **Note** 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 2 Click **WLANs** to open the WLANs page.

Step 3 Click the ID number of the WLAN for which you wish to assign an interface. The WLANs > Edit (General) page appears.

Step 4 On the General tab, uncheck the **Status** check box and click **Apply** to disable the WLAN.

Step 5 Re-click the ID number of the WLAN.

Step 6 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 box.

Step 7 Click the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 8 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, check the **DHCP Server Override** check box and enter the IP address of the desired DHCP server in the **DHCP Server IP Addr** edit 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.

Step 9 If you want to require all clients to obtain their IP addresses from a DHCP server, check 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.

Step 10 Click **Apply** to commit your changes.

Step 11 On the General tab, check the **Status** check box and click **Apply** to re-enable the WLAN.

Step 12 Click **Save Configuration** to save your changes.

Using the CLI to Configure DHCP

Follow these steps to configure DHCP using the CLI.

Step 1 Follow the instructions in the "Using the GUI to Configure the Management, AP-Manager, Virtual, and Service-Port Interfaces" section on page 3-11 or "Using the GUI to Configure Dynamic Interfaces" section on page 3-16 to configure a primary DHCP server for a management, AP-manager, or dynamic interface that will be assigned to the WLAN.

Step 2 To disable the WLAN, enter this command:

config wlan disable *wlan_id*

Step 3 To specify the interface for which you configured a primary DHCP server to be used with this WLAN, enter this command:

config wlan interface *wlan_id interface_name*

Step 4 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.

Step 5 To re-enable the WLAN, enter this command:

config wlan enable *wlan_id*

Using the CLI to Debug DHCP

Use these CLI commands to obtain debug information:

- **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 network administrators 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.

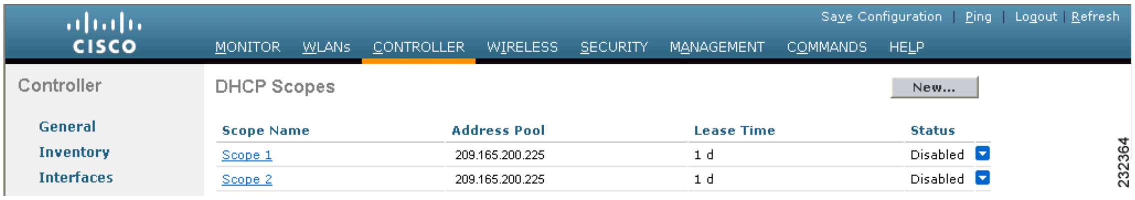
DHCP scopes are needed for internal DHCP to work. Once DHCP is defined on the controller, we can then point the primary DHCP server IP address on the management, AP-manager, and dynamic interfaces to controller's management interface. You can configure up to 16 DHCP scopes using the controller GUI or CLI.

Using the GUI to Configure DHCP Scopes

Follow these steps to configure DHCP scopes using the GUI.

Step 1 Click **Controller** > **Internal DHCP Server** > **DHCP Scope** to open the DHCP Scopes page (see Figure 6-5).

Figure 6-5 DHCP Scopes Page



DHCP Scopes

Scope Name	Address Pool	Lease Time	Status
Scope 1	209.165.200.225	1 d	Disabled
Scope 2	209.165.200.225	1 d	Disabled

This page lists any DHCP scopes that have already been configured.

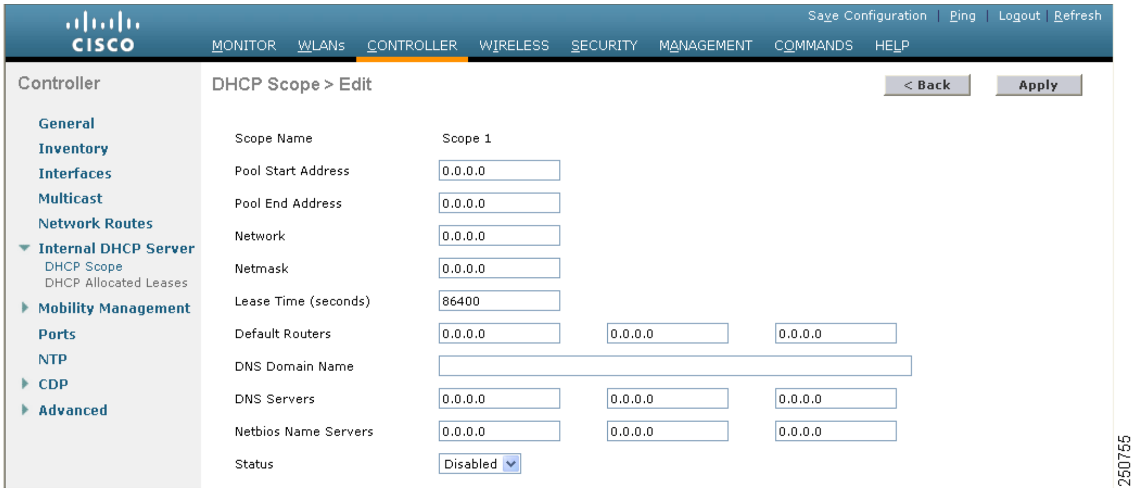
Note If you ever want to delete an existing DHCP scope, hover your cursor over the blue drop-down arrow for that scope and choose **Remove**.

Step 2 To add a new DHCP scope, click **New**. The DHCP Scope > New page appears.

Step 3 In the Scope Name field, 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 (see Figure 6-6).

Figure 6-6 DHCP Scope > Edit Page



DHCP Scope > Edit

Scope Name	Scope 1		
Pool Start Address	0.0.0.0		
Pool End Address	0.0.0.0		
Network	0.0.0.0		
Netmask	0.0.0.0		
Lease Time (seconds)	86400		
Default Routers	0.0.0.0	0.0.0.0	0.0.0.0
DNS Domain Name			
DNS Servers	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
Status	Disabled		

Step 5 In the Pool Start Address field, 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 field, 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 field, enter the network served by this DHCP scope. This is the IP address used by the management interface with Netmask applied, as configured on the Interfaces page.

Step 8 In the Netmask field, enter the subnet mask assigned to all wireless clients.

Step 9 In the Lease Time field, 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 field, enter the IP address of the optional router(s) 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 field, 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 field, enter the IP address of the optional DNS server(s). 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 field, enter the IP address of the optional Microsoft Network Basic Input Output System (NetBIOS) name server(s), such as a s Internet Naming Service (WINS) server.

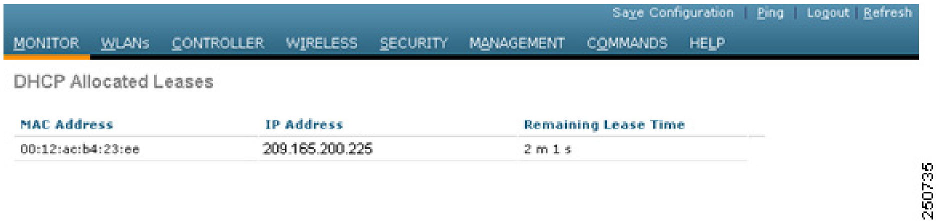
Step 14 From the Status drop-down box, choose **Enabled** to enable this DHCP scope or **Disabled** to disable it.

Step 15 Click **Apply** to commit your changes.

Step 16 Click **Save Configuration** to save your changes.

Step 17 To see the remaining lease time for wireless clients, click **DHCP Allocated Leases**. The DHCP Allocated Lease page appears (see Figure 6-7), showing the MAC address, IP address, and remaining lease time for the wireless clients.

Figure 6-7 DHCP Allocated Lease Page



DHCP Allocated Leases

MAC Address	IP Address	Remaining Lease Time
00:12:ac:b4:23:ee	209.165.200.225	2 m 1 s

Using the CLI to Configure DHCP Scopes

Follow these steps to configure DHCP scopes using the CLI.

Step 1 To create a new DHCP scope, enter 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 To specify the starting and ending IP address in the range assigned to the clients, enter 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 To specify the network served by this DHCP scope (the IP address used by the management interface with Netmask applied) and the subnet mask assigned to all wireless clients, enter this command:

config dhcp network *scope network netmask*

Step 4 To specify the amount of time (from 0 to 65536 seconds) that an IP address is granted to a client, enter this command:

config dhcp lease *scope lease_duration*

Step 5 To specify the IP address of the optional router(s) connecting the controllers, enter 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 To specify the optional domain name system (DNS) domain name of this DHCP scope for use with one or more DNS servers, enter this command:

config dhcp domain *scope domain*

Step 7 To specify the IP address of the optional DNS server(s), enter 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 To specify the IP address of the optional Microsoft Network Basic Input Output System (NetBIOS) name server(s), such as a s Internet Naming Service (WINS) server, enter this command:

config dhcp netbios-name-server *scope wins1* [*wins2*] [*wins3*]

Step 9 To enable or disable this DHCP scope, enter this command:

config dhcp {**enable** | **disable**} *scope*

Step 10 To save your changes, enter this command:

save config

Step 11 To see the list of configured DHCP scopes, enter this command:

show dhcp summary

Information similar to the following appears:

```
Scope Name           Enabled             Address Range
Scope 1                No          0.0.0.0 -> 0.0.0.0
Scope 2                No          0.0.0.0 -> 0.0.0.0
```

Step 12 To display the DHCP information for a particular scope, enter 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
```

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.

Enabling MAC Filtering

Use these commands to enable MAC filtering on a WLAN:

- Enter **config wlan mac-filtering enable** *wlan_id* to enable MAC filtering.
- Enter **show wlan** to verify that you have MAC filtering enabled for the WLAN.

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.

Creating a Local MAC Filter

Controllers have built-in MAC filtering capability, similar to that provided by a RADIUS authorization server.

Use these commands to add MAC addresses to a WLAN MAC filter:

- Enter **config macfilter add** *mac_addr wlan_id* [*interface_name*] [*description*] [*IP_addr*] to create a MAC filter entry on the controller, where the following parameters are optional:
  - *interface_name*—The name of the interface.
  - *description*—A brief description of the interface in double quotes (for example, “Interface1”).
  - *IP_addr*—The IP address of the local MAC filter database.
- Enter **config macfilter ip-address** *mac_addr IP_addr* to assign an IP address to an existing MAC filter entry, if one was not assigned in the **config macfilter add** command.
- Enter **show macfilter** to verify that MAC addresses are assigned to the WLAN.

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:

- Enter **config wlan exclusionlist** *wlan_id timeout* to configure the timeout for disabled clients. Enter a timeout from **1** to **65535** seconds, or enter **0** to permanently disable the client.
- Use the **show wlan** command to verify the current timeout.

Assigning WLANs to Interfaces

Use these commands to assign a WLAN to an interface:

- Enter this command to assign a WLAN to an interface:

  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.
- Enter **show wlan summary** to verify the interface assignment status.

Configuring 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.

Normally, 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 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 longer battery life.

Many applications cannot tolerate a long time between broadcast and multicast messages, resulting in poor protocol and application performance. Cisco recommends 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, 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.

Note When you upgrade the controller software to release 5.0 or later, the DTIM period that was configured for a radio network is copied to all of the existing WLANs on the controller.

Using the GUI to Configure the DTIM Period

Using the GUI, follow these steps to configure the DTIM period for a WLAN.

Step 1 Click **WLANs** to open the WLANs page.

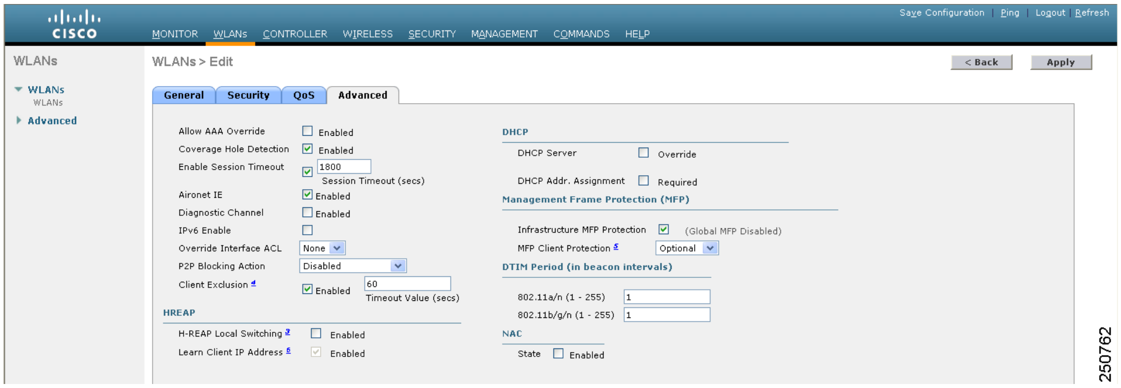
Step 2 Click the ID number of the WLAN for which you want to configure the DTIM period.

Step 3 Uncheck the **Status** check box to disable the WLAN.

Step 4 Click **Apply** to commit your changes.

Step 5 Click the **Advanced** tab to open the WLANs > Edit (Advanced) page (see Figure 6-8).

Figure 6-8 WLANs > Edit (Advanced) Page



Allow AAA Override ☐ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel ☐ Enabled
IPv6 Enable ☐
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] ☑ Enabled 60 Timeout Value (secs)

HREAP
H-REAP Local Switching [2] ☐ Enabled
Learn Client IP Address [5] ☑ Enabled

DHCP
DHCP Server ☐ Override
DHCP Addr. Assignment ☐ Required

Management Frame Protection (MFP)
Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
State ☐ Enabled

Step 6 Under DTIM Period, enter a value between 1 and 255 (inclusive) in the 802.11a/n and 802.11b/g/n fields. The default value is 1 (transmit broadcast and multicast frames after every beacon).

Step 7 Click **Apply** to commit your changes.

Step 8 Click the **General** tab to open the WLANs > Edit (General) page.

Step 9 Check the **Status** check box to re-enable the WLAN.

Step 10 Click **Save Configuration** to save your changes.

Using the CLI to Configure the DTIM Period

Using the CLI, follow these steps to configure the DTIM period for a WLAN.

Step 1 To disable the WLAN, enter this command:

config wlan disable *wlan_id*

Step 2 To configure the DTIM period for either the 802.11a/n or 802.11b/g/n radio network on a specific WLAN, enter 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 To re-enable the WLAN, enter this command:

config wlan enable *wlan_id*

Step 4 To save your changes, enter this command:

save config

Step 5 To verify the DTIM period, enter this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... employee1
Network Name (SSID).............................. employee
Status........................................... Enabled
```

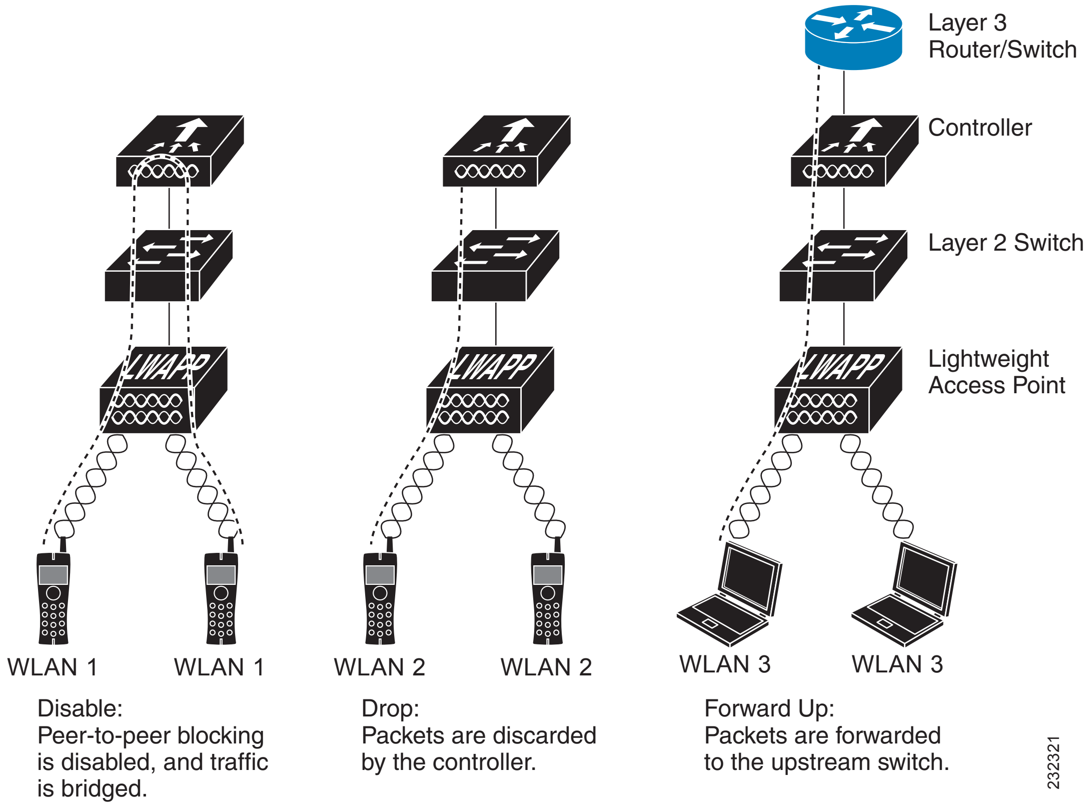
```
...
DTIM period for 802.11a radio.................... 1
DTIM period for 802.11b radio.................... 1
Local EAP Authentication..................... Disabled
...
```

Configuring Peer-to-Peer Blocking

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, 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 4.2 or later, 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 6-9 illustrates each option.

Figure 6-9 Peer-to-Peer Blocking Examples



Guidelines for Using Peer-to-Peer Blocking

Follow these guidelines when using peer-to-peer blocking:

- 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, ARP requests are directed according to the behavior set for peer-to-peer blocking.
- Peer-to-peer blocking does not apply to multicast traffic.
- Locally switched hybrid-REAP WLANs and hybrid-REAP access points in standalone mode do not support peer-to-peer blocking.
- If you upgrade to controller software release 4.2 or later 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.

Using the GUI to Configure Peer-to-Peer Blocking

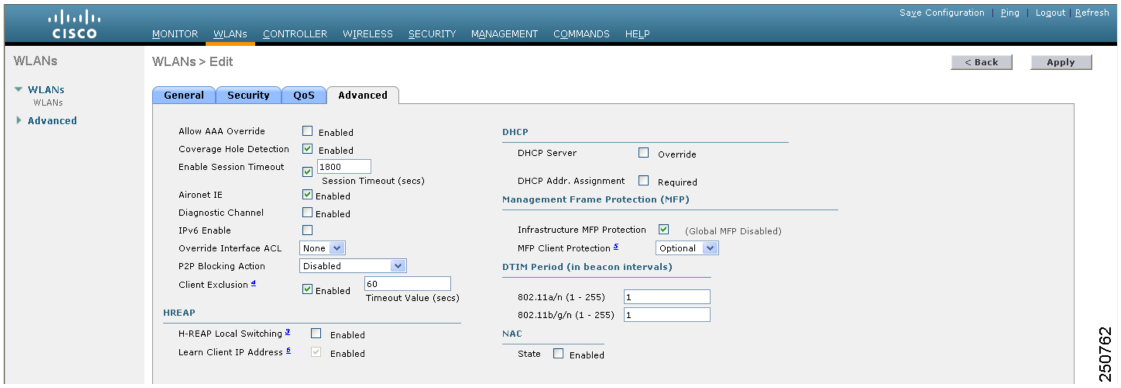
Follow these steps to configure a WLAN for peer-to-peer blocking using the GUI.

Step 1 Click **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure peer-to-peer blocking.

Step 3 Click the **Advanced** tab to open the WLANs > Edit (Advanced) page (see Figure 6-10).

Figure 6-10 WLANs > Edit (Advanced) Page



WLANs > Edit

Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] ☑ Enabled 60 Timeout Value (secs)

HREAP
H-REAP Local Switching [3] □ Enabled
Learn Client IP Address [6] ☑ Enabled

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)
Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
State □ Enabled

Step 4 Choose one of the following options from the P2P Blocking drop-down box:

- **Disabled**—Disables peer-to-peer blocking and bridges traffic locally within the controller whenever possible. This is the default value.

  Note Traffic is never bridged across VLANs in the controller.

- **Drop**—Causes the controller to discard the packets.
- **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.

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

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

Using the CLI to Configure Peer-to-Peer Blocking

Follow these steps to configure a WLAN for peer-to-peer blocking using the CLI.

Step 1 To configure a WLAN for peer-to-peer blocking, enter this command:

config wlan peer-blocking {**disable** | **drop** | **forward-upstream**} *wlan_id*

Note See the description of each parameter in the "Using the GUI to Configure Peer-to-Peer Blocking" section above.

Step 2 To save your changes, enter this command:

save config

Step 3 To see the status of peer-to-peer blocking for a WLAN, enter this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
Status........................................... Enabled
...
...
...
Peer-to-Peer Blocking Action..................... Disabled
Radio Policy..................................... All
Local EAP Authentication...................... Disabled
```

Configuring Layer 2 Security

This section explains how to assign Layer 2 security settings to WLANs.

Note Clients using the Microsoft Wireless Configuration Manager and 802.1X must use WLANs configured for 40- or 104-bit key length. Configuring for 128-bit key length results in clients that can associate but not authenticate.

Static WEP Keys

Controllers can control static WEP keys across access points. Use these commands to configure static WEP for WLANs:

- Enter this command to disable 802.1X encryption:

  config wlan security 802.1X disable *wlan_id*

- Enter this command to configure 40/64, 104/128, or 128/152-bit WEP keys:

  config wlan security static-wep-key encryption *wlan_id* {**40** | **104** | **128**} {**hex** | **ascii**} *key key_index*

  - Use the **40**, **104**, or **128** options to specify 40/64-bit, 104/128-bit, or 128/152-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; enter 26 hexadecimal or 13 ASCII characters for 104-bit/128-bit keys; enter 32 hexadecimal or 16 ASCII characters for 128-bit/152-bit keys.
  - Enter a key index (sometimes called a *key slot*) of **1** through **4**.

Dynamic 802.1X Keys and Authorization

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).

- Enter **show wlan** *wlan_id* to check the security settings of each WLAN. 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.
- To disable or enable the 802.1X authentication, use 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.

- If you want to change the 802.1X encryption level for a WLAN, use this command:

  config wlan security 802.1X encryption *wlan_id* [**40** | **104** | **128**]

  - 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.)
  - Use the 128 option to specify 128/152-bit encryption.

Configuring a 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: PSK, CCKM, and 802.1X+CCKM.

- **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 pre-shared key* or *WPA passphrase*), you need to configure a pre-shared 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.

  Note 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 6-39 for more information on CCX.

- **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.

You can configure WPA1+WPA2 through either the GUI or the CLI.

Using the GUI to Configure WPA1+WPA2

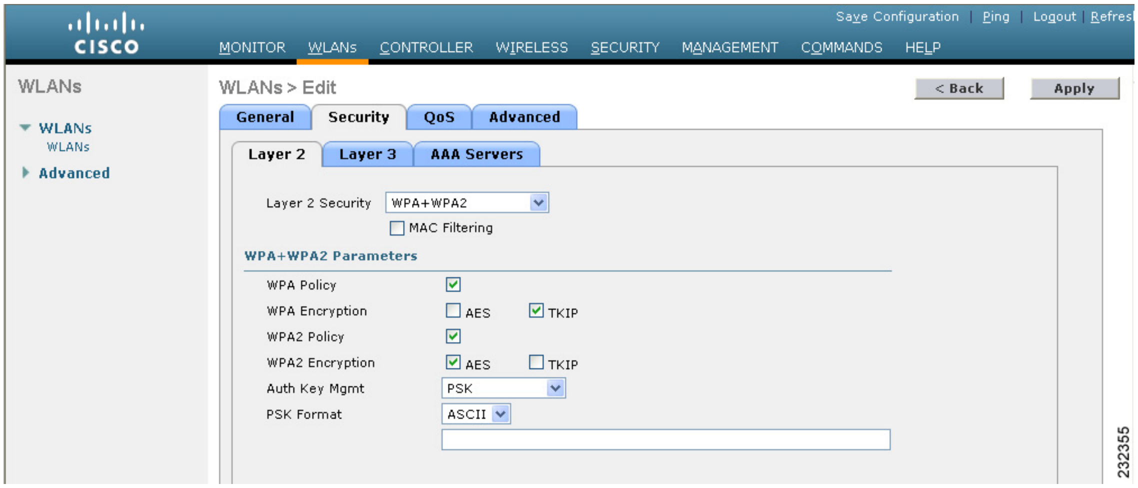
Follow these steps to configure a WLAN for WPA1+WPA2 using the controller GUI.

Step 1 Click **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Click the **Security** and **Layer 2** tabs to open the WLANs > Edit (Security > Layer 2) page (see Figure 6-11).

Figure 6-11 WLANs > Edit (Security > Layer 2) Page


Save Configuration | Ping | Logout | Refresh
cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
232355

Layer 2 Security WPA+WPA2
□ MAC Filtering

WPA+WPA2 Parameters

WPA Policy ☑
WPA Encryption □ AES ☑ TKIP
WPA2 Policy ☑
WPA2 Encryption ☑ AES □ TKIP
Auth Key Mgmt PSK
PSK Format ASCII

Step 4 Choose **WPA+WPA2** from the Layer 2 Security drop-down box.

Step 5 Under WPA+WPA2 Parameters, check the **WPA Policy** check box to enable WPA1, check the **WPA2 Policy** check box to enable WPA2, or check 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 you choose in Step 7.

Step 6 Check 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 box: **802.1X**, **CCKM**, **PSK**, or **802.1X+CCKM**.

Step 8 If you chose PSK in Step 7, choose **ASCII** or **HEX** from the PSK Format drop-down box and then enter a pre-shared key in the blank field. WPA pre-shared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Using the CLI to Configure WPA1+WPA2

Follow these steps to configure a WLAN for WPA1+WPA2 using the controller CLI.

Step 1 Enter this command to disable the WLAN:

config wlan disable *wlan_id*

Step 2 Enter this command to enable or disable WPA for the WLAN:

config wlan security wpa {**enable** | **disable**} *wlan_id*

Step 3 Enter this command to enable or disable WPA1 for the WLAN:

config wlan security wpa wpa1 {**enable** | **disable**} *wlan_id*

Step 4 Enter this command to enable or disable WPA2 for the WLAN:

config wlan security wpa wpa2 {**enable** | **disable**} *wlan_id*

Step 5 Enter these commands to enable or disable AES or TKIP data encryption for WPA1 or WPA2:

- **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 Enter this command to enable or disable 802.1X, PSK, or CCKM authenticated key management:

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 pre-shared key:

config wlan security wpa akm psk set-key {**ascii** | **hex**} *psk-key wlan_id*

WPA pre-shared 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:

```
PMK-CCKM Cache
                            Entry
Type        Station         Lifetime   VLAN Override        IP Override
------  ------------------- --------   ------------------   ---------------
CCKM    00:07:0e:b9:3a:1b   150                          0.0.0.0
```

If you enabled WPA2 with 802.1X 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 Enter this command to enable the WLAN:

config wlan enable *wlan_id*

Step 10 Enter this command to save your settings:

save config

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, message integrity check (MIC), and message sequence number. Software release 4.0 or later supports CKIP with 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 this CKIP feature.

CKIP requires that 5-byte and 13-byte encryption keys be expanded to 16-byte keys. The algorithm to perform key expansion happens at the access point. The key is appended to itself repeatedly until the length reaches 16 bytes. All lightweight access points support CKIP.

You can configure CKIP through either the GUI or the CLI.

Using the GUI to Configure CKIP

Follow these steps to configure a WLAN for CKIP using the controller GUI.

Step 1 Click **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Click the **Advanced** tab.

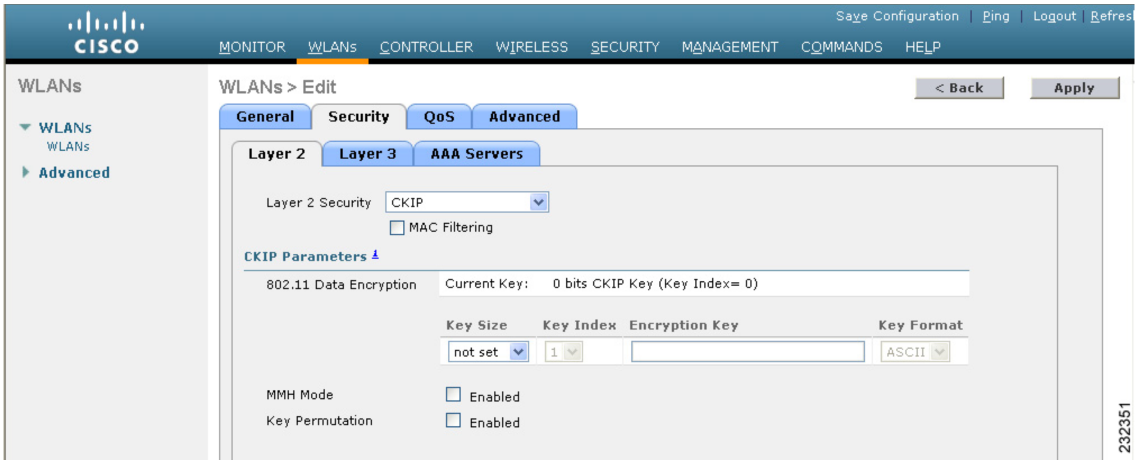
Step 4 Check the **Aironet IE** check box to enable Aironet IEs for this WLAN and click **Apply**.

Step 5 Click the **General** tab.

Step 6 Uncheck the **Status** check box, if checked, to disable this WLAN and click **Apply**.

Step 7 Click the **Security** and **Layer 2** tabs to open the WLANs > Edit (Security > Layer 2) page (see Figure 6-12).

Figure 6-12 WLANs > Edit (Security > Layer 2) Page



Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General Security QoS Advanced
Layer 2 Layer 3 AAA Servers
232351

Layer 2 Security: CKIP

□ MAC Filtering

CKIP Parameters [1]

802.11 Data Encryption — Current Key: 0 bits CKIP Key (Key Index= 0)

Key Size	Key Index	Encryption Key	Key Format
not set	1		ASCII

MMH Mode □ Enabled

Key Permutation □ Enabled

Step 8 Choose **CKIP** from the Layer 2 Security drop-down box.

Step 9 Under CKIP Parameters, choose the length of the CKIP encryption key from the Key Size drop-down box.

Range: Not Set, 40 bits, or 104 bits

Default: Not Set

Step 10 Choose the number to be assigned to this key from the Key Index drop-down box. You can configure up to four keys.

Step 11 Choose **ASCII** or **HEX** from the Key Format drop-down box and then enter an encryption key in the Encryption Key field. 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 Check the **MMH Mode** check box to enable MMH MIC data protection for this WLAN. The default value is disabled (or unchecked).

Step 13 Check the **Key Permutation** check box to enable this form of CKIP data protection. The default value is disabled (or unchecked).

Step 14 Click **Apply** to commit your changes.

Step 15 Click the **General** tab.

Step 16 Check 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.

Using the CLI to Configure CKIP

Follow these steps to configure a WLAN for CKIP using the controller CLI.

Step 1 Enter this command to disable the WLAN:

config wlan disable *wlan_id*

Step 2 Enter this command to enable Aironet IEs for this WLAN:

config wlan ccx aironet-ie enable *wlan_id*

Step 3 Enter this command to enable or disable CKIP for the WLAN:

config wlan security ckip {**enable** | **disable**} *wlan_id*

Step 4 Enter this command to specify a CKIP encryption key for the WLAN:

config wlan security ckip akm psk set-key *wlan_id* {**40** | **104**} {**hex** | **ascii**} *key key_index*

Step 5 Enter this command to enable or disable CKIP MMH MIC for the WLAN:

config wlan security ckip mmh-mic {**enable** | **disable**} *wlan_id*

Step 6 Enter this command to enable or disable CKIP key permutation for the WLAN:

config wlan security ckip kp {**enable** | **disable**} *wlan_id*

Step 7 Enter this command to enable the WLAN:

config wlan enable *wlan_id*

Step 8 Enter this command to save your settings:

save config

Configuring a Session Timeout

Using the controller GUI or CLI, you can configure a session timeout for wireless clients on a WLAN. The session timeout is the maximum time for a client session to remain active before requiring reauthorization.

Using the GUI to Configure a Session Timeout

Using the controller GUI, follow these steps to configure a session timeout for wireless clients on a WLAN.

Step 1 Click **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, click the **Advanced** tab. The WLANs > Edit (Advanced) page appears.

Step 4 To configure a session timeout for this WLAN, check the **Enable Session Timeout** check box. Otherwise, uncheck the check box. The default value is checked.

Step 5 In the Session Timeout field, 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; and WPA+WPA2 with 802.1X, CCKM, or 802.1X+CCKM authentication key management and 0 seconds for all other Layer 2 security types. A value of 0 is equivalent to no timeout.

Note When using WPA1 or WPA2, if the timeout is set to infinite, the clients still reauthenticate at a frequency of 12 hours. The workaround is to enable the AAA override and push through the radius server a longer session timeout period. The timeout period can be longer than one day, which is the maximum period you can manually configure.

Step 6

Step 7 Click **Apply** to commit your changes.

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

Using the CLI to Configure a Session Timeout

Using the controller CLI, follow these steps to configure a session timeout for wireless clients on a WLAN.

Step 1 To configure a session timeout for wireless clients on a WLAN, enter 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; and WPA+WPA2 with 802.1X, CCKM, or 802.1X+CCKM authentication key management and 0 seconds for all other Layer 2 security types. A value of 0 is equivalent to no timeout.

Note When using WPA1 or WPA2, if the timeout is set to infinite, the clients still reauthenticate at a frequency of 12 hours. The workaround is to enable the AAA override and push through the radius server a longer session timeout period. The timeout period can be longer than one day, which is the maximum period you can manually configure.

Step 2 To save your changes, enter this command:

save config

Step 3 To see the current session timeout value for a WLAN, enter 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

This section explains how to configure Layer 3 security settings for a WLAN on the controller.

Note Layer 2 Tunnel Protocol (L2TP) and IPSec are not supported on controllers running software release 4.0 or later.

VPN Passthrough

Using the GUI to Configure VPN Passthrough

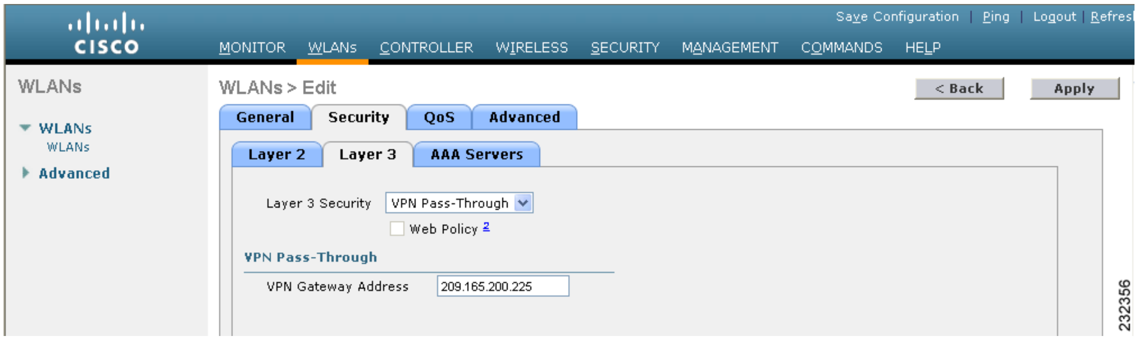
Follow these steps to configure a WLAN for VPN passthrough using the controller GUI.

Step 1 Click **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure VPN passthrough. The WLANs > Edit page appears.

Step 3 Click the **Security** and **Layer 3** tabs to open the WLANs > Edit (Security > Layer 3) page (see Figure 6-13).

Figure 6-13 WLANs > Edit (Security > Layer 3) Page


CISCO
Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General Security QoS Advanced
Layer 2 Layer 3 AAA Servers
232356

Layer 3 Security VPN Pass-Through

□ Web Policy 2

VPN Pass-Through

VPN Gateway Address 209.165.200.225

Step 4 Choose **VPN Pass-Through** from the Layer 3 Security drop-down box.

Step 5 In the VPN Gateway Address field, enter the IP address of the gateway router that is terminating the VPN tunnels initiated by the client and passed through the controller.

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

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

Using the CLI to Configure VPN Passthrough

Enter these commands to configure a WLAN for VPN passthrough using the controller CLI:

- **config wlan security passthru** {**enable** | **disable**} *wlan_id gateway*

  For *gateway*, enter the IP address of the router that is terminating the VPN tunnel.

- Enter **show wlan** to verify that the passthrough is enabled.

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.

Note 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.

Note The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.

Note Before enabling web authentication, make sure that all proxy servers are configured for ports other than port 53.

Note When you enable web authentication for a WLAN, a message appears indicating that the controller will forward DNS traffic to and from wireless clients prior to authentication. Cisco recommends 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.

Using the GUI to Configure Web Authentication

Follow these steps to configure a WLAN for web authentication using the controller GUI.

Step 1 Click **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 Click the **Security** and **Layer 3** tabs to open the WLANs > Edit (Security > Layer 3) page.

Step 4 Check 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.

Using the CLI to Configure Web Authentication

Enter these commands to configure a WLAN for web authentication using the controller CLI:

- **config wlan security web-auth** {**enable** | **disable**} *wlan_id*
- Enter **show wlan** to verify that web authentication is enabled.

Assigning a QoS Profile to a WLAN

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 6-1 to derive the IP DSCP value that is visible on the wired LAN.

Table 6-1 Access Point QoS Translation Values

AVVID Traffic Type	AVVID IP DSCP	QoS Profile	AVVID 802.1p	IEEE 802.11e UP
Network control	56 (CS7)	Platinum	7	7
Inter-network control (CAPWAP control, 802.11 management)	48 (CS6)	Platinum	6	7
Voice	46 (EF)	Platinum	5	6
Interactive video	34 (AF41)	Gold	4	5
Streaming video	32 (CS4)	Gold	4	5
Mission critical	26 (AF31)	Gold	3	4
Call signaling	24 (CS3)	Gold	3	4
Transactional	18 (AF21)	Silver	2	3
Network management	16 (CS2)	Silver	2	3
Bulk data	10 (AF11)	Bronze	1	2
Best effort	0 (BE)	Silver	0	0
Scavenger	8 (CS1)	Bronze	0	1

You can assign a QoS profile to a WLAN using the controller GUI or CLI.

Using the GUI to Assign a QoS Profile to a WLAN

Using the controller GUI, follow these steps to assign a QoS profile to a WLAN.

Step 1 If you have not already done so, configure one or more QoS profiles using the instructions in the "Using the GUI to Configure QoS Profiles" section on page 4-45.

Step 2 Click **WLANs** to open the WLANs page.

Step 3 Click the ID number of the WLAN to which you want to assign a QoS profile.

Step 4 When the WLANs > Edit page appears, click the **QoS** tab.

Step 5 From the Quality of Service (QoS) drop-down box, choose one of the following:

- Platinum (voice)
- Gold (video)
- Silver (best effort)
- Bronze (background)

Note Silver (best effort) is the default value.

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

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

Using the CLI to Assign a QoS Profile to a WLAN

Using the controller CLI, follow these steps to assign a QoS profile to a WLAN.

Step 1 If you have not already done so, configure one or more QoS profiles using the instructions in the "Using the CLI to Configure QoS Profiles" section on page 4-47.

Step 2 To assign a QoS profile to a WLAN, enter this command:

config wlan qos *wlan_id* {**bronze** | **silver** | **gold** | **platinum**}

Silver is the default value.

Step 3 To save your changes, enter this command:

save config

Step 4 To verify that you have properly assigned the QoS profile to the WLAN, enter this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist.................................... Disabled
Session Timeout.................................. 0
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... 1.100.163.24
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
...
```

Configuring 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.

You can use the controller GUI or CLI to configure QBSS. QBSS is disabled by default.

Guidelines for Configuring QBSS

Follow these guidelines when configuring QBSS on a WLAN:

- 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. This becomes particularly important if you have many more 7920 users than 7921 users.

Note Refer to Chapter 4 for more information and configuration instructions for load-based CAC.

Additional Guidelines for Using 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.

Using the GUI to Configure QBSS

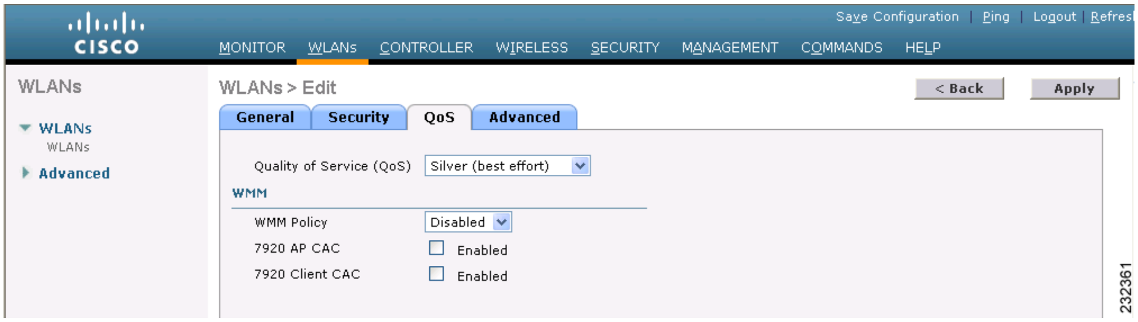
Using the controller GUI, follow these steps to configure QBSS.

Step 1 Click **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, click the **QoS** tab to open the WLANs > Edit (Qos) page (see Figure 6-14).

Figure 6-14 WLANs > Edit (QoS) Page



Quality of Service (QoS) Silver (best effort)

WMM Policy Disabled

7920 AP CAC □ Enabled

7920 Client CAC □ Enabled

Step 4 From the WMM Policy drop-down box, 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 Check 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 unchecked.

Step 6 Check 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 unchecked.

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.

Using the CLI to Configure QBSS

Using the controller CLI, follow these steps to configure QBSS.

Step 1 To determine the ID number of the WLAN to which you want to add QBSS support, enter this command:

show wlan summary

Step 2 To disable the WLAN, enter this command:

config wlan disable *wlan_id*

Step 3 To configure WMM mode for 7921 phones and other devices that meet the WMM standard, enter this command:

config wlan wmm {**disabled** | **allowed** | **required**} *wlan_id*

where

- The **disabled** parameter disables WMM mode on the WLAN.
- The **allowed** parameter allows client devices to use WMM on the WLAN.
- The **required** parameter requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 4 To enable or disable 7920 support mode for phones that require client-controlled CAC, enter 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 To enable or disable 7920 support mode for phones that require access point-controlled CAC, enter this command:

config wlan 7920-support ap-cac-limit {**enable** | **disable**} *wlan_id*

Step 6 To re-enable the WLAN, enter this command:

config wlan enable *wlan_id*

Step 7 To save your changes, enter this command:

save config

Step 8 To verify that the WLAN is enabled and the Dot11-Phone Mode (7920) field is configured for compat mode, enter this command:

show wlan *wlan_id*

Configuring IPv6 Bridging

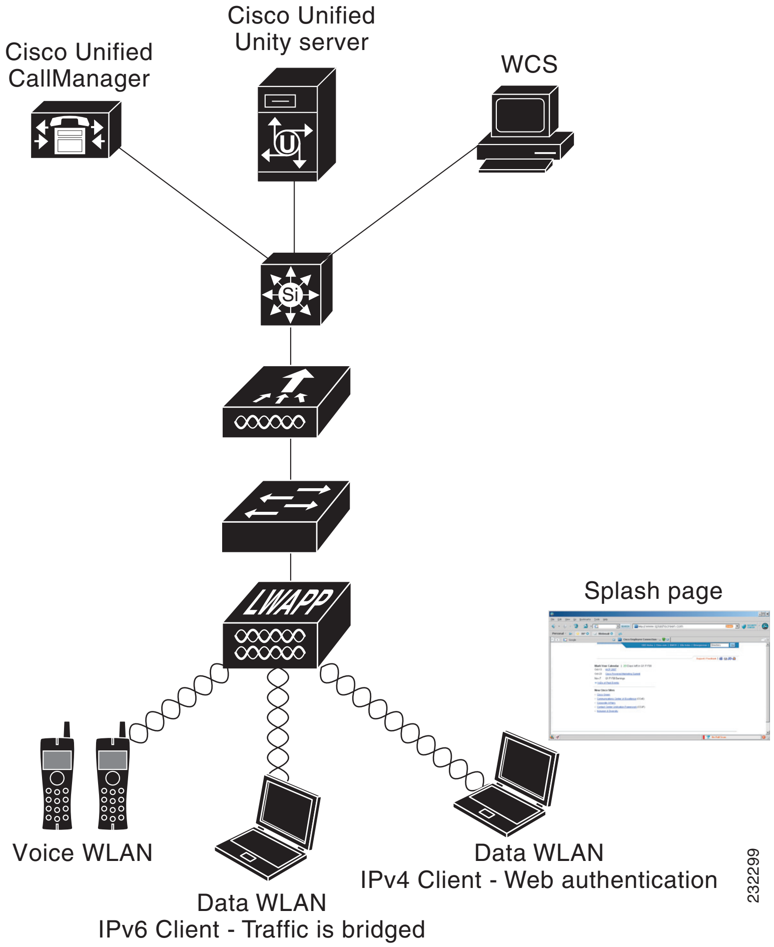
Internet Protocol version 6 (IPv6) is the next-generation network layer Internet protocol intended to replace version 4 (IPv4) in the TCP/IP suite of protocols. This new version increases Internet global address space to accommodate users and applications that require unique global IP addresses. IPv6 incorporates 128-bit source and destination addresses, providing significantly more addresses than the 32-bit IPv4 addresses. Follow the instructions in this section to configure a WLAN for IPv6 bridging using either the controller GUI or CLI.

Guidelines for Using IPv6 Bridging

Follow these guidelines when using IPv6 bridging:

- IPv6 bridging is supported only on the following controllers: 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Integrated Wireless LAN Controller Switch.
- To enable IPv6 bridging, Layer 3 security must be set to *None*.
- Hybrid-REAP with central switching is supported for use with IPv6 bridging. Hybrid-REAP with local switching is not supported.
- Auto-anchor mobility is not supported for use with IPv6 bridging.
- If symmetric mobility tunneling is enabled, all IPv4 traffic is bidirectionally tunneled to and from the client, but the IPv6 client traffic is bridged locally.
- In controller software release 4.2 or later, you can enable IPv6 bridging and IPv4 web authentication on the same WLAN, a combination that previously was not supported. The controller bridges IPv6 traffic from all clients on the WLAN while IPv4 traffic goes through the normal web authentication process. The controller begins bridging IPv6 as soon as the client associates and even before web authentication for IPv4 clients is complete. No other Layer 2 or Layer 3 security policy configuration is supported on the WLAN when IPv6 bridging and web authentication are enabled. Figure 6-15 illustrates how IPv6 bridging and IPv4 web authentication can be used on the same WLAN.

Figure 6-15 IPv6 Bridging and IPv4 Web Authentication


Cisco Unified CallManager
Cisco Unified Unity server
WCS
U
Si
LWAPP
Splash page
Voice WLAN
Data WLAN
IPv6 Client - Traffic is bridged
Data WLAN
IPv4 Client - Web authentication
232299

Note The Security Policy Completed field in both the controller GUI and CLI shows "No for IPv4 (bridging allowed for IPv6)" until web authentication is completed. You can view this field from the Clients > Detail page on the GUI or from the **show client detail** CLI command.

Using the GUI to Configure IPv6 Bridging

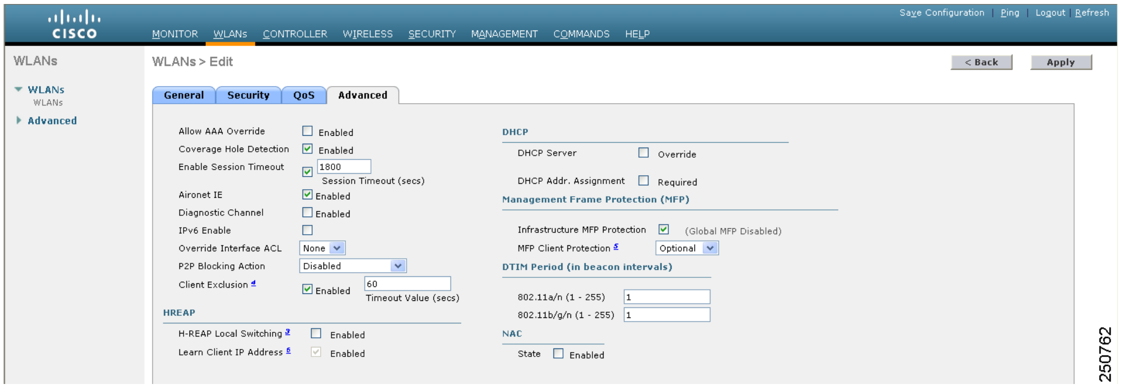
Follow these steps to configure a WLAN for IPv6 bridging using the GUI.

Step 1 Click **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Click the **Advanced** tab to open the WLANs > Edit (Advanced tab) page (see Figure 6-16).

Figure 6-16 WLANs > Edit (Advanced) Page



Allow AAA Override ☐ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel ☐ Enabled
IPv6 Enable ☐
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] ☑ Enabled 60 Timeout Value (secs)

HREAP
H-REAP Local Switching [3] ☐ Enabled
Learn Client IP Address [6] ☑ Enabled

DHCP
DHCP Server ☐ Override
DHCP Addr. Assignment ☐ Required

Management Frame Protection (MFP)
Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
State ☐ Enabled

Step 4 Check the **IPv6 Enable** check box if you want to enable clients that connect to this WLAN to accept IPv6 packets. Otherwise, leave the check box unchecked, which is the default value.

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

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

Using the CLI to Configure IPv6 Bridging

To configure a WLAN for IPv6 bridging using the CLI, enter this command:

config wlan IPv6support {**enable** | **disable**} *wlan_id*

The default value is disabled.

Configuring 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 related to increased security, enhanced performance, fast roaming, and superior power management.

The 4.2 or later release of controller software supports 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.

Follow the instructions in this section to configure a WLAN for the CCX Aironet IE feature and to see the CCX version supported by specific client devices using either the GUI or the CLI.

Using the GUI to Configure CCX Aironet IEs

Follow these steps to configure a WLAN for CCX Aironet IEs using the GUI.

Step 1 Click **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Click the **Advanced** tab to open the WLANs > Edit (Advanced tab) page (see Figure 6-16).

Step 4 Check the **Aironet IE** check box if you want to enable support for Aironet IEs for this WLAN. Otherwise, uncheck this check box. The default value is enabled (or checked).

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

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

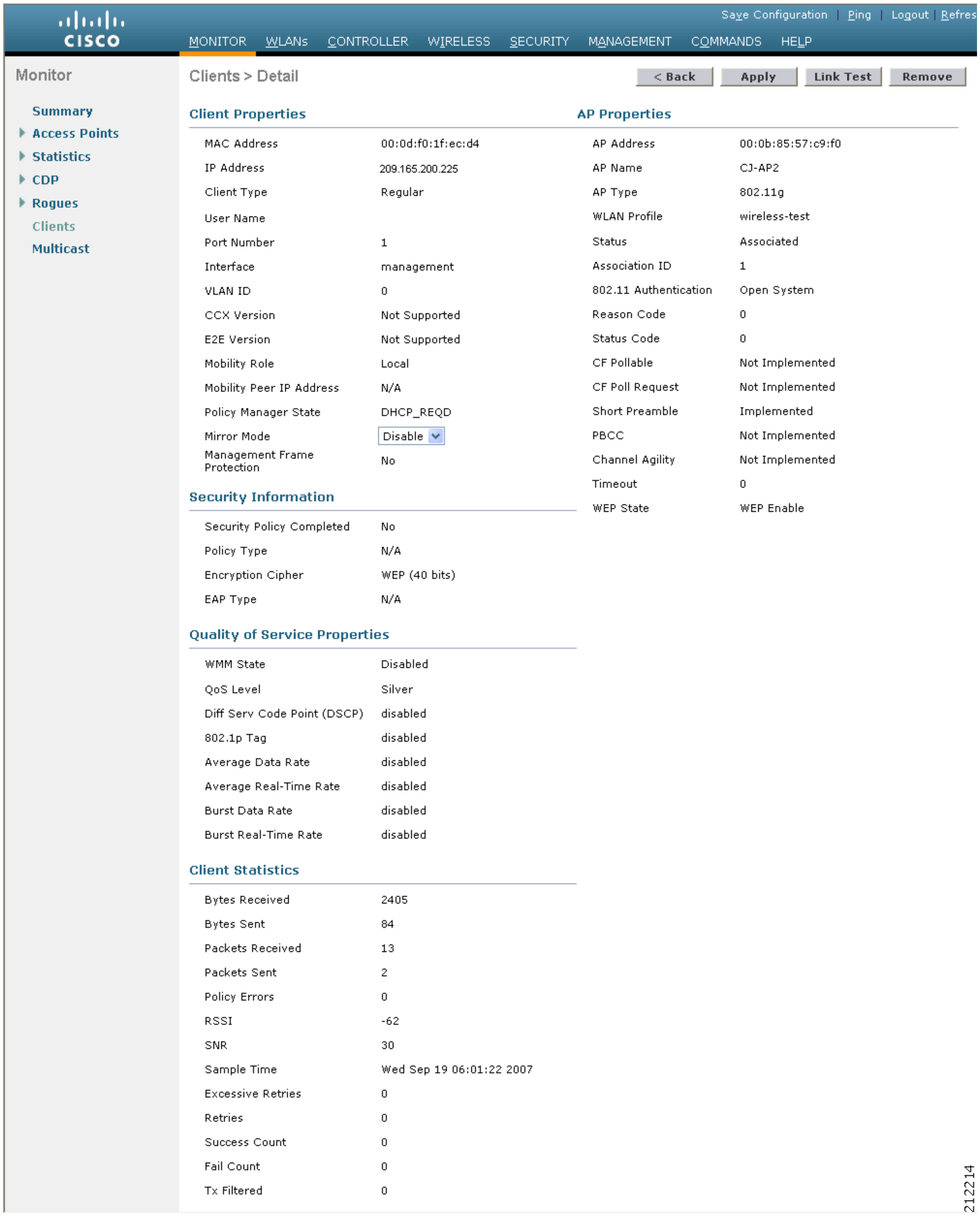
Using the GUI to View a Client's CCX Version

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. Follow these steps to see the CCX version supported by a particular client device using the GUI.

Step 1 Click **Monitor** > **Clients** to open the Clients page.

Step 2 Click the MAC address of the desired client device to open the Clients > Detail page (see Figure 6-17).

Figure 6-17 Clients > Detail Page


Save Configuration | Ping | Logout | Refres
cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Access Points
Statistics
CDP
Rogues
Clients
Multicast
< Back
Apply
Link Test
Remove
212214

Clients > Detail

Client Properties

MAC Address	00:0d:f0:1f:ec:d4
IP Address	209.165.200.225
Client Type	Regular
User Name	
Port Number	1
Interface	management
VLAN ID	0
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	DHCP_REQD
Mirror Mode	Disable
Management Frame Protection	No

AP Properties

AP Address	00:0b:85:57:c9:f0
AP Name	CJ-AP2
AP Type	802.11g
WLAN Profile	wireless-test
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	No
Policy Type	N/A
Encryption Cipher	WEP (40 bits)
EAP Type	N/A

Quality of Service Properties

WMM State	Disabled
QoS Level	Silver
Diff Serv Code Point (DSCP)	disabled
802.1p Tag	disabled
Average Data Rate	disabled
Average Real-Time Rate	disabled
Burst Data Rate	disabled
Burst Real-Time Rate	disabled

Client Statistics

Bytes Received	2405
Bytes Sent	84
Packets Received	13
Packets Sent	2
Policy Errors	0
RSSI	-62
SNR	30
Sample Time	Wed Sep 19 06:01:22 2007
Excessive Retries	0
Retries	0
Success Count	0
Fail Count	0
Tx Filtered	0

The CCX Version field 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.

Using the CLI to Configure CCX Aironet IEs

To enable or disable support for Aironet IEs for a particular WLAN, enter this command:

```
config wlan ccx aironet-ie {enable | disable} wlan_id
```

The default value is enabled.

Using the CLI to View a Client's CCX Version

To see the CCX version supported by a particular client device, enter this command:

```
show client detail client_mac
```

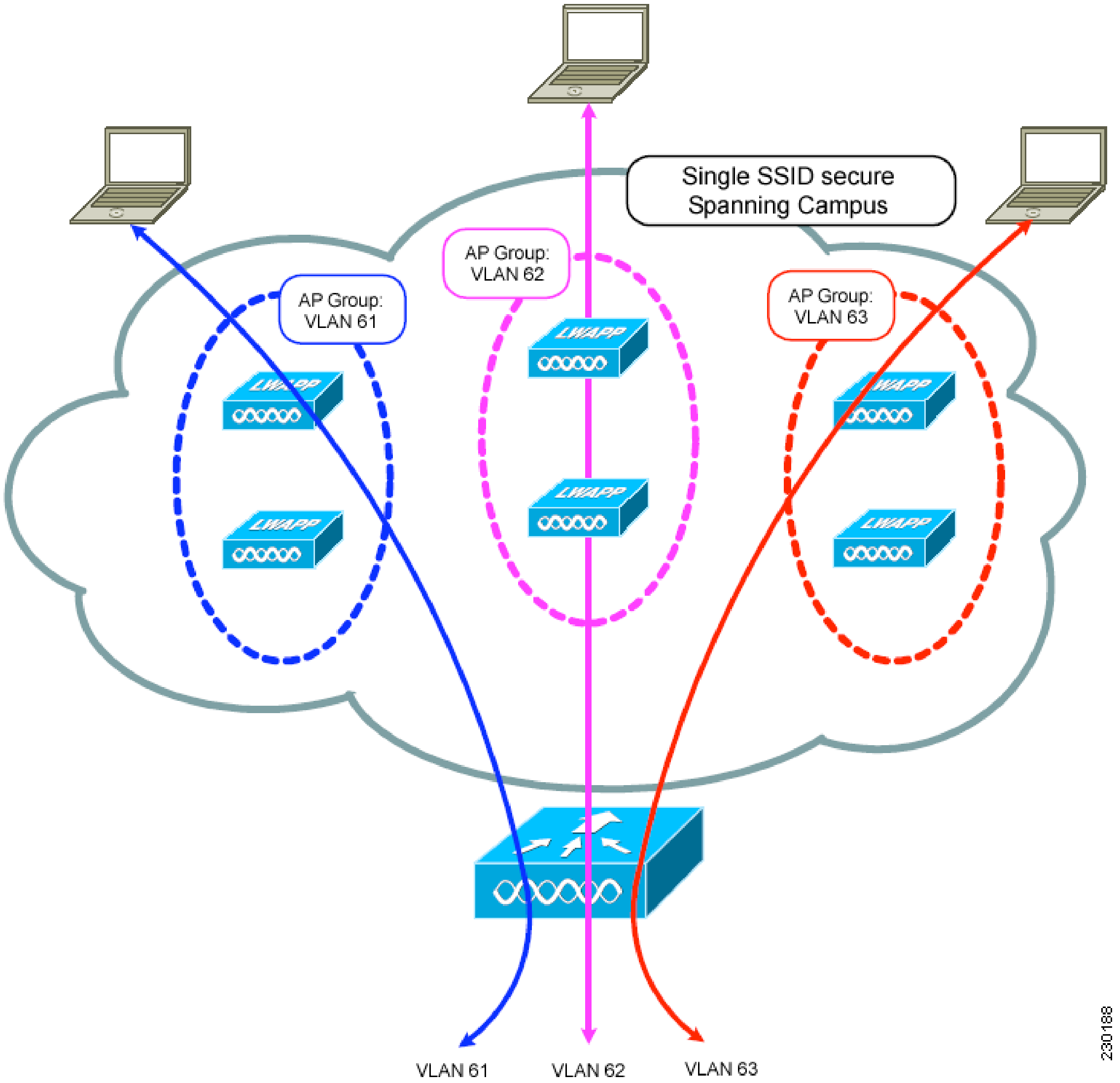
Configuring Access Point Groups

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, as illustrated in Figure 6-18.

Note The required access control list (ACL) must be defined on the router that serves the VLAN or subnet.

Note 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.

Figure 6-18 Access Point Groups



In Figure 6-18, 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 in Figure 6-18, the controller internally treats roaming between access points as a Layer 3 roaming event. In this way, WLAN clients maintain their original IP addresses.

To configure access point groups, follow these top-level steps:

1. Configure the appropriate dynamic interfaces and map them to the desired VLANs.

   For example, to implement the network in Figure 6-18, create dynamic interfaces for VLANs 61, 62, and 63 on the controller. Refer to Chapter 3 for information on how to configure dynamic interfaces.
2. Create the access point groups. Refer to the "Creating Access Point Groups" section below.
3. Assign access points to the appropriate access point groups. Refer to the "Creating Access Point Groups" section below.

Creating Access Point Groups

After all access points have joined the controller, you can create up to 150 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.

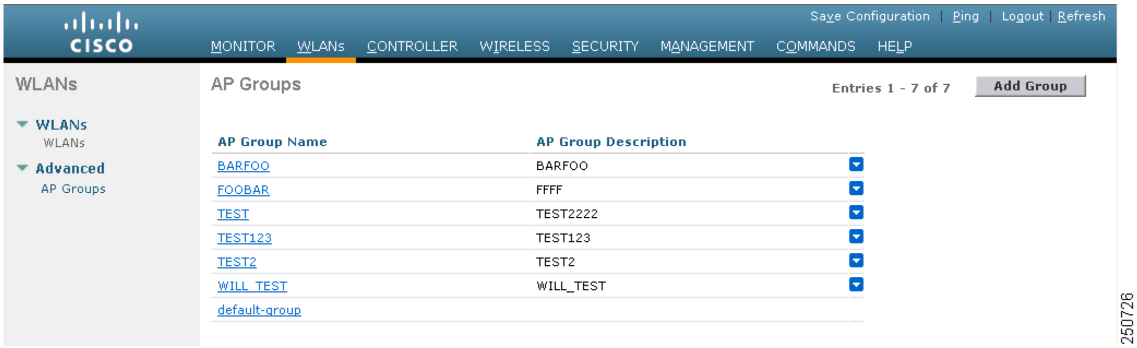
Note If you clear the configuration on the controller, all of the access point groups disappear except for the default access point group "default-group," which is created automatically.

Using the GUI to Create Access Point Groups

Using the controller GUI, follow these steps to create an access point group.

Step 1 Click **WLANs > Advanced > AP Groups** to open the AP Groups page (see Figure 6-19).

Figure 6-19 AP Groups Page



AP Groups

Entries 1 - 7 of 7

AP Group Name	AP Group Description
BARFOO	BARFOO
FOOBAR	FFFF
TEST	TEST2222
TEST123	TEST123
TEST2	TEST2
WILL_TEST	WILL_TEST
default-group	

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, 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 nor 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 field, enter the group's name.

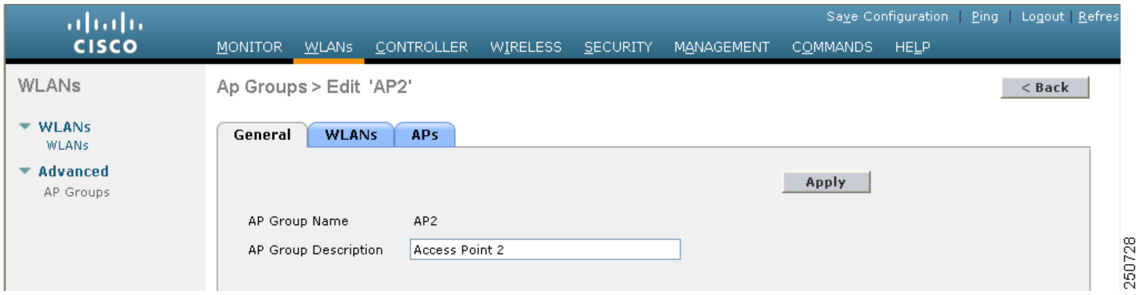
Step 4 In the Description field, enter the group's description.

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**. A message appears asking you to confirm your decision. If you proceed, any access points assigned to this access point group are moved to the default-group access point group.

Step 6 To edit this new group, click the name of the group. The AP Groups > Edit (General) page appears (see Figure 6-20).

Figure 6-20 AP Groups > Edit (General) Page


Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
AP Groups
< Back
General
WLANs
APs
Apply
250728

Ap Groups > Edit 'AP2'

AP Group Name AP2

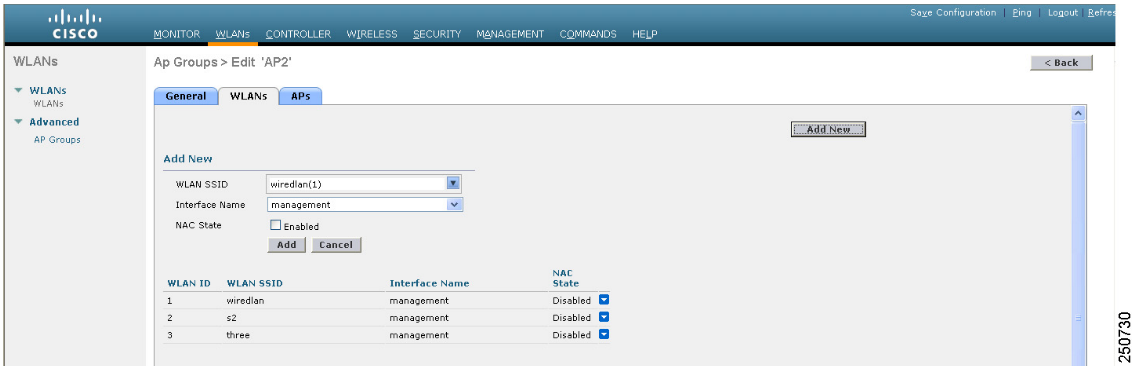
AP Group Description Access Point 2

Step 7 To change the description of this access point group, enter the new text in the AP Group Description field and click **Apply**.

Step 8 Click 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 (see Figure 6-21).

Figure 6-21 AP Groups > Edit (WLANs) Page


CISCO
Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
AP Groups
< Back
General
WLANs
APs
Add New
Add
Cancel
250730

Ap Groups > Edit 'AP2'

Add New

WLAN SSID: wiredlan(1)
Interface Name: management
NAC State: □ Enabled

WLAN ID	WLAN SSID	Interface Name	NAC State
1	wiredlan	management	Disabled
2	s2	management	Disabled
3	three	management	Disabled

Step 10 From the WLAN SSID drop-down box, choose the SSID of the WLAN.

Step 11 From the Interface Name drop-down box, 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 To enable NAC out-of-band support for this access point group, check the **NAC State** check box. To disable NAC out-of-band support, leave the check box unchecked, which is the default value. Refer to the "Configuring NAC Out-of-Band Integration" section on page 6-55 for more information on NAC.

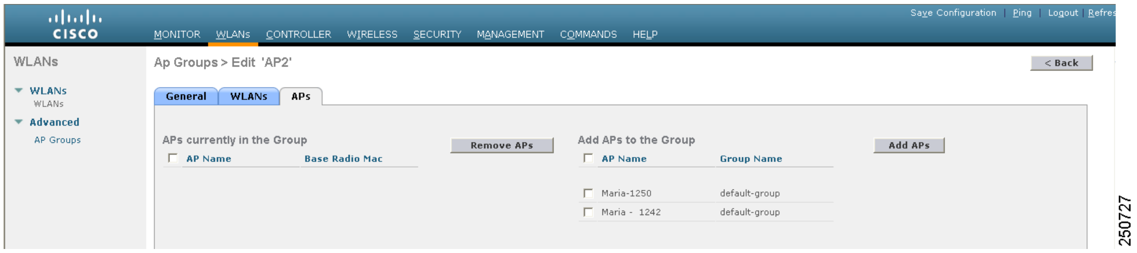
Step 13 Click **Add** to add this WLAN to the access point group. This WLAN appears in the list of WLANs that are assigned to this access point group.

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 Click 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" (see Figure 6-22).

Figure 6-22 AP Groups > Edit (APs) Page


CISCO
Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
AP Groups
< Back
General
WLANs
APs
Remove APs
Add APs
250727

Ap Groups > Edit 'AP2'

APs currently in the Group

□	AP Name	Base Radio Mac

Add APs to the Group

□	AP Name	Group Name
□	Maria-1250	default-group
□	Maria - 1242	default-group

Step 16 To add an access point to this access point group, check the check box to the left of the access point name and click **Add APs**. 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, check the **AP Name** check box. All of the access points are then selected.

Note If you ever want to remove an access point from the group, check the check box to the left of the access point name and click **Remove APs**. To select all of the access points at once, check 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, click **Wireless** > **Access Points** > **All APs** > *ap_name* > **Advanced** tab, choose the name of another access point group from the **AP Group Name** drop-down box, and click **Apply**.

Step 17 Click **Save Configuration** to save your changes.

Using the CLI to Create Access Point Groups

Using the controller CLI, follow these steps to create access point groups.

Step 1 To create an access point group, enter this command:

config wlan apgroup add *group_name*

Note To delete an access point group, enter this command: **config wlan apgroup delete** *group_name*. A warning message appears if you try to delete an access point group that is used by at least one access point. If you proceed, any access points assigned to this access point group are moved to the default-group access point group.

Step 2 To add a description to an access point group, enter this command:

config wlan apgroup description *group_name description*

Step 3 To assign a WLAN to an access point group, enter 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 this command: **config wlan apgroup interface-mapping delete** *group_name wlan_id*.

Step 4 To enable or disable NAC out-of-band support for this access point group, enter this command:

config wlan apgroup nac {**enable** | **disable**} *group_name wlan_id*

Step 5 To assign an access point to an access point group, enter this command:

config ap group-name *group_name Cisco_AP*

Note To remove an access point from an access point group, re-enter this command and assign the access point to another group.

Step 6 To save your changes, enter this command:

save config

Using the CLI to View Access Point Groups

Use these CLI commands to view information about or to troubleshoot access point groups.

1. To see a list of all access point groups on the controller, enter 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

AP Name Slots AP Model      Ethernet MAC   Location Port Country Priority GroupName
------- ---- -------------- ----------------- ------- ---- ------- -------- ---------
AP1242   2  AP1242AG-A-K9 00:14:1c:ed:23:9a default  1    US       1      AP2
...
```

2. To see the BSSIDs for each WLAN assigned to an access point group, enter 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
```

3. To see the number of WLANs enabled for an access point group, enter this command:

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

   Information similar to the following appears:

```
Cisco AP Identifier.............................. 166
Cisco AP Name................................. AP2
...
Station Configuration
      Configuration ............................ AUTOMATIC
      Number Of WLANs .......................... 2
...
```

4. To enable or disable debugging of access point groups, enter this command:

   debug group {**enable** | **disable**}

Configuring 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.

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

Follow these steps to configure your RADIUS server.

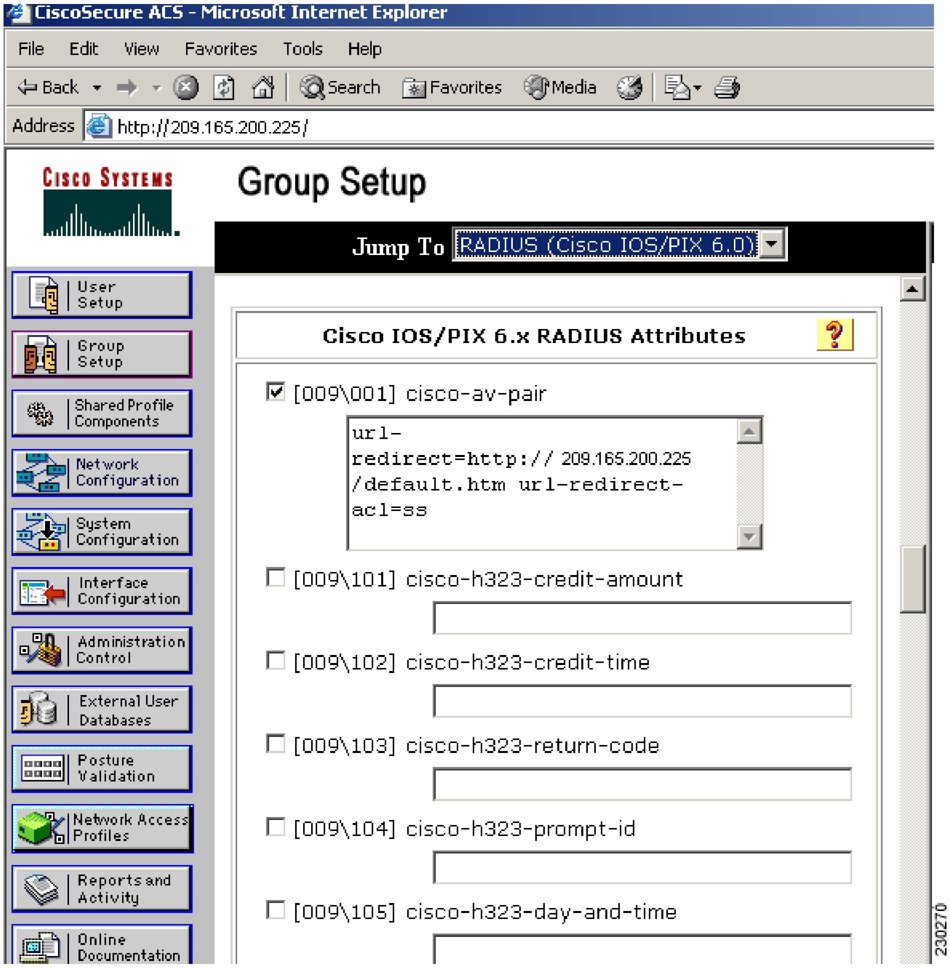
Note These instructions are specific to the CiscoSecure ACS; however, they should be similar to those for other RADIUS servers.

Step 1 From the CiscoSecure ACS main menu, click **Group Setup**.

Step 2 Click **Edit Settings**.

Step 3 From the Jump To drop-down menu, choose **RADIUS (Cisco IOS/PIX 6.0**). The window shown in Figure 6-23 appears.

Figure 6-23 ACS Server Configuration



Address http://209.165.200.225/

Jump To RADIUS (Cisco IOS/PIX 6.0)

☑ [009\001] cisco-av-pair

```
url-
redirect=http:// 209.165.200.225
/default.htm url-redirect-
acl=ss
```

☐ [009\101] cisco-h323-credit-amount

☐ [009\102] cisco-h323-credit-time

☐ [009\103] cisco-h323-return-code

☐ [009\104] cisco-h323-prompt-id

☐ [009\105] cisco-h323-day-and-time

Step 4 Check the **[009\001] cisco-av-pair** check box.

Step 5 Enter the following Cisco AV-pairs in the [009\001] 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*

Using the GUI to Configure Web Redirect

Using the controller GUI, follow these steps to configure conditional or splash page web redirect.

Step 1 Click **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN. The WLANs > Edit page appears.

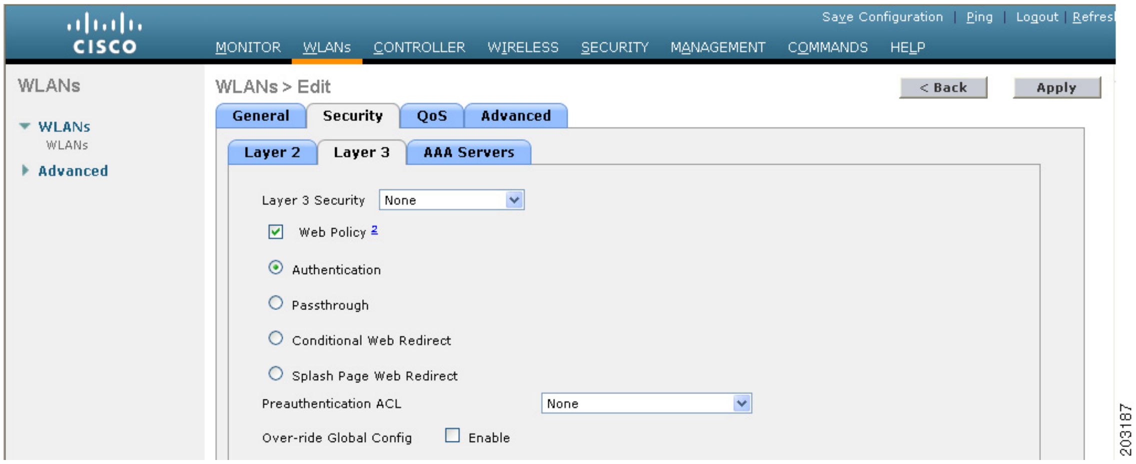
Step 3 Click the **Security** and **Layer 2** tabs to open the WLANs > Edit (Security > Layer 2) page.

Step 4 Choose **802.1X** or **WPA+WPA2** from the Layer 2 Security drop-down box.

Step 5 Set any additional parameters for 802.1X or WPA+WPA2.

Step 6 Click the **Layer 3** tab to open the WLANs > Edit (Security > Layer 3) page (see Figure 6-24).

Figure 6-24 WLANs > Edit (Security > Layer 3) Page



Layer 3 Security None

☑ Web Policy [2]

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

Preauthentication ACL None

Over-ride Global Config □ Enable

Step 7 Choose **None** from the Layer 3 Security drop-down box.

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.

Using the CLI to Configure Web Redirect

Using the controller CLI, follow these steps to configure conditional or splash page web redirect.

Step 1 To enable or disable conditional web redirect, enter this command:

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

Step 2 To enable or disable splash page web redirect, enter this command:

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

Step 3 To save your settings, enter this command:

save config

Step 4 To see the status of the web redirect features for a particular WLAN, enter 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

This section provides instructions for disabling all accounting servers on a WLAN. Disabling accounting servers disables all accounting operations and prevents the controller from falling back to the default RADIUS server for the WLAN.

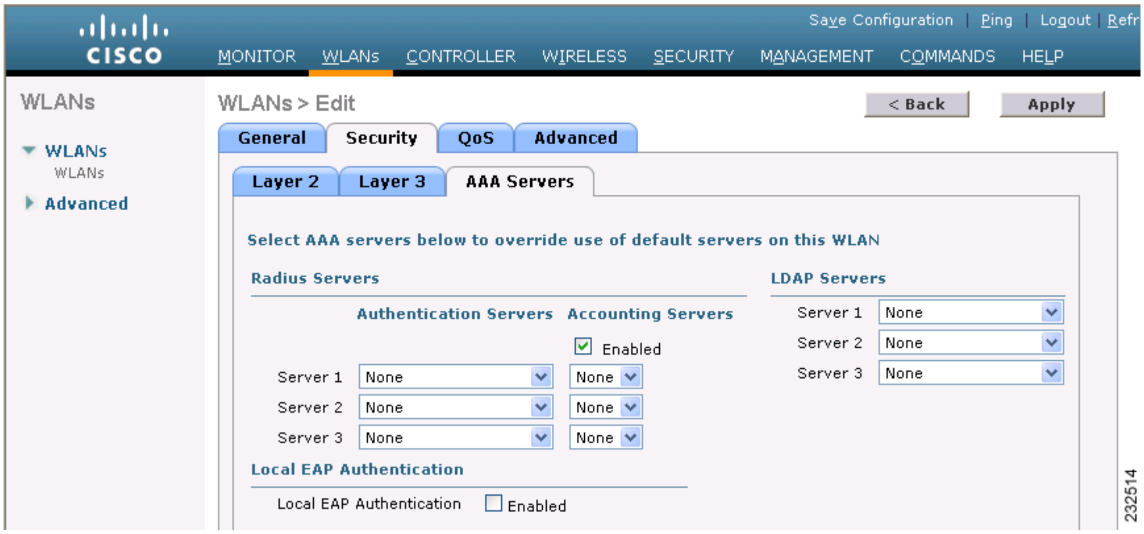
Follow these steps to disable all accounting servers for a RADIUS authentication server.

Step 1 Click **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 Click the **Security** and **AAA Servers** tabs to open the WLANs > Edit (Security > AAA Servers) page (see Figure 6-25).

Figure 6-25 WLANs > Edit (Security > AAA Servers) Page



Select AAA servers below to override use of default servers on this WLAN

Radius Servers

	Authentication Servers	Accounting Servers
		☑ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None

LDAP Servers

Server 1	None
Server 2	None
Server 3	None

Local EAP Authentication

Local EAP Authentication □ Enabled

Step 4 Uncheck 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

This section provides instructions for disabling coverage hole detection on a WLAN.

Coverage hole detection is enabled globally on the controller. See the "Coverage Hole Detection and Correction" section on page 11-4 and the "Using the GUI to Configure Coverage Hole Detection" section on page 11-15 for more information.

In software release 5.2, 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.

Using the GUI to Disable Coverage Hole Detection on a WLAN

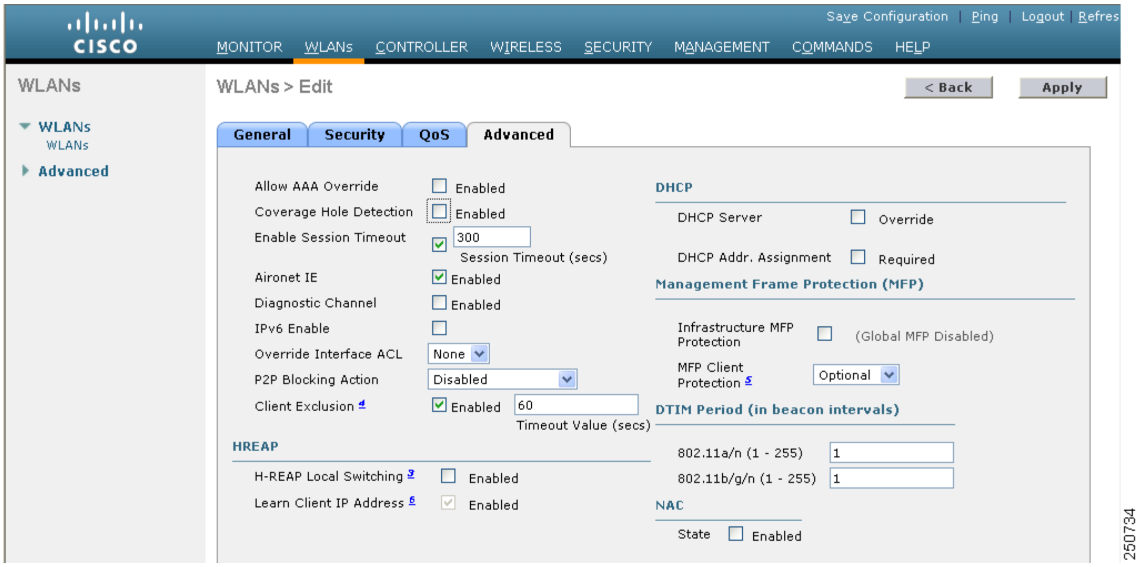
Using the controller GUI, follow these steps to disable coverage hole detection on a WLAN.

Step 1 Click **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 Click the **Advanced** tab to display the WLANs > Edit (Advanced) page (see Figure 6-26).

Figure 6-26 WLANs > Edit (Advanced) Page


Save Configuration | Ping | Logout | Refres
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
250734

WLANs > Edit

Allow AAA Override ☐ Enabled
Coverage Hole Detection ☐ Enabled
Enable Session Timeout ☑ 300 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel ☐ Enabled
IPv6 Enable ☐
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion 4 ☑ Enabled 60 Timeout Value (secs)

HREAP
H-REAP Local Switching 3 ☐ Enabled
Learn Client IP Address 6 ☑ Enabled

DHCP
DHCP Server ☐ Override
DHCP Addr. Assignment ☐ Required

Management Frame Protection (MFP)
Infrastructure MFP Protection ☐ (Global MFP Disabled)
MFP Client Protection 5 Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
State ☐ Enabled

Step 4 Uncheck the **Coverage Hole Detection Enabled** check box.

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

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

Using the CLI to Disable Coverage Hole Detection on a WLAN

Using the controller CLI, follow these steps to disable coverage hole detection on a WLAN.

Step 1 To disable coverage hole detection on a WLAN, enter this command:

config wlan chd *wlan_id* **disable**

Step 2 To save your settings, enter this command:

save config

Step 3 To see the coverage hole detection status for a particular WLAN, enter 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
```

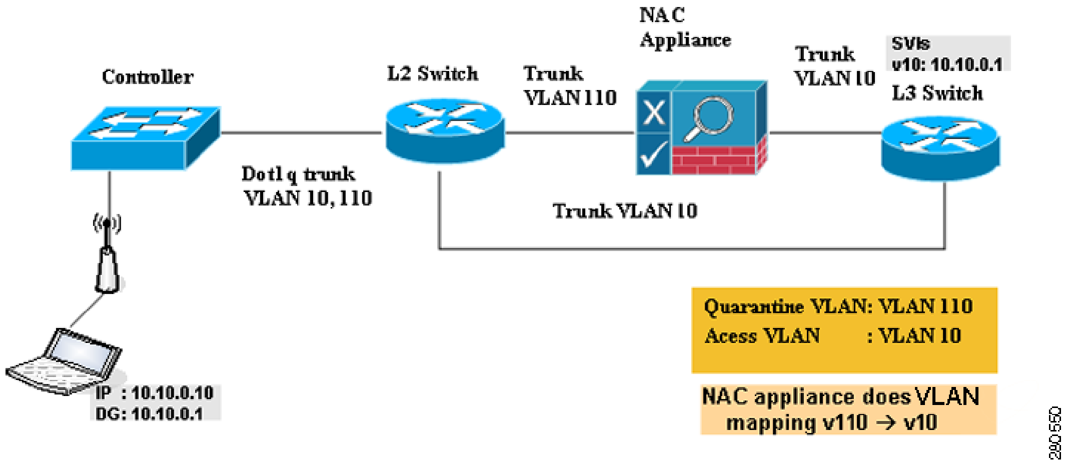
Configuring NAC Out-of-Band Integration

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).

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, 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.

To implement the NAC out-of-band feature on the controller, you need to 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. Figure 6-27 provides an example of NAC out-of-band integration.

Figure 6-27 NAC Out-of-Band Integration



In Figure 6-27, 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.

Follow the instructions in this section to configure NAC out-of-band integration using either the controller GUI or CLI.

Guidelines for Using NAC Out-of-Band Integration

Follow these guidelines when using NAC out-of-band integration:

- The NAC appliance supports up to 3500 users, and the controller supports up to 5000 users. Therefore, multiple NAC appliances might need to be deployed.
- CCA software release 4.5 or later 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 hybrid-REAP central switching. It is not supported for use on WLANs configured for hybrid-REAP local switching.

Note Refer to Chapter 13 for more information on hybrid REAP.

- 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 Refer to the Cisco NAC appliance configuration guides for configuration instructions: http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Using the GUI to Configure NAC Out-of-Band Integration

Using the controller GUI, follow these steps to configure NAC out-of-band integration.

Step 1 To configure the quarantine VLAN for a dynamic interface, follow these steps:

a. Click **Controller** > **Interfaces** to open the Interfaces page.

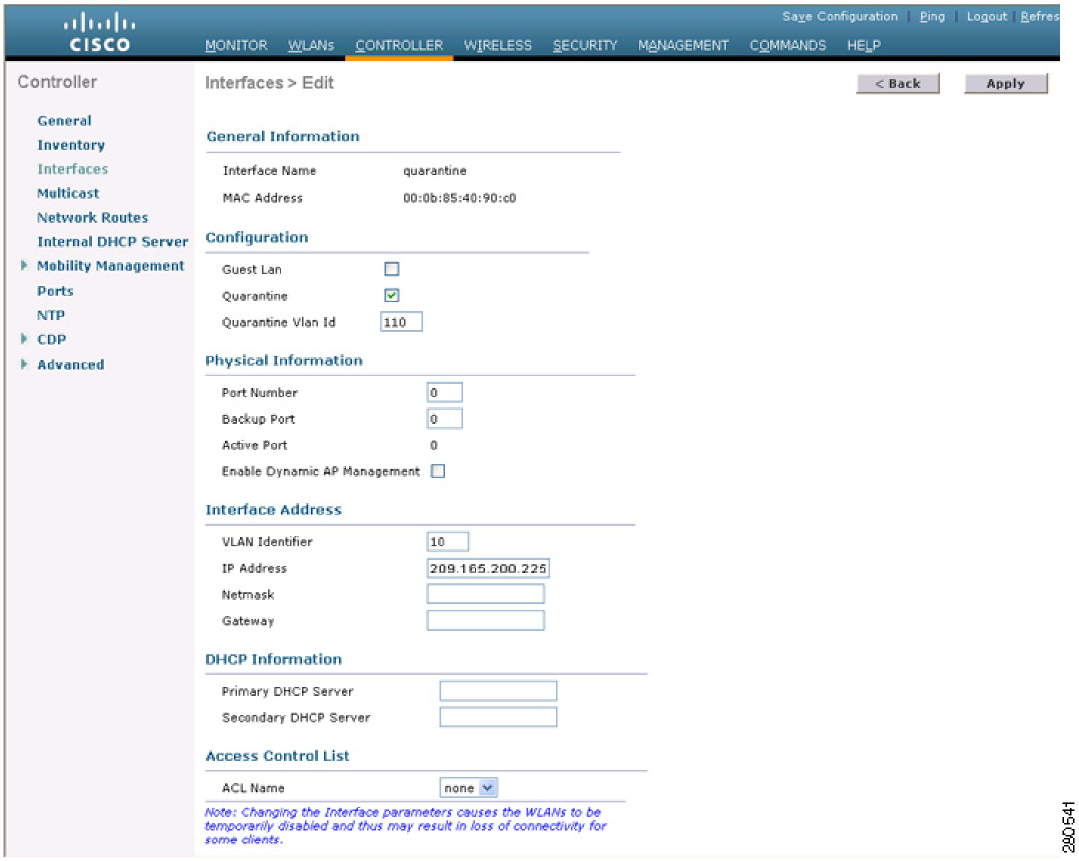
b. Click **New** to create a new dynamic interface.

c. In the Interface Name field, enter a name for this interface, such as “quarantine.”

d. In the VLAN ID field, enter a non-zero value for the access VLAN ID, such as “10.”

e. Click **Apply** to commit your changes. The Interfaces > Edit page appears (see Figure 6-28).

Figure 6-28 Interfaces > Edit Page



Interfaces > Edit

General Information

Interface Name quarantine

MAC Address 00:0b:85:40:90:c0

Configuration

Guest Lan □

Quarantine ☑

Quarantine Vlan Id 110

Physical Information

Port Number 0

Backup Port 0

Active Port 0

Enable Dynamic AP Management □

Interface Address

VLAN Identifier 10

IP Address 209.165.200.225

Netmask

Gateway

DHCP Information

Primary DHCP Server

Secondary DHCP Server

Access Control List

ACL Name none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

f. Check the **Quarantine** check box and enter a non-zero value for the quarantine VLAN ID, such as "110."

Note Cisco recommends 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 fields for this interface, such as the IP address, netmask, and default gateway.

h. Click **Apply** to save your changes.

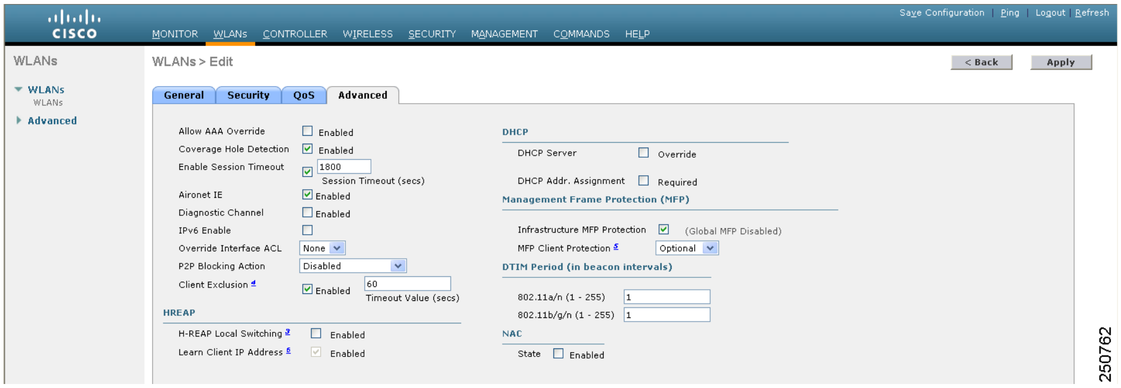
Step 2 To configure NAC out-of-band support on a WLAN or guest LAN, follow these steps:

a. Click **WLANs** to open the WLANs page.

b. Click the ID number of the desired WLAN or guest LAN. The WLANs > Edit page appears.

c. Click the **Advanced** tab to open the WLANs > Edit (Advanced) page (see Figure 6-29).

Figure 6-29 WLANs > Edit (Advanced) Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
250762

WLANs > Edit

Allow AAA Override ☐ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel ☐ Enabled
IPv6 Enable ☐
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion 4 ☑ Enabled 60 Timeout Value (secs)

HREAP
H-REAP Local Switching 2 ☐ Enabled
Learn Client IP Address 6 ☑ Enabled

DHCP
DHCP Server ☐ Override
DHCP Addr. Assignment ☐ Required

Management Frame Protection (MFP)
Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection 5 Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
State ☐ Enabled

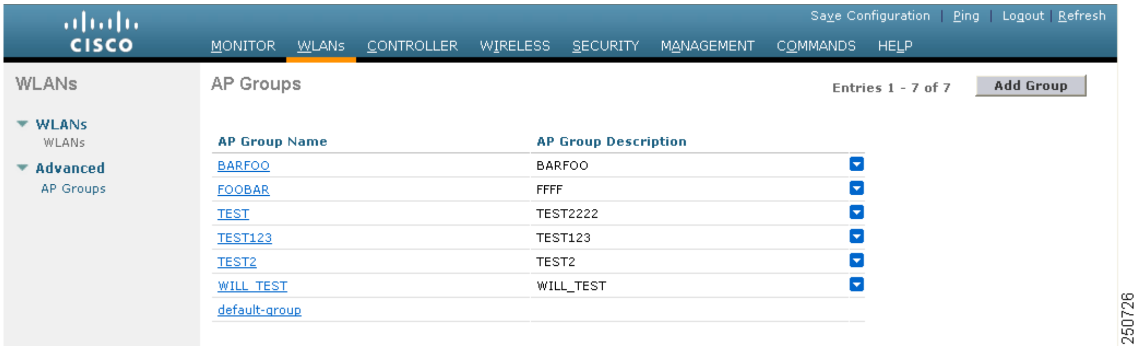
d. To configure NAC out-of-band support for this WLAN or guest LAN, check the **NAC State** check box. To disable NAC out-of-band support, leave the check box unchecked, which is the default value.

e. Click **Apply** to commit your changes.

Step 3 To configure NAC out-of-band support for a specific access point group, follow these steps:

a. Click **WLANs** > **Advanced** > **AP Groups** to open the AP Groups page (see Figure 6-30).

Figure 6-30 AP Groups Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
AP Groups
Add Group
250726

AP Groups

Entries 1 - 7 of 7

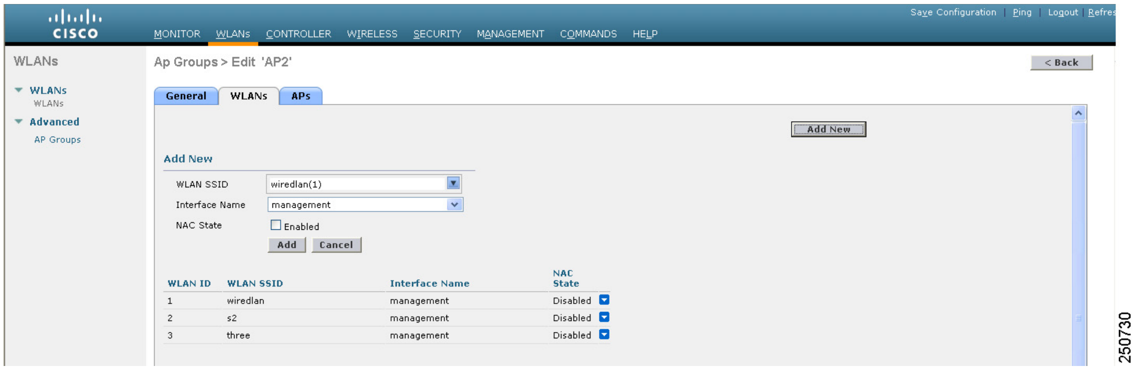
AP Group Name	AP Group Description
BARFOO	BARFOO
FOOBAR	FFFF
TEST	TEST2222
TEST123	TEST123
TEST2	TEST2
WILL_TEST	WILL_TEST
default-group	

b. Click the name of the desired access point group.

c. Click 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 (see Figure 6-31).

Figure 6-31 AP Groups > Edit (WLANs) Page


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Save Configuration | Ping | Logout | Refres
WLANs
WLANs
WLANs
Advanced
AP Groups
< Back
General
WLANs
APs
Add New
Add
Cancel
250730

Ap Groups > Edit 'AP2'

Add New

WLAN SSID wiredlan(1)

Interface Name management

NAC State □ Enabled

WLAN ID	WLAN SSID	Interface Name	NAC State
1	wiredlan	management	Disabled
2	s2	management	Disabled
3	three	management	Disabled

e. From the WLAN SSID drop-down box, choose the SSID of the WLAN.

f. From the Interface Name drop-down box, 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, check the **NAC State** check box. To disable NAC out-of-band support, leave the check box unchecked, 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 To see the current state of the client (either Quarantine or Access), follow these steps:

a. Click **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.

Using the CLI to Configure NAC Out-of-Band Integration

Using the controller CLI, follow these steps to configure NAC out-of-band integration.

Step 1 To configure the quarantine VLAN for a dynamic interface, enter 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 To enable or disable NAC out-of-band support for a WLAN or guest LAN, enter this command:

config {**wlan** | **guest-lan**} **nac** {**enable** | **disable**} {*wlan_id* | *guest_lan_id*}

Step 3 To enable or disable NAC out-of-band support for a specific access point group, enter this command:

config wlan apgroup nac {**enable** | **disable**} *group_name wlan_id*

Step 4 To save your changes, enter this command:

save config

Step 5 To see the configuration of a WLAN or guest LAN, including the NAC state, enter this command:

show {**wlan** *wlan_ id* | **guest-lan** *guest_lan_id*}

Information similar to the following appears:

```
WLAN Identifier.................................. 1
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 To see the current state of the client (either Quarantine or Access), enter this command:

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.

CHAPTER 7

Controlling Lightweight Access Points

This chapter describes the Cisco lightweight access points and explains how to connect them to the controller and manage access point settings. It contains these sections:

- Access Point Communication Protocols, page 7-2
- Configuring Global Credentials for Access Points, page 7-5
- Configuring Authentication for Access Points, page 7-9
- Embedded Access Points, page 7-14
- Autonomous Access Points Converted to Lightweight Mode, page 7-16
- Cisco Workgroup Bridges, page 7-34
- Configuring Backup Controllers, page 7-41
- Configuring Failover Priority for Access Points, page 7-46
- Configuring Country Codes, page 7-49
- Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain, page 7-55
- Using the W56 Band in Japan, page 7-58
- Dynamic Frequency Selection, page 7-58
- Optimizing RFID Tracking on Access Points, page 7-59
- Configuring Probe Request Forwarding, page 7-62
- Retrieving the Unique Device Identifier on Controllers and Access Points, page 7-63
- Performing a Link Test, page 7-64
- Configuring Link Latency, page 7-67
- Configuring Power over Ethernet, page 7-70
- Configuring Flashing LEDs, page 7-74
- Viewing Clients, page 7-74

Access Point Communication Protocols

In controller software release 5.2 or later, Cisco lightweight access points use the IETF standard Control and Provisioning of Wireless Access Points protocol (CAPWAP) to communicate between the controller and other lightweight access points on the network. Controller software releases prior to 5.2 use the Lightweight Access Point Protocol (LWAPP) for these communications.

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 being implemented in controller software release 5.2 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 exception is the Cisco Aironet 1140 Series Access Point, which supports only CAPWAP and therefore joins only controllers running CAPWAP. For example, an 1130 series access point can join a controller running either CAPWAP or LWAPP whereas an 1140 series access point can join only a controller running CAPWAP.

Guidelines for Using CAPWAP

Follow these guidelines when using CAPWAP:

- 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.

The 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.

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.

Note 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.

Note You must install software release 4.0.155.0 or later 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.

Note The Cisco controllers cannot edit or query any access point information using the CLI if the name of the access point contains a space.

Note Make sure 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**—Can occur on different subnets from the access point and uses IP addresses and UDP packets rather the MAC addresses used by Layer 2 discovery.
- **Over-the-air provisioning (OTAP)**—This feature is supported by Cisco 4400 series controllers. If this feature is enabled on the controller (on the controller General page), all associated access points transmit wireless CAPWAP or LWAPP neighbor messages, and new access points receive the controller IP address from these messages. This feature is disabled by default and should remain disabled when all access points are installed.

  Note You can find additional information about OTAP at this link: http://www.ciscosystems.com/en/US/products/ps6366/products_tech_note09186a008093d74a.shtml

- **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 non-volatile 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 7-24.
- **DNS discovery**—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-LWAPP-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*. 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, you need to make sure that access points join the new controller.

Using the GUI to Verify that Access Points Join the Controller

Follow these steps to ensure that access points join the new controller.

Step 1 Follow these steps to configure the new controller as a master controller.

a. Click **Controller** > **Advanced** > **Master Controller Mode** to open the Master Controller Configuration page.

b. Check 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. Ask your network administrator for more information about this step.

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 unchecking the **Master Controller Mode** check box on the Master Controller Configuration page.

Using the CLI to Verify that Access Points Join the Controller

Follow these steps to ensure that access points join the new controller.

Step 1 To configure the new controller as a master controller, enter this command:

config network master-base enable

Step 2 (Optional) Flush the ARP and MAC address tables within the network infrastructure. Ask your network administrator for more information about this step.

Step 3 Restart the access points.

Step 4 To configure the controller not to be a master controller once all the access points have joined the new controller, enter this command:

config network master-base disable

Viewing CAPWAP MTU Information

To view the maximum transmission unit (MTU) for the CAPWAP path on the controller, enter this command. The MTU specifies the maximum size of any packet (in bytes) in a transmission.

show ap config general *Cisco_AP*

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.

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 non-privileged 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.

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, you can set a global username, password, and enable password that all access points inherit as they join the controller. This includes all access points that are currently joined to the controller and any that join in the future. 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, 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 non-privileged mode, and you must enter the enable password in order to use the privileged mode.

Note These controller software release 5.0(or later) 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.

Note 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 ever 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 **clear config** on the controller CLI. To clear the access point's configuration, enter **clear ap config** *Cisco_AP* on the controller CLI. Once the access point rejoins a controller, it adopts the default *Cisco*/*Cisco* username and password.

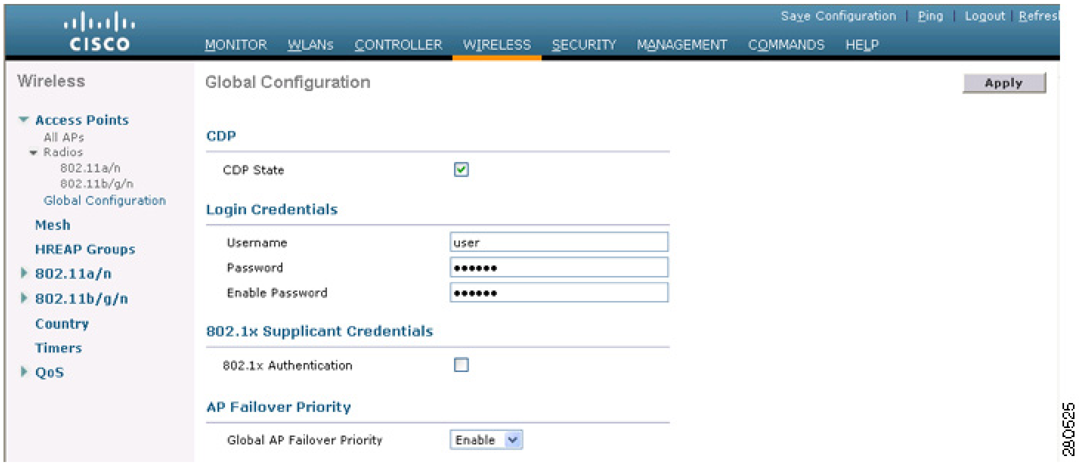
You can use the controller GUI or CLI to configure global credentials for access points that join the controller.

Using the GUI to Configure Global Credentials for Access Points

Using the controller GUI, follow these steps to configure global credentials for access points that join the controller.

Step 1 Click **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page (see Figure 7-1).

Figure 7-1 Global Configuration Page



Global Configuration

CDP

CDP State ☑

Login Credentials

Username user
Password ••••••
Enable Password ••••••

802.1x Supplicant Credentials

802.1x Authentication □

AP Failover Priority

Global AP Failover Priority Enable

Step 2 In the Username field, enter the username that is to be inherited by all access points that join the controller.

Step 3 In the Password field, enter the password that is to be inherited by all access points that join the controller.

Step 4 In the Enable Password field, 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.

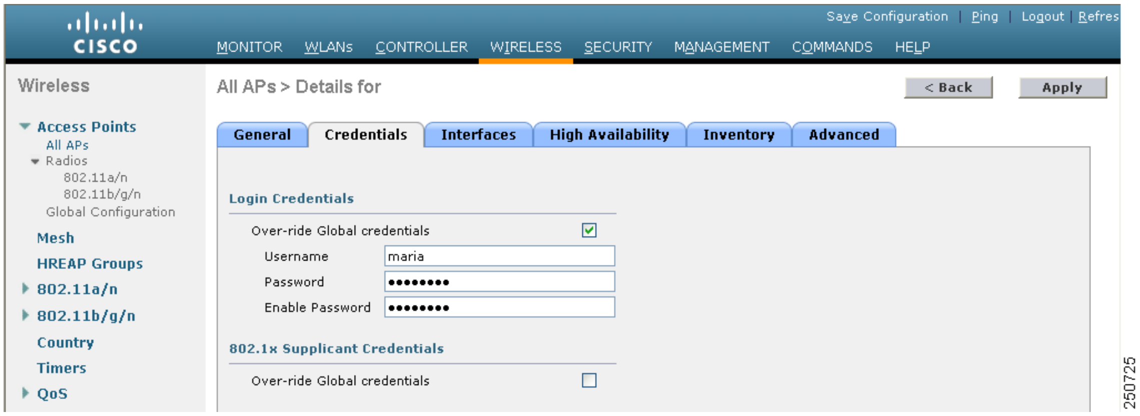
Step 7 If desired, you can choose to override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point. Follow these steps to do so:

a. Click **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. Click the **Credentials** tab. The All APs > Details for (Credentials) page appears (see Figure 7-2).

Figure 7-2 All APs > Details for (Credentials) Page



Login Credentials

Over-ride Global credentials ☑

Username: maria

Password: ••••••••

Enable Password: ••••••••

802.1x Supplicant Credentials

Over-ride Global credentials □

d. Check 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 unchecked.

e. In the Username, Password, and Enable Password fields, 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.

f. Click **Apply** to commit your changes.

g. Click **Save Configuration** to save your changes.

Note If you ever want to force this access point to use the controller's global credentials, simply uncheck the **Over-ride Global Credentials** check box.

Using the CLI to Configure Global Credentials for Access Points

Using the controller CLI, follow these steps to configure global credentials for access points that join the controller.

Step 1 To 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, enter this command:

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password* **all**

Step 2 If desired, you can choose to override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point. To do so, enter 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 ever want to force this access point to use the controller's global credentials, enter this command: **config ap mgmtuser delete** *Cisco_AP*. The following message appears after you execute this command: "AP reverted to global username configuration."

Step 3 To save your changes, enter this command:

save config

Step 4 To verify that global credentials are configured for all access points that join the controller, enter 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
-------- ------ ------------------ ------------------ ----------------- ----  -------
HReap      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 field shows "Not Configured."

Step 5 To see the global credentials configuration for a specific access point, enter 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................................ HReap
...
AP User Mode.................................... AUTOMATIC
AP User Name.................................... globalap
...
```

Note If this access point is configured for global credentials, the AP User Mode fields shows "Automatic." If the global credentials have been overwritten for this access point, the AP User Mode field shows "Customized."

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.

This feature is supported on the following hardware:

- Cisco Aironet 1130, 1140, 1240, and 1250 series access points
- All controller platforms running in local, hybrid-REAP, monitor, or sniffer mode. Bridge mode is not supported.

  Note In hybrid-REAP mode, you cannot configure local switching with 802.1X authentication; you can configure central switching only.

- All Cisco switches that support authentication

  Note Refer to the *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 5.2* for a list of supported switch hardware and minimum supported software.

You can configure global authentication settings that all access points inherit as they join the controller. This includes 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.

Observe the following flow for configuring authentication for access points:

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 the following command:

      lwapp ap dot1x username *username* **password** *password*

Note If you choose to follow this suggested flow and enable 802.1X authentication on the switch port after the access point has joined the controller and received the configured 802.1X credentials, you do not need to enter this command.

Note This command is available only for access points that are running the 5.1 or 5.2 recovery image.

c. Connect the access point to the switch port.

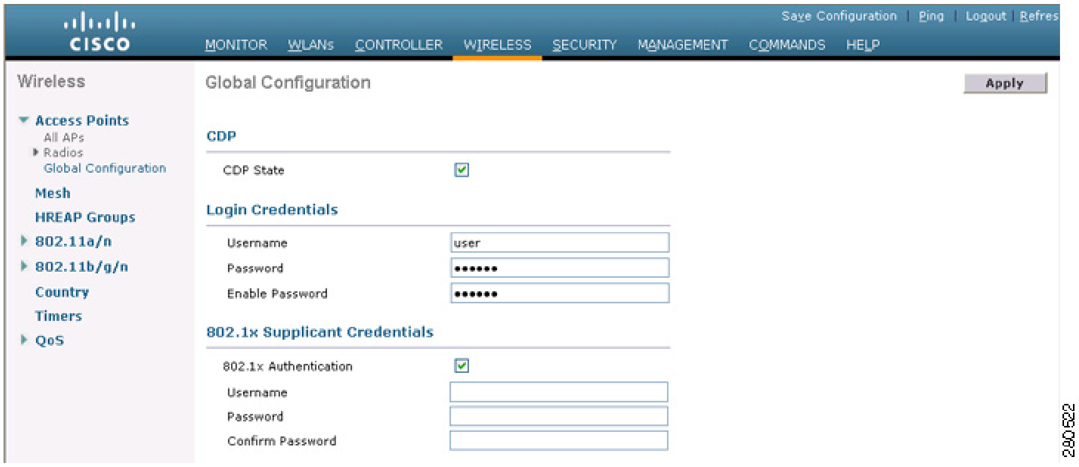
2. Install the 5.1 or 5.2 image on the controller and reboot the controller.
3. Allow all access points to join the controller.
4. Configure authentication on the controller. See the "Using the GUI to Configure Authentication for Access Points" section on page 7-10 or the "Using the CLI to Configure Authentication for Access Points" section on page 7-12 for information on configuring authentication on the controller.
5. Configure the switch to allow authentication. See the "Configuring the Switch for Authentication" section on page 7-14 for information on configuring the switch for authentication.

Using the GUI to Configure Authentication for Access Points

Using the controller GUI, follow these steps to configure authentication for access points that join the controller.

Step 1 Click **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page (see Figure 7-3).

Figure 7-3 Global Configuration Page



Global Configuration

CDP

CDP State ☑

Login Credentials

Username user

Password ••••••

Enable Password ••••••

802.1x Supplicant Credentials

802.1x Authentication ☑

Username

Password

Confirm Password

Step 2 Under 802.1x Supplicant Credentials, check the **802.1x Authentication** check box.

Step 3 In the Username field, enter the username that is to be inherited by all access points that join the controller.

Step 4 In the Password and Confirm Password fields, 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 fields. Strong passwords have the following characteristics:
- They are at least eight characters long.
- They contain a combination of upper- 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.

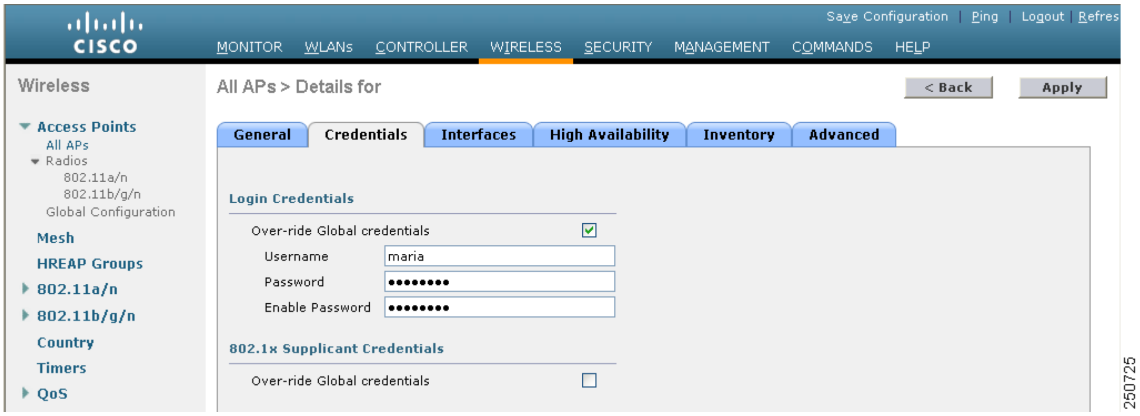
Step 7 If desired, you can choose to override the global authentication settings and assign a unique username and password to a specific access point. Follow these steps to do so:

a. Click **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. Click the **Credentials** tab to open the All APs > Details for (Credentials) page (see Figure 7-4).

Figure 7-4 All APs > Details for (Credentials) Page



Login Credentials

Over-ride Global credentials ☑

Username maria

Password ••••••••

Enable Password ••••••••

802.1x Supplicant Credentials

Over-ride Global credentials ☐

d. Under 802.1x Supplicant Credentials, check 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 unchecked.

e. In the Username, Password, and Confirm Password fields, 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 ever want to force this access point to use the controller's global authentication settings, simply uncheck the **Over-ride Global Credentials** check box.

Using the CLI to Configure Authentication for Access Points

Using the controller CLI, follow these steps to configure authentication for access points that join the controller.

Step 1 To 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, enter this command:

config ap dot1xuser add username *user* **password** *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 upper- and lowercase letters, numbers, and symbols.
- They are not a word in any language.

Step 2 If desired, you can choose to override the global authentication settings and assign a unique username and password to a specific access point. To do so, enter this command:

config 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 ever want to force this access point to use the controller's global authentication settings, enter this command: **config ap dot1xuser delete** *Cisco_AP*. The following message appears after you execute this command: "AP reverted to global username configuration."

Step 3 To save your changes, enter this command:

save config

Step 4 If you ever want to disable 802.1X authentication for all access points or for a specific access point, enter this command:

config 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 To view the authentication settings for all access points that join the controller, enter 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 field shows "Not Configured."

Step 6 To view the authentication settings for a specific access point, enter 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................................ HReap
...
AP Dot1x User Mode............................. AUTOMATIC
AP Dot1x User Name............................. globalDot1x
...
```

Note If this access point is configured for global authentication, the AP Dot1x User Mode fields shows "Automatic." If the global authentication settings have been overwritten for this access point, the AP Dot1x User Mode field shows "Customized."

Configuring the Switch for Authentication

On the switch CLI, enter these commands to enable 802.1X authentication on a switch port:

```
Switch# configure terminal
Switch(config)# dot1x system-auth-control
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# radius-server host ip_addr auth-port port acct-port port key key
Switch(config)# interface fastethernet2/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
```

Embedded Access Points

Controller software release 5.1 or later supports the AP801, which is the integrated access point on the Cisco 800 Series Integrated Services Routers (ISRs). This access point uses a Cisco IOS software image that is separate from the router Cisco IOS software image. It can operate as an autonomous access point that is configured and managed locally, or it can operate as a centrally managed access point utilizing the CAPWAP or LWAPP protocol. The AP801 is preloaded with both an autonomous Cisco IOS release and a recovery image for the unified mode.

Note Before you use an AP801 Series Lightweight Access Point with controller software release 5.2, you must upgrade the software in the Cisco 800 Series Integrated Services Router (ISR) to Cisco IOS Release 12.4(22)T.

When you want to use the AP801 with a controller, you must enable the recovery image for the unified mode on the access point by entering this CLI command on the router in privileged EXEC mode: **service-module wlan-ap 0 bootimage unified**.

Note 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 this CLI command on the router to shut down and reboot the access point: **service-module wlan-ap 0 reload**. 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.

Note To use the CLI commands mentioned above, the router must be running Cisco IOS Release 12.4(20)T or later. If you experience any problems, refer to the "Troubleshooting an Upgrade or Reverting the AP to Autonomous Mode" section in the ISR configuration guide at this URL:
http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/admin_ap.html#wp1061143

In order 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 IOS image on the router. Refer to this URL for licensing information:

http://www.cisco.com/en/US/products/ps7138/index.html

After the AP801 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 802.11n radio supports lower power levels than the 802.11n radio in the Cisco Aironet 1250 series access points. The AP801 stores 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 can be used in hybrid-REAP mode. Refer to Chapter 13 for more information on hybrid REAP.

Note For more information on the AP801, refer to the documentation for the Cisco 800 Series ISRs at this URL:
http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html

Autonomous Access Points Converted to Lightweight Mode

You can use an upgrade conversion tool to convert autonomous Cisco Aironet 1100, 1130AG, 1200, 1240AG, 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.

Refer to 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:

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00804fc3dc.html

Guidelines for Using Access Points Converted to Lightweight Mode

Keep these guidelines in mind when you use autonomous access points that have been converted to lightweight mode:

- Converted access points support 2006, and 4400, and WiSM controllers only. When you convert an autonomous access point to lightweight mode, the access point can communicate with Cisco 2006 series controllers, and 4400 series controllers, or the controllers on a Cisco WiSM only.
- 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 equivalent to WDS when the access point associates to it.
- In controller software release 4.2 or later, 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 hybrid-REAP mode. See Chapter 13 for details.
- 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 7-6). Then, using the second controller's GUI, open the same page and paste the key-hash into the SHA1 Key Hash field 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). 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.

Using a Controller to Return to a Previous Release

Follow these steps to revert from lightweight mode to autonomous mode using a wireless LAN controller:

Step 1 Log into the CLI on the controller to which the access point is associated.

Step 2 Enter 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.

Using the MODE Button and a TFTP Server to Return to a Previous Release

Follow these steps to revert from lightweight mode to autonomous mode by using the access point MODE (reset) button to load a Cisco IOS release from a TFTP server:

Step 1 The PC on which your TFTP server software runs must be configured 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 7-33 to check 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, you can configure the controller to use a local significant certificate (LSC).

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 means of a secure key distribution requiring X.509 certificates on both the access point and controller. CAPWAP relies on a priori 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.

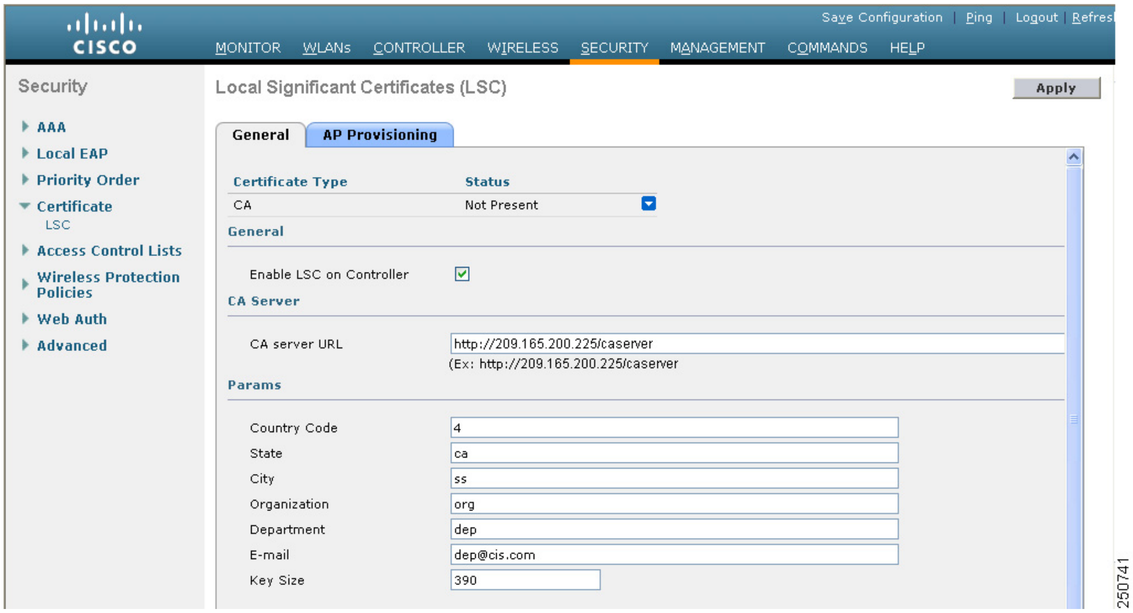
Note Access points that are configured for bridge mode are not supported.

Using the GUI to Configure LSC

Using the controller GUI, follow these steps to enable the use of LSC on the controller.

Step 1 Click **Security** > **Certificate** > **LSC** to open the Local Significant Certificates (LSC) page (see Figure 7-5).

Figure 7-5 Local Significant Certificates (LSC) Page



Local Significant Certificates (LSC)

Certificate Type	Status
CA	Not Present

General

Enable LSC on Controller ☑

CA Server

CA server URL http://209.165.200.225/caserver
(Ex: http://209.165.200.225/caserver

Params

Country Code	4
State	ca
City	ss
Organization	org
Department	dep
E-mail	dep@cis.com
Key Size	390

Step 2 Click the **General** tab.

Step 3 To enable LSC on the system, check the **Enable LSC on Controller** check box.

Step 4 In the CA Server URL field, enter the URL to the CA server. You can enter either a domain name or an IP address.

Step 5 In the Params fields, 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 6 Click **Apply** to commit your changes.

Step 7 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 8 To provision the LSC on the access point, click the **AP Provisioning** tab and check the **Enable AP Provisioning** check box.

Step 9 To add access points to the provision list, enter the access point MAC address in the AP Ethernet MAC Addresses field and click **Add**.

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 10 Click **Apply** to commit your changes.

Using the CLI to Configure LSC

Using the controller CLI, follow these steps to enable the use of LSC on the controller.

Step 1 To enable LSC on the system, enter this command:

config certificate lsc {**enable** | **disable**}

Step 2 To configure the URL to the CA server, enter 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; then configure a different CA server.

Step 3 To add the LSC CA certificate into the controller's CA certificate database, enter this command:

config certificate lsc ca-cert {**add** | **delete**}

Step 4 To configure the parameters for the device certificate, enter this command:

config certificate lsc subject-params *country state city orgn dept email*

Note The common name (CN) is generated automatically on the access point using the current MIC/SSC format C*xxxx-MacAddr*, where *xxxx* is the product number.

Step 5 To configure a key size, enter 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 To add access points to the provision list, enter this command:

config certificate lsc ap-provision auth-list add *AP_mac_addr*

Note To remove access points from the provision list, enter this command: **config certificate lsc ap-provision auth-list delete** *AP_mac_addr.*

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 To 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), enter 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.

If you set the number of retries to a non-zero 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, Cisco recommends that you configure a non-zero value.

Step 8 To provision the LSC on the access point, enter this command:

config certificate lsc ap-provision {**enable** | **disable**}

Step 9 To view the LSC summary, enter 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 To view details about the access points that are provisioned using LSC, enter this command:

show certificate lsc ap-provision

Information similar to the following appears:

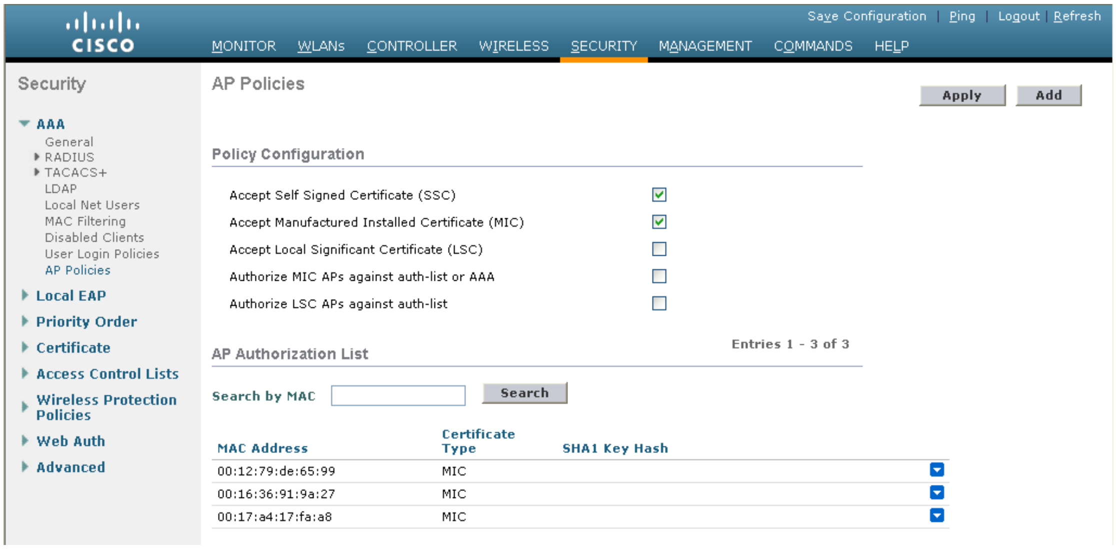
```
LSC AP-Provisioning.......................... Yes
Provision-List............................... Present

Idx     Mac Address
---     ------------
1       00:18:74:c7:c0:90
```

Using the GUI to Authorize Access Points

Using the controller GUI, follow these steps to authorize access points.

Step 1 Click **Security** > **AAA** > **AP Policies** to open the AP Policies page (see Figure 7-6).

Figure 7-6 AP Policies Page



AP Policies

Policy Configuration

Accept Self Signed Certificate (SSC) ☑

Accept Manufactured Installed Certificate (MIC) ☑

Accept Local Significant Certificate (LSC) □

Authorize MIC APs against auth-list or AAA □

Authorize LSC APs against auth-list □

AP Authorization List

Entries 1 - 3 of 3

Search by MAC

MAC Address	Certificate Type	SHA1 Key Hash
00:12:79:de:65:99	MIC	
00:16:36:91:9a:27	MIC	
00:17:a4:17:fa:a8	MIC	

Step 2 If you want the access point to accept self-signed certificates (SSCs), manufactured-installed certificates (MICs), or local significant certificates (LSCs), check the appropriate check box.

Step 3 If you want the access points to be authorized using a AAA RADIUS server, check the **Authorize MIC APs against auth-list or AAA** check box.

Step 4 If you want the access points to be authorized using an LSC, check the **Authorize LSC APs against auth-list** check box.

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

Step 6 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 field, enter the MAC address of the access point.

c. From the Certificate Type drop-down box, choose **MIC**, **SSC**, or **LSC**.

d. Click **Add**. The access point appears in the access point authorization list.

Note To remove an access point from the authorization list, hover your cursor over the blue drop-down arrow for the access point and choose **Remove**.

Note To search for a specific access point in the authorization list, enter the MAC address of the access point in the Search by MAC field and click **Search**.

Using the CLI to Authorize Access Points

Using the controller CLI, follow these steps to authorize access points.

Step 1 To configure an access point authorization policy, enter this command:

config auth-list ap-policy {**authorize-ap** {**enable** | **disable**} | **authorize-lsc-ap** {**enable** | **disable**}}

Step 2 To configure an access point to accept manufactured-installed certificates (MICs), self-signed certificates (SSCs), or local significant certificates (LSCs), enter this command:

config auth-list ap-policy {**mic** | **ssc** | **lsc** {**enable** | **disable**}}

Step 3 To add an access point to the authorization list, enter 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.

Note To delete an access point from the authorization list, enter this command: **config auth-list delete** *ap_mac*.

Step 4 To view the access point authorization list, enter this command:

show auth-list

Information similar to the following appears:

```
Authorize MIC APs against AAA ....................... disabled
Authorize LSC APs against Auth-List ................ disabled

Allow APs with MIC - Manufactured Installed C ....... enabled
Allow APs with SSC - Self-Signed Certificate ........ enabled
Allow APs with LSC - Locally Significant Cert ....... enabled

Mac Addr                  Cert Type    Key Hash
-----------------------   ----------   ---------------------------------------------
00:12:79:de:65:99          SSC        ca528236137130d37049a5ef3d1983b30ad7e543
00:16:36:91:9a:27          MIC        593f34e7cb151997a28cc7da2a6cac040b329636
```

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 access point's DHCP Vendor Class Identifier (VCI) string (DHCP Option 60). Table 7-1 lists the VCI strings for Cisco access points capable of operating in lightweight mode.

Table 7-1 VCI Strings For Lightweight Access Points

Access Point	VCI String
Cisco Aironet 1130 Series	Cisco AP c1130
Cisco Aironet 1140 Series	Cisco AP c1140
Cisco Aironet 1200 Series	Cisco AP c1200
Cisco Aironet 1240 Series	Cisco AP c1240
Cisco Aironet 1250 Series	Cisco AP c1250
Cisco AP801 Embedded Access Point	Cisco AP801

This is the format of the TLV block:

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

Refer to 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.

Troubleshooting the Access Point Join Process

Access points can fail to join a controller for many reasons: 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.

Controller software release 5.2 enables 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. Therefore, 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 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 2100 series controllers and 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 running software release 4.2 or later has been newly deployed.
- An existing access point running a software release prior to 4.2 has been upgraded to 4.2 or a later release.
- An existing access point running software release 4.2 or later 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. The relevant command is **lwapp ap log-server** *syslog_server_IP_address*.

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.

You can configure the syslog server for access points and view the access point join information only from the controller CLI.

Configuring the Syslog Server for Access Points

Follow these steps to configure the syslog server for access points using the controller 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, indicating that it 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 To save your changes, enter this command:

save config

Step 3 To see the global syslog server settings for all access points that join the controller, enter this command:

show ap config global

Information similar to the following appears:

```
AP global system logging host................... 255.255.255.255
```

Step 4 To see the syslog server settings for a specific access point, enter this command:

show ap config general *Cisco_AP*

Viewing Access Point Join Information

Join statistics for an access point that sent 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 if the controller is rebooted.

Use these CLI commands to view access point join information:

- To see the MAC addresses of all the access points that are joined to the controller or that have tried to join, enter this command:

  show ap join stats summary all

Information similar to the following appears:

```
Number of APs.............................................. 3

00:0b:85:1b:7c:b0.......................................... Joined
00:12:44:bb:25:d0.......................................... Joined
00:13:19:31:9c:e0.......................................... Not joined
```

- To see the last join error detail for a specific access point, enter 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 this command on the access point CLI: **show interfaces Dot11Radio 0**

  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
```

- To see all join-related statistics collected for a specific access point, enter 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
```

Using a Controller to Send Debug Commands to Access Points Converted to Lightweight Mode

Enter this command to enable the controller to send debug commands to an access point converted to lightweight mode:

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.

Converted Access Points Send Crash Information to 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.

Converted Access Points Send Radio Core Dumps to 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 alerting the network administrator, and the administrator can retrieve the radio core file from the access point.

The retrieved core file is stored in the controller flash and can subsequently 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.

Using the CLI to Retrieve Radio Core Dumps

Using the controller CLI, follow these steps to retrieve the radio core dump file.

Step 1 To transfer the radio core dump file from the access point to the controller, enter 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 To verify that the file was downloaded to the controller, enter this command:

show ap crash-file

Information similar to the following appears:

```
Local Core Files:
lrad_AP1130.rdump0   (156)
```

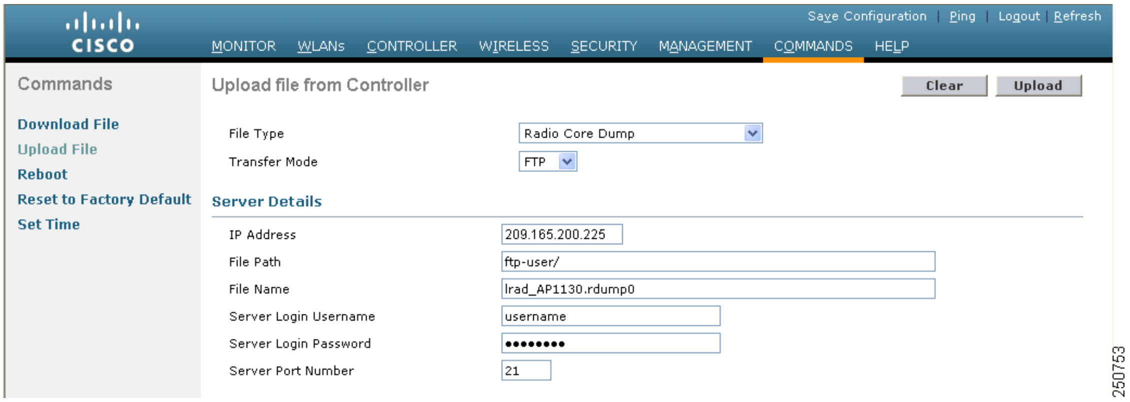
The number in parentheses indicates the size of the file. The size should be greater than zero if a core dump file is available.

Using the GUI to Upload Radio Core Dumps

Using the controller GUI, follow these steps to upload the radio core dump file to a TFTP or FTP server.

Step 1 Click **Commands** > **Upload File** to open the Upload File from Controller page (see Figure 7-7).

Figure 7-7 Upload File from Controller Page



Upload file from Controller

File Type: Radio Core Dump
Transfer Mode: FTP

Server Details

IP Address: 209.165.200.225
File Path: ftp-user/
File Name: lrad_AP1130.rdump0
Server Login Username: username
Server Login Password: ••••••••
Server Port Number: 21

Step 2 From the File Type drop-down box, choose **Radio Core Dump**.

Step 3 From the Transfer Mode drop-down box, choose **TFTP** or **FTP**.

Step 4 In the IP Address field, enter the IP address of the TFTP or FTP server.

Step 5 In the File Path field, enter the directory path of the file.

Step 6 In the File Name field, 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 field, enter the FTP server login name.

b. In the Server Login Password field, enter the FTP server login password.

c. In the Server Port Number field, 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.

Using the CLI to Upload Radio Core Dumps

Using the controller CLI, follow these steps to upload the radio core dump file to a TFTP or FTP server.

Step 1 To transfer the file from the controller to a TFTP or FTP server, enter 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*
- **transfer upload filename** *filename*

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 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 To view the updated settings, enter 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

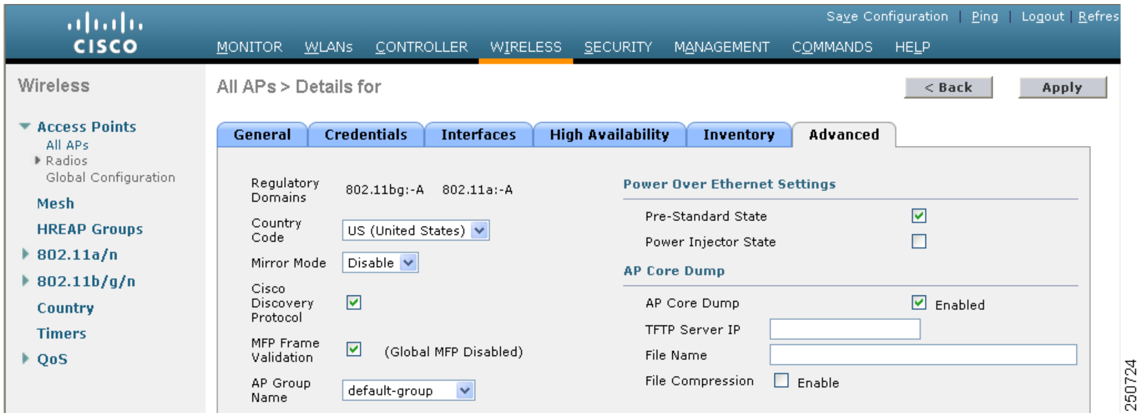
By default, access points converted to lightweight mode do not send memory core dumps to the controller. This section provides instructions to upload access point core dumps using the controller GUI or CLI.

Using the GUI to Upload Access Point Core Dumps

Using the controller GUI, follow these steps to upload a core dump file of the access point.

Step 1 Click **Wireless** > **Access Points** > **All APs** > *access point name* > the **Advanced** tab to open the All APs > Details for (Advanced) page (see Figure 7-8).

Figure 7-8 All APs > Details for (Advanced) Page



Regulatory Domains 802.11bg:-A 802.11a:-A

Country Code US (United States)

Mirror Mode Disable

Cisco Discovery Protocol ☑

MFP Frame Validation ☑ (Global MFP Disabled)

AP Group Name default-group

Power Over Ethernet Settings

Pre-Standard State ☑

Power Injector State □

AP Core Dump

AP Core Dump ☑ Enabled

TFTP Server IP

File Name

File Compression □ Enable

Step 2 To upload a core dump of the access point, check the **AP Core Dump** check box.

Step 3 In the TFTP Server IP field, enter the IP address of the TFTP server.

Step 4 In the File Name field, enter a name of the access point core dump file (such as *dump.log*).

Step 5 To compress the access point core dump file, check the **File Compression** check box. 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.

Using the CLI to Upload Access Point Core Dumps

Using the controller CLI, follow these steps to upload a core dump file of the access point.

Step 1 To upload a core dump of the access point, enter this command on the controller:

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,

  Note The access point must be able to reach the TFTP server.

- *filename* is the name that the access points 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, and

  Note 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 whereas **all** is all access points converted to lightweight mode.

Step 2 To save your changes, enter this command:

save config

Display of 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 an Access Point Converted to Lightweight Mode

After an access point converted to lightweight mode associates to a controller, enter this command to configure a static IP address on the access point:

config ap static-ip enable *ap-name ip-address mask gateway*

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, the **show ap config general** *Cisco_AP* CLI command correctly shows 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.

Supporting Oversized Access Point Images

Controller software release 5.0 or later allows 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.

Follow these steps to perform 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.

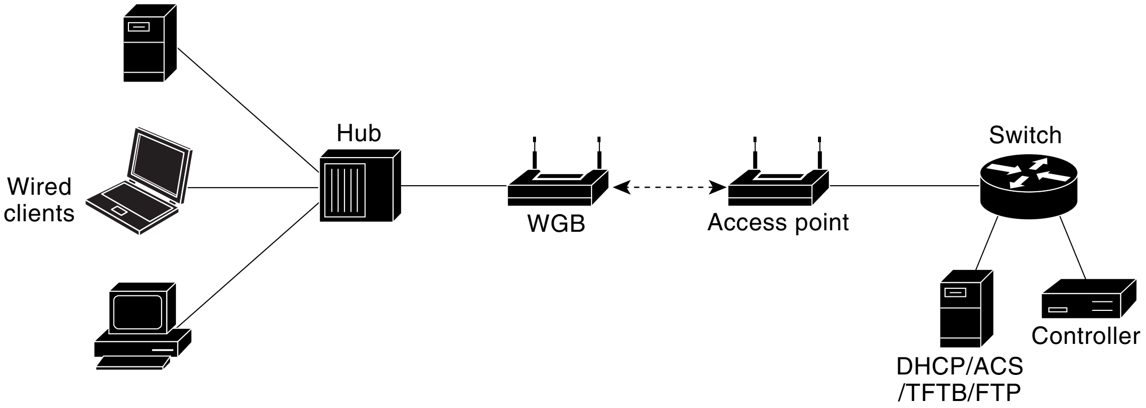
Step 2 Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the controller to download the oversized access point image and complete the upgrade procedure.

Step 3 After the access point has been recovered, you may remove the TFTP server.

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 7-9.

Figure 7-9 WGB Example



Note If the lightweight access point fails, the WGB attempts to associate to another access point.

Guidelines for Using WGBs

Follow these guidelines for using WGBs on your network:

- 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 (on 32-MB access points) or Cisco IOS Release 12.3(8)JEB or later (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. Cisco recommends that you disable the second radio.

  Note The controller supports only Cisco WGB products. Linksys and OEM WGB devices are not supported. Although the Cisco Wireless Unified Solution does not support the Linksys WET54G and WET11B Ethernet Bridges, you can use these devices in a Wireless Unified Solution configuration if you follow these guidelines:
  1. Connect only one device to the WET54G or WET11B.
  2. Enable the MAC cloning feature on the WET54G or WET11B to clone the connected device.
  3. Install the latest drivers and firmware on devices connected to the WET54G or WET11B. This guideline is especially important for JetDirect printers because early firmware versions might cause problems with DHCP.
  Note: Because these devices are not supported in the Cisco Wireless Unified Solution, Cisco Technical Support cannot help you troubleshoot any problems associated with them.

  Perform one of the following to enable the workgroup bridge mode on the WGB:

  - 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 this command: **station-role workgroup-bridge**

  Note See the sample WGB access point configuration in the "Sample WGB Configuration" section on page 7-37.

- The WGB can associate only to lightweight access points.
- Only WGBs in client mode (which is the default value) are supported. Those in infrastructure mode are not supported. 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 this command: **no infrastructure client**.

  Note VLANs are not supported for use with WGBs.

Note See the sample WGB access point configuration in the "Sample WGB Configuration" section on page 7-37.

- 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
- These features are not supported for use with a WGB:
  - Cisco Centralized Key Management (CCKM)
  - Hybrid REAP
  - 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, Cisco recommends 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 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. Cisco recommends 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.

Sample WGB Configuration

Here is a sample 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)#WGB_with_static_WEP
ap(config-if)#end
```

To verify that the WGB is associated to an access point, enter this command on the WGB:

show dot11 association

Information similar to the following appears:

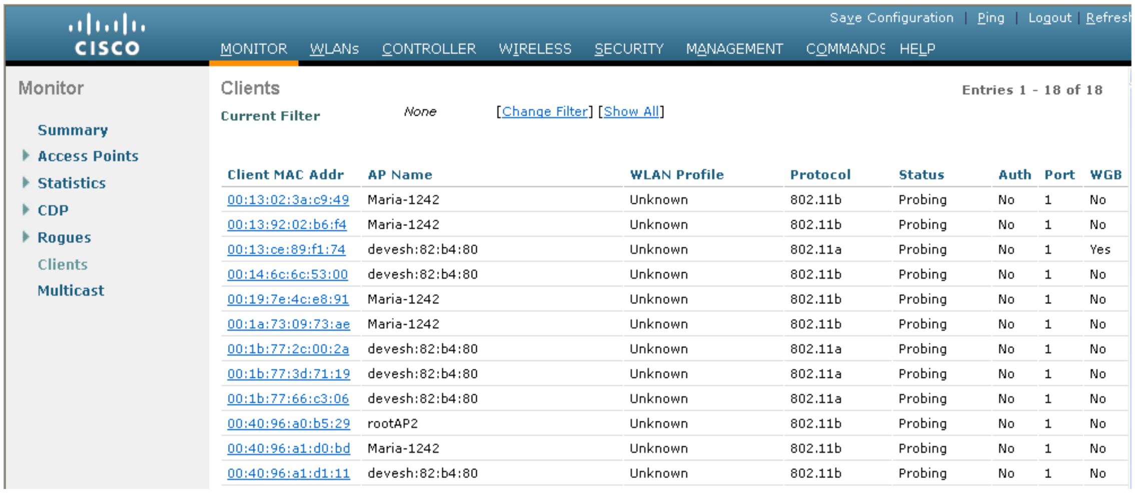
```
ap#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address    IP address      Device        Name            Parent         State
000b.8581.6aee 10.11.12.1      WGB-client    map1            -              Assoc
ap#
```

Using the GUI to View the Status of Workgroup Bridges

Follow these steps to view the status of WGBs on your network using the controller GUI.

Step 1 Click **Monitor** > **Clients** to open the Clients page (see Figure 7-10).

Figure 7-10 Clients Page


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Access Points
Statistics
CDP
Rogues
Clients
Multicast
212211

Clients

Entries 1 - 18 of 18

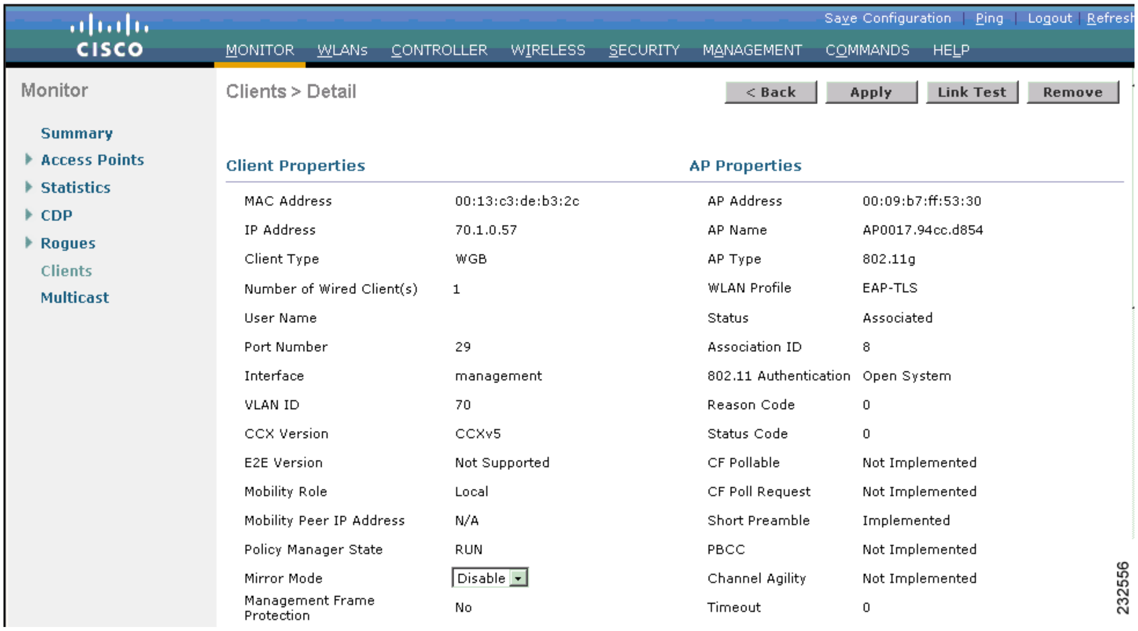
Current Filter None [Change Filter] [Show All]

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:13:02:3a:c9:49	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:13:92:02:b6:f4	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:13:ce:89:f1:74	devesh:82:b4:80	Unknown	802.11a	Probing	No	1	Yes
00:14:6c:6c:53:00	devesh:82:b4:80	Unknown	802.11b	Probing	No	1	No
00:19:7e:4c:e8:91	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:1a:73:09:73:ae	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:1b:77:2c:00:2a	devesh:82:b4:80	Unknown	802.11a	Probing	No	1	No
00:1b:77:3d:71:19	devesh:82:b4:80	Unknown	802.11a	Probing	No	1	No
00:1b:77:66:c3:06	devesh:82:b4:80	Unknown	802.11a	Probing	No	1	No
00:40:96:a0:b5:29	rootAP2	Unknown	802.11b	Probing	No	1	No
00:40:96:a1:d0:bd	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:40:96:a1:d1:11	devesh:82:b4:80	Unknown	802.11b	Probing	No	1	No

The WGB field 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 (see Figure 7-11).

Figure 7-11 Clients > Detail Page


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Access Points
Statistics
CDP
Rogues
Clients
Multicast
< Back
Apply
Link Test
Remove
232556

Clients > Detail

Client Properties		AP Properties	
MAC Address	00:13:c3:de:b3:2c	AP Address	00:09:b7:ff:53:30
IP Address	70.1.0.57	AP Name	AP0017.94cc.d854
Client Type	WGB	AP Type	802.11g
Number of Wired Client(s)	1	WLAN Profile	EAP-TLS
User Name		Status	Associated
Port Number	29	Association ID	8
Interface	management	802.11 Authentication	Open System
VLAN ID	70	Reason Code	0
CCX Version	CCXv5	Status Code	0
E2E Version	Not Supported	CF Pollable	Not Implemented
Mobility Role	Local	CF Poll Request	Not Implemented
Mobility Peer IP Address	N/A	Short Preamble	Implemented
Policy Manager State	RUN	PBCC	Not Implemented
Mirror Mode	Disable	Channel Agility	Not Implemented
Management Frame Protection	No	Timeout	0

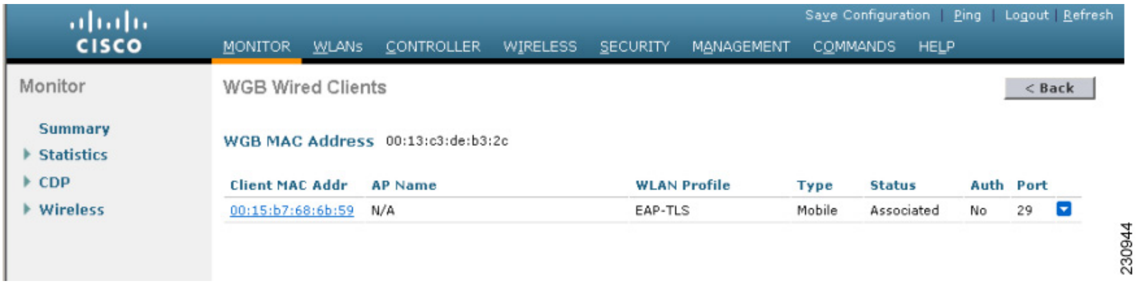
The Client Type field under Client Properties shows "WGB" if this client is a workgroup bridge, and the Number of Wired Client(s) field shows the number of wired clients that are connected to this WGB.

Step 3 To see the details of any wired clients that are connected to a particular WGB, follow these steps:

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 (see Figure 7-12).

Figure 7-12 WGB Wired Clients Page


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Statistics
CDP
Wireless
< Back
230944

WGB Wired Clients

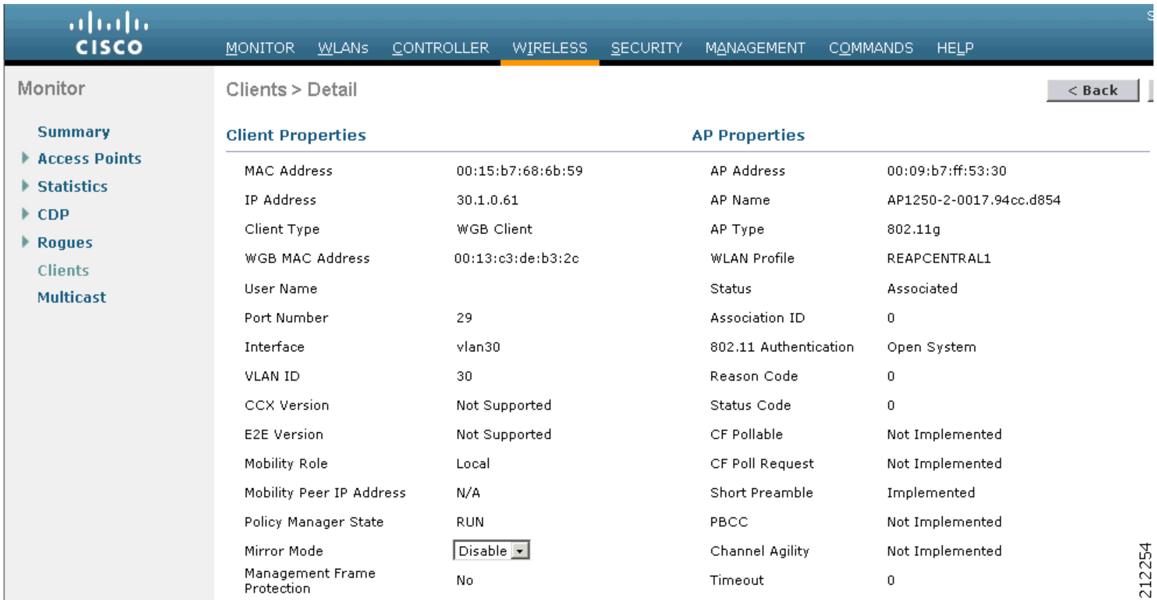
WGB MAC Address 00:13:c3:de:b3:2c

Client MAC Addr	AP Name	WLAN Profile	Type	Status	Auth	Port
00:15:b7:68:6b:59	N/A	EAP-TLS	Mobile	Associated	No	29

Note If you ever 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 (see Figure 7-13).

Figure 7-13 Clients > Detail Page



Clients > Detail

Client Properties		AP Properties	
MAC Address	00:15:b7:68:6b:59	AP Address	00:09:b7:ff:53:30
IP Address	30.1.0.61	AP Name	AP1250-2-0017.94cc.d854
Client Type	WGB Client	AP Type	802.11g
WGB MAC Address	00:13:c3:de:b3:2c	WLAN Profile	REAPCENTRAL1
User Name		Status	Associated
Port Number	29	Association ID	0
Interface	vlan30	802.11 Authentication	Open System
VLAN ID	30	Reason Code	0
CCX Version	Not Supported	Status Code	0
E2E Version	Not Supported	CF Pollable	Not Implemented
Mobility Role	Local	CF Poll Request	Not Implemented
Mobility Peer IP Address	N/A	Short Preamble	Implemented
Policy Manager State	RUN	PBCC	Not Implemented
Mirror Mode	Disable	Channel Agility	Not Implemented
Management Frame Protection	No	Timeout	0

The Client Type field under Client Properties shows "WGB Client," and the rest of the fields on this page provide additional information for this client.

Using the CLI to View the Status of Workgroup Bridges

Follow these steps to view the status of WGBs on your network using the controller CLI.

Step 1 To see any WGBs on your network, enter this command:

show wgb summary

Information similar to the following appears:

```
Number of WGBs.................................. 1

MAC Address        IP Address AP Name  Status  WLAN  Auth  Protocol  Clients
----------------- ----------  -------- ------  ----  ----- --------- --------
00:0d:ed:dd:25:82  10.24.8.73      a1   Assoc   3     Yes   802.11b   1
```

Step 2 To see the details of any wired clients that are connected to a particular WGB, enter this command:

show wgb detail *wgb_mac_address*

Information similar to the following appears:

```
Number of wired client(s): 1

MAC Address         IP Address AP Name  Mobility   WLAN   Auth
------------------- ---------- -------- ---------  -----  -----
00:0d:60:fc:d5:0b   10.24.8.75   a1      Local      3     Yes
```

Using the CLI to Debug WGB Issues

Use the commands in this section if you experience any problems with the WGB.

1. To enable debugging for IAPP messages, errors, and packets, enter 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.
2. If you experience a roaming issue, enter this command:

   debug mobility handoff enable
3. If you experience an IP assignment issue and DHCP is used, enter these commands:
   - **debug dhcp message enable**
   - **debug dhcp packet enable**
4. If you experience an IP assignment issue and static IP is used, enter these commands:
   - **debug dot11 mobile enable**
   - **debug dot11 state enable**

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 need not be in the same mobility group. In controller software release 4.2 or later, 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.

In controller software release 5.0 or later, 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.

Note You can configure the fast heartbeat timer only for access points in local and hybrid-REAP 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, 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.

Note 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 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 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.

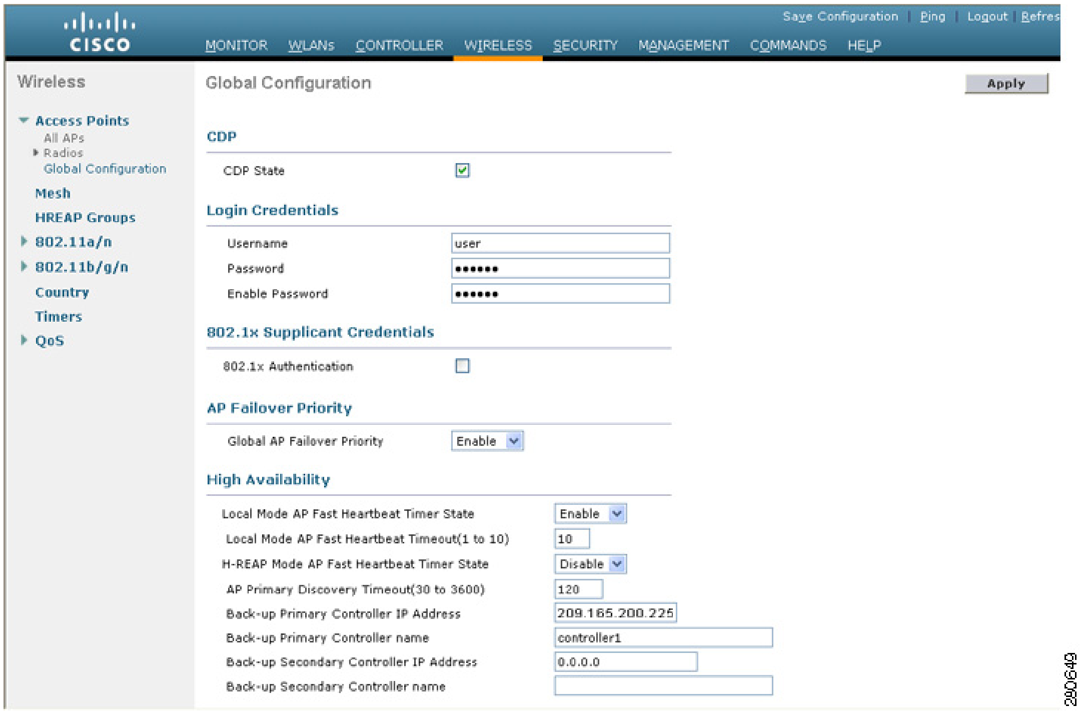
Note If you inadvertently configure a controller that is running software release 5.2 with a failover controller that is running a different software release (such as 4.2, 5.0, or 5.1), the access point might take a long time to join the failover controller because the access point starts the discovery process in CAPWAP and then changes to LWAPP discovery.

Using the GUI to Configure Backup Controllers

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

Step 1 Click **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page (see Figure 7-14).

Figure 7-14 Global Configuration Page



Global Configuration

CDP

CDP State ☑

Login Credentials

Username: user
Password: ••••••
Enable Password: ••••••

802.1x Supplicant Credentials

802.1x Authentication ☐

AP Failover Priority

Global AP Failover Priority: Enable

High Availability

Local Mode AP Fast Heartbeat Timer State: Enable
Local Mode AP Fast Heartbeat Timeout(1 to 10): 10
H-REAP Mode AP Fast Heartbeat Timer State: Disable
AP Primary Discovery Timeout(30 to 3600): 120
Back-up Primary Controller IP Address: 209.165.200.225
Back-up Primary Controller name: controller1
Back-up Secondary Controller IP Address: 0.0.0.0
Back-up Secondary Controller name:

Step 2 From the Local Mode AP Fast Heartbeat Timer State drop-down box, choose **Enable** to enable the fast heartbeat timer for access points in local mode or **Disable** to disable this timer. The default value is Disable.

Step 3 If you chose Enable in Step 2, enter a number between 1 and 10 seconds (inclusive) in the Local Mode AP Fast Heartbeat Timeout field 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 default value is 0 seconds, which disables the timer.

Step 4 From the H-REAP Mode AP Fast Heartbeat Timer State drop-down box, choose **Enable** to enable the fast heartbeat timer for hybrid-REAP access points or **Disable** to disable this timer. The default value is Disable.

Step 5 If you chose Enable in Step 4, enter a value between 1 and 10 seconds (inclusive) in the H-REAP Mode AP Fast Heartbeat Timeout field to configure the fast heartbeat timer for hybrid-REAP access points. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure. The default value is 0 seconds, which disables the timer.

Step 6 In the AP Primary Discovery Timeout field, 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 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 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 field and the name of the controller in the Back-up Secondary Controller Name field.

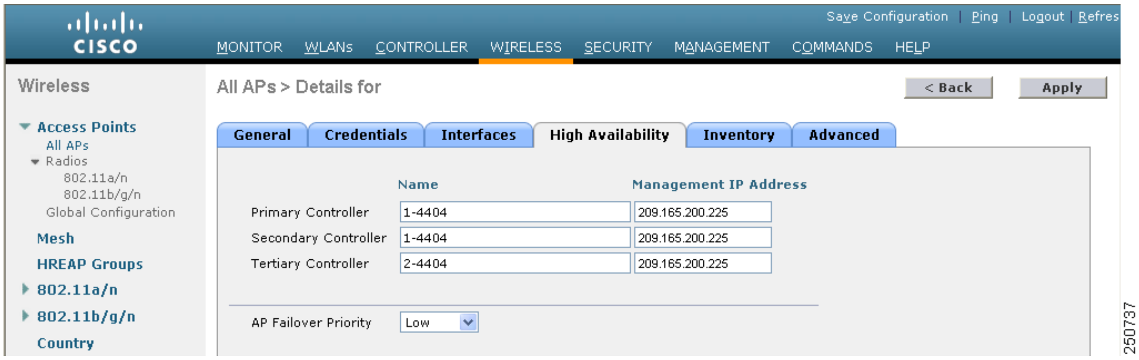
> **Note** The default value for the IP address is 0.0.0.0, which disables the secondary backup controller.

Step 9 Click **Apply** to commit your changes.

Step 10 If you want to configure primary, secondary, and tertiary backup controllers for a specific point, follow these steps:

- **a.** Click **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 to open the All APs > Details for (High Availability) page (see Figure 7-15).

Figure 7-15 All APs > Details for (High Availability) Page



	Name	Management IP Address
Primary Controller	1-4404	209.165.200.225
Secondary Controller	1-4404	209.165.200.225
Tertiary Controller	2-4404	209.165.200.225

AP Failover Priority: Low

- **d.** If desired, enter the name and IP address of the primary backup controller for this access point in the Primary Controller fields.

> **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 backup controller for this access point in the Secondary Controller fields.

f. If desired, enter the name and IP address of the tertiary backup controller for this access point in the Tertiary Controller fields.

g. Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Using the CLI to Configure Backup Controllers

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

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

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

Step 3 To configure a tertiary controller for a specific 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 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 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 enable or disable the fast heartbeat timer for local or hybrid-REAP access points, enter this command:

config advanced timers ap-fast-heartbeat {**local** | **hreap** | **all**} {**enable** | **disable**} *interval*

where **all** is both local and hybrid-REAP access points, and *interval* is a value between 1 and 10 seconds (inclusive). Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure. The default value is disabled.

Step 7 To configure the access point heartbeat timer, enter 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.

Step 8 To configure the 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 9 To configure the 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 10 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 11 To save your changes, enter this command:

save config

Step 12 To view an access point's configuration, enter 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 Hreap mode Fast Heartbeat (seconds).......... disable
AP Primary Discovery Timeout (seconds).......... 120
```

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.

In controller software releases prior to 5.1, the backup controllers accept association requests in the order 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, 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.

Note 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. You can do so using the controller GUI or CLI.

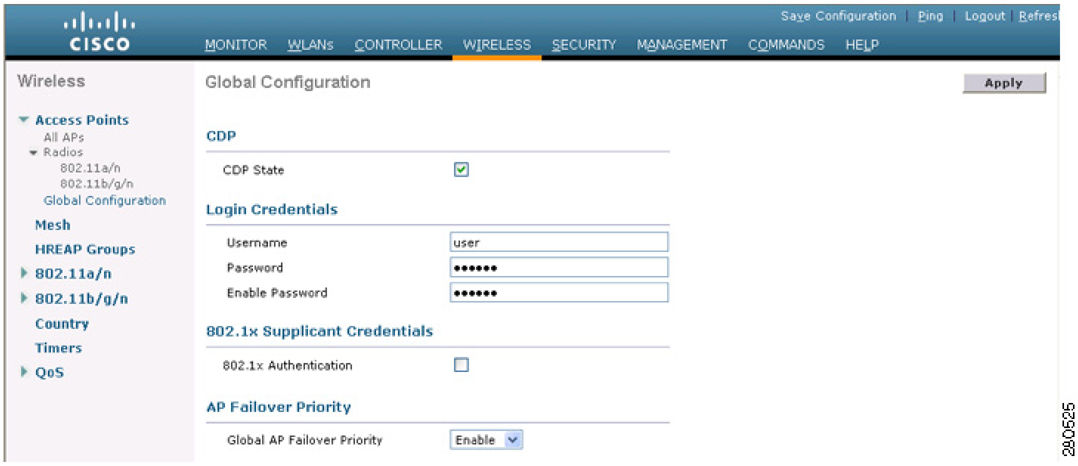
By default, all access points are set to priority level 1, which is the lowest priority level. Therefore, you need to assign a priority level only to those access points that warrant a higher priority.

Using the GUI to Configure Failover Priority for Access Points

Using the controller GUI, follow these steps to configure failover priority for access points that join the controller.

Step 1 Click **Wireless > Access Points > Global Configuration** to open the Global Configuration page (see Figure 7-16).

Figure 7-16 *Global Configuration Page*



Global Configuration

CDP

CDP State ☑

Login Credentials

Username user
Password ••••••
Enable Password ••••••

802.1x Supplicant Credentials

802.1x Authentication □

AP Failover Priority

Global AP Failover Priority Enable

Step 2 From the Global AP Failover Priority drop-down box, choose **Enable** to enable access point failover priority or **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.

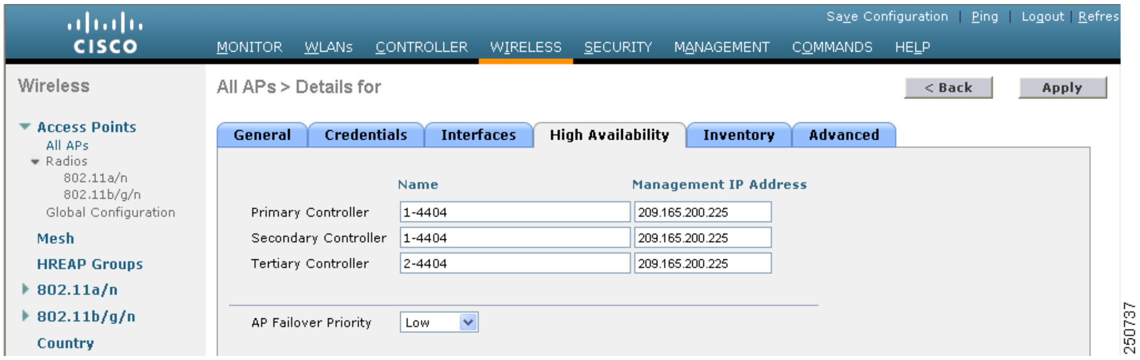
Step 4 Click **Save Configuration** to save your changes.

Step 5 Click **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 Click the **High Availability** tab. The All APs > Details for (High Availability) page appears (see Figure 7-17).

Figure 7-17 *All APs > Details for (High Availability) Page*



All APs > Details for

	Name	Management IP Address
Primary Controller	1-4404	209.165.200.225
Secondary Controller	1-4404	209.165.200.225
Tertiary Controller	2-4404	209.165.200.225

AP Failover Priority Low

Step 8 From the AP Failover Priority drop-down box, 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.

Using the CLI to Configure Failover Priority for Access Points

Using the controller CLI, follow these steps to configure failover priority for access points that join the controller.

Step 1 To enable or disable access point failover priority, enter this command:

config network ap-priority {**enable** | **disable**}

Step 2 To specify the priority of an access point, enter this command:

config ap priority {**1** | **2** | **3** | **4**} *Cisco_AP*

where 1 is the lowest priority level and 4 is the highest priority level. The default value is 1.

Step 3 To save your changes, enter this command:

save config

Using the CLI to View Failover Priority Settings

Use these commands to view the failover priority configuration settings on your network:

- To confirm whether access point failover priority is enabled on your network, enter this command:

  show network summary

  Information similar to the following appears:

```
RF-Network Name............................. mrf
Web Mode.................................... Enable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable
Ethernet Broadcast Mode..................... Disable
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority......................... Enabled
...
```

- To see the failover priority for each access point, enter this command:

  show ap summary

  Information similar to the following appears:

```
Number of APs.................................. 2
Global AP User Name............................ user
Global AP Dot1x User Name...................... Not Configured

AP Name  Slots  AP Model           Ethernet MAC       Location   Port Country Priority
-------  -----  ------------------ -----------------  ---------  ---- ------- -------
ap:1252  2      AIR-LAP1252AG-A-K9 00:1b:d5:13:39:74  hallway 6  1    US      1
ap:1121  1      AIR-LAP1121G-A-K9  00:1b:d5:a9:ad:08  reception  1    US      3
```

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.

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 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.

Note 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://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps6087_Products_Data_Sheet.html.

Guidelines for Configuring Multiple Country Codes

Follow these guidelines when configuring multiple country codes:

- 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.
- When multiple countries are configured and the radio resource management (RRM) auto-RF feature is enabled, the auto-RF feature is limited to only the channels that are legal in all configured countries and to the lowest power level common to all configured countries. The access points are always able to use all legal frequencies, but non-common channels can only be assigned manually.

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.

You can configure country codes through the controller GUI or CLI.

Using the GUI to Configure Country Codes

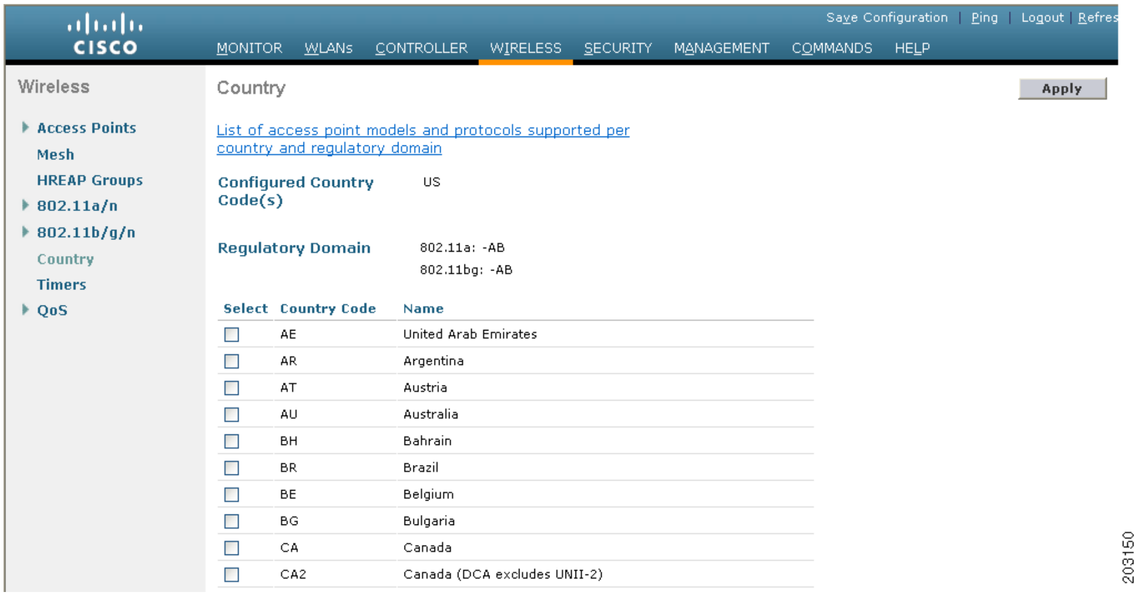
Follow these steps to configure country codes using the GUI.

Step 1 Follow these steps to disable the 802.11a and 802.11b/g networks:

- **a.** Click **Wireless > 802.11a/n > Network**.
- **b.** Uncheck the **802.11a Network Status** check box.
- **c.** Click **Apply** to commit your changes.
- **d.** Click **Wireless > 802.11b/g/n > Network**.
- **e.** Uncheck the **802.11b/g Network Status** check box.
- **f.** Click **Apply** to commit your changes.

Step 2 Click **Wireless > Country** to open the Country page (see Figure 7-18).

Figure 7-18 Country Page



Country

List of access point models and protocols supported per country and regulatory domain

Configured Country Code(s) US

Regulatory Domain 802.11a: -AB
802.11bg: -AB

Select	Country Code	Name
□	AE	United Arab Emirates
□	AR	Argentina
□	AT	Austria
□	AU	Australia
□	BH	Bahrain
□	BR	Brazil
□	BE	Belgium
□	BG	Bulgaria
□	CA	Canada
□	CA2	Canada (DCA excludes UNII-2)

Step 3 Check the check box for each country where your access points are installed.

Step 4 If you checked more than one check box in Step 3, a message appears indicating that RRM channels and power levels are limited to common channels and power levels. Click **OK** to continue or **Cancel** to cancel the operation.

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

Step 6 If you selected multiple country codes in Step 3, each access point is assigned to a country. Follow these steps to see the default country chosen for each access point and to choose a different country if necessary.

> **Note** If you ever 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.

a. Perform one of the following:

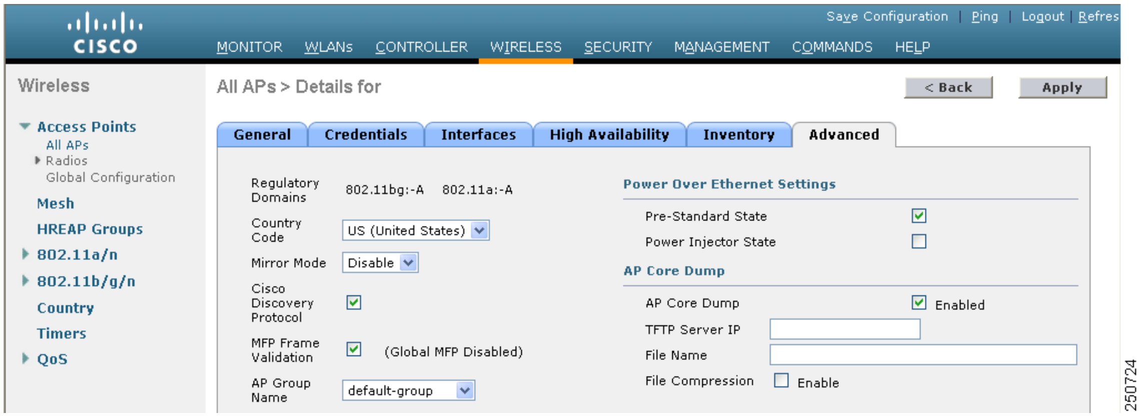
- Leave the 802.11a and 802.11b/g networks disabled.
- Re-enable the 802.11a and 802.11b/g networks and then disable only the access points for which you are configuring a country code. To disable an access point, click **Wireless** > **Access Points** > **All APs**, click the link of the desired access point, choose **Disable** from the Status drop-down box, and click **Apply**.

b. Click **Wireless** > **Access Points** > **All APs** to open the All APs page.

c. Click the link for the desired access point.

d. Click the **Advanced** tab to open the All APs > Details for (Advanced) page (see Figure 7-19).

Figure 7-19 All APs > Details for (Advanced) Page



All APs > Details for

Regulatory Domains 802.11bg:-A 802.11a:-A

Country Code US (United States)

Mirror Mode Disable

Cisco Discovery Protocol ☑

MFP Frame Validation ☑ (Global MFP Disabled)

AP Group Name default-group

Power Over Ethernet Settings

Pre-Standard State ☑

Power Injector State ☐

AP Core Dump

AP Core Dump ☑ Enabled

TFTP Server IP

File Name

File Compression ☐ Enable

e. The default country for this access point appears in the Country Code drop-down box. If the access point is installed in a country other than the one shown, choose the correct country from the drop-down box. 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. Re-enable any access points that you disabled in Step a.

Step 7 Re-enable the 802.11a and 802.11b/g networks, provided you did not re-enable them in Step 6.

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

Using the CLI to Configure Country Codes

Follow these steps to configure country codes using the CLI.

Step 1 To see a list of all available country codes, enter this command:

show country supported

Step 2 Enter these commands to disable the 802.11a and 802.11b/g networks:

config 802.11a disable network

config 802.11b disable network

Step 3 To configure the country codes for the countries where your access points are installed, enter this command:

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 2 3 4 5 6 7 8 9 0 1 2 3 4
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : A * * * * A * * * * A . . .
 CA (-AB)   : A * * * * A * * * * A . . .
 MX (-NA)   : A * * * * A * * * * A . . .
 Auto-RF    : C x x x x C x x x x C . . .
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11A    :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels    : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
--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
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 CA (-ABN)  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 MX (-N)    : . A . A . A . A A A A A . . . . . . . . . . . A A A A *
    Auto-RF : . C . C . C . C C C C C . . . . . . . . . . . C C C C x
```

Step 5 To verify your country code configuration, enter this command:

show country

Step 6 To see the list of available channels for the country codes configured on your controller, enter 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
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : A * * * * A * * * * A . . .
 CA (-AB)   : A * * * * A * * * * A . . .
 MX (-NA)   : A * * * * A * * * * A . . .
 Auto-RF    : C x x x x C x x x x C . . .
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11A    :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels    : 3 3 3 4 4 4 4 4 5 5 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 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 CA (-ABN)  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 MX (-N)    : . A . A . A . A A A A A . . . . . . . . . . . A A A A *
    Auto-RF : . C . C . C . C C C C C . . . . . . . . . . . C C C C x
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Step 7 To save your settings, enter this command:

save config

Step 8 To see the countries to which your access points have been assigned, enter this command:

show ap summary

Information similar to the following appears:

```
Number of APs.................................. 2

AP Name  Slots  AP Model          Ethernet MAC       Location          Port    Country
-------- ------ ----------------- -----------------  ----------------  ------- --------
ap1        2   AP1030            00:0b:85:5b:8e:c0  default location     1      US
ap2        2   AIR-AP1242AG-A-K9  00:14:1c:ed:27:fe  default location     1      US
```

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.
- Re-enable the 802.11a and 802.11b/g networks and then disable only the access points for which you are configuring a country code. To re-enable 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

AP Name     Country  Status
---------   -------- --------
ap2          US     enabled (Disable AP before configuring country)
ap1          MX     changed (New country configured, AP rebooting)
```

c. To re-enable any access points that you disabled in Step a, enter this command:

config ap enable *ap_name*

Step 10 If you did not re-enable the 802.11a and 802.11b/g networks in Step 9, enter these commands to re-enable them now:

config 802.11a enable network

config 802.11b enable network

Step 11 To save your settings, enter this command:

save config

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 field 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 = W52

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, as explained in the previous section, 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
- J3—Uses the -U frequencies but allows both -U and -P radios 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, you can use the multiple-country feature, explained in the previous section, to choose both J2 and J3. Then you can manually configure your -P radios to use the channels not supported by J3.

Refer to 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 for Migration

Follow these guidelines before migrating your access points to the -U regulatory domain:

- 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 greater 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 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 non-functioning 802.11a radios under software release 4.0.

Migrating Access Points to the -U Regulatory Domain

Follow these steps to migrate your access points from the -J regulatory domain to the -U regulatory domain using the controller CLI. This process cannot be performed using the controller GUI.

Step 1 To determine which access points in your network are eligible for migration, enter this command:

show ap migrate

Information similar to the following appears:

```
These 1 APs are eligible for migration:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9ap1240      "J"Reg. Domain

No APs have already been migrated.
```

Step 2 Enter these commands to disable the 802.11a and 802.11b/g networks:

config 802.11a disable network

config 802.11b disable network

Step 3 Enter this command to change the country code of the access points to be migrated to J3:

config country J3

Step 4 Wait for any access points that may have rebooted to rejoin the controller.

Step 5 Enter this command to migrate the access points from the -J regulatory domain to the -U regulatory domain:

config 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: migrateapj52w52@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 Enter this command to verify migration for all access points:

show ap migrate

Information similar to the following appears:

```
No APs are eligible for migration.

These 1 APs have already been migrated:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9ap1240      "U"Reg. Domain
```

Step 9 Enter these commands to re-enable the 802.11a and 802.11b/g networks:

config 802.11a enable network

config 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 migrateapj52w52@cisco.com. We recommend that you cut and paste the output from the **show ap migrate** command in Step 8 into this 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):

Channel	Frequency (MHz)	Maximum Power for AIR-LAP1132AG-Q-K9	Maximum Power for AIR-LAP1242AG-Q-K9
100	5500	17	15
104	5520	17	15
108	5540	17	15
112	5560	17	15
116	5580	17	15
120	5600	17	15
124	5620	17	15
128	5640	17	15
132	5660	17	15
136	5680	17	15
140	5700	17	15

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 7-2, 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 you selected. If there is radar activity on the channel you selected, the controller automatically selects a different channel, and after 30 minutes, the access point retries the channel you selected.

Note After radar has been detected on a DFS-enabled channel, it cannot be used for 30 minutes.

Note Rogue Location Detection Protocol (RLDP) and rogue containment are not supported on the channels listed in Table 7-2.

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 7-2 DFS-Enabled 5-GHz Channels

52 (5260 MHz)	104 (5520 MHz)	124 (5620 MHz)
56 (5280 MHz)	108 (5540 MHz)	128 (5640 MHz)
60 (5300 MHz)	112 (5560 MHz)	132 (5660 MHz)
64 (5320 MHz)	116 (5580 MHz)	136 (5680 MHz)
100 (5500 MHz)	120 (5600 MHz)	140 (5700 MHz)

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 7-2, 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

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).

You can use the controller GUI or CLI to configure the access point for monitor mode and to then enable tracking optimization on the access point radio.

Using the GUI to Optimize RFID Tracking on Access Points

Using the controller GUI, follow these steps to optimize RFID tracking.

Step 1 Click **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 for page appears.

Step 3 From the AP Mode drop-down box, choose **Monitor**.

Step 4 Click **Apply** to commit your changes.

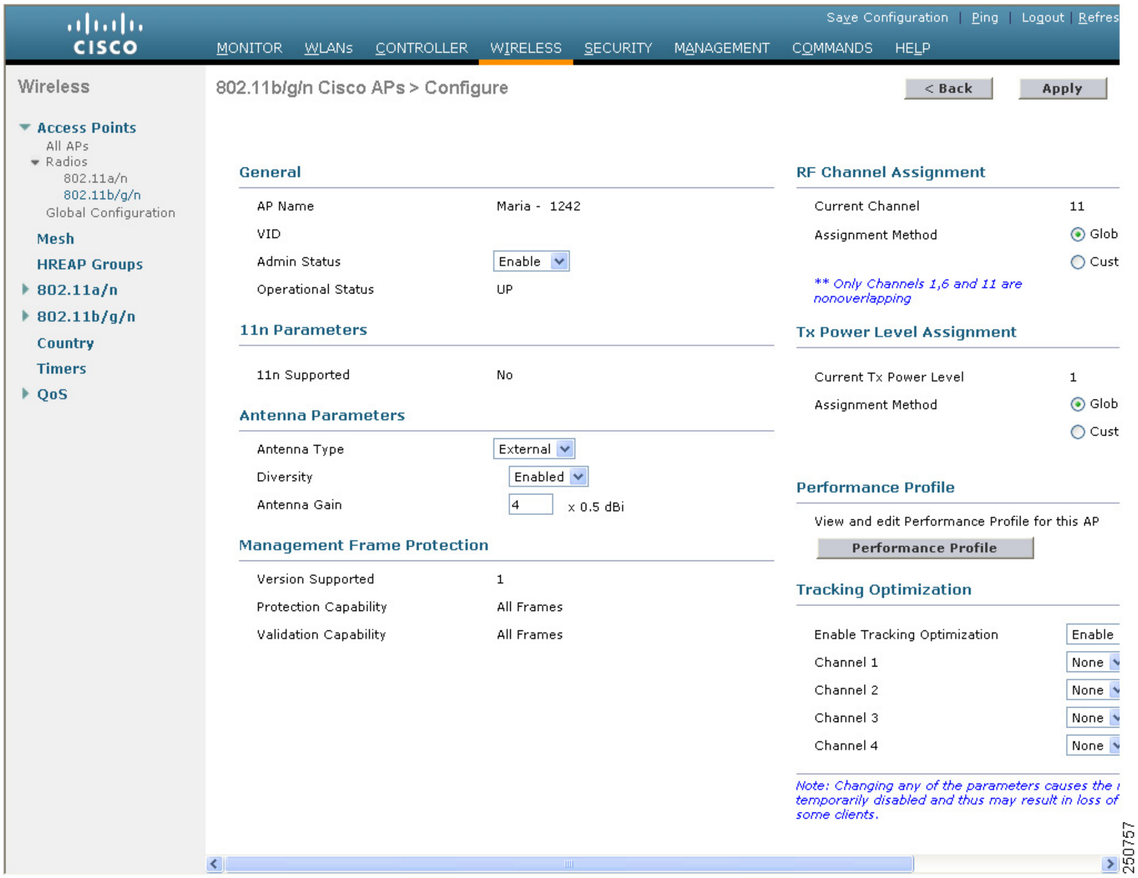
Step 5 Click **OK** when warned that the access point will be rebooted.

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

Step 7 Click **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 (see Figure 7-20).

Figure 7-20 802.11b/g/n Cisco APs > Configure Page



802.11b/g/n Cisco APs > Configure

General

AP Name	Maria - 1242
VID	
Admin Status	Enable
Operational Status	UP

11n Parameters

11n Supported	No

Antenna Parameters

Antenna Type	External
Diversity	Enabled
Antenna Gain	4 x 0.5 dBi

Management Frame Protection

Version Supported	1
Protection Capability	All Frames
Validation Capability	All Frames

RF Channel Assignment

Current Channel	11
Assignment Method	● Glob ○ Cust

** Only Channels 1,6 and 11 are nonoverlapping

Tx Power Level Assignment

Current Tx Power Level	1
Assignment Method	● Glob ○ Cust

Performance Profile

View and edit Performance Profile for this AP

Tracking Optimization

Enable Tracking Optimization	Enable
Channel 1	None
Channel 2	None
Channel 3	None
Channel 4	None

Note: Changing any of the parameters causes the temporarily disabled and thus may result in loss of some clients.

Step 9 To disable the access point radio, choose **Disable** from the Admin Status drop-down box and click **Apply**.

Step 10 To enable tracking optimization on the radio, choose **Enable** from the Enable Tracking Optimization drop-down box.

Step 11 From the four Channel drop-down boxes, 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 re-enable the access point radio, choose **Enable** from the Admin Status drop-down box and click **Apply**.

Step 15 Click **Save Configuration** to save your changes.

Using the CLI to Optimize RFID Tracking on Access Points

Using the controller CLI, follow these steps to optimize RFID tracking.

Step 1 To configure an access point for monitor mode, enter 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 To save your changes, enter this command:

save config

Step 4 To disable the access point radio, enter this command:

config 802.11b disable *Cisco_AP*

Step 5 To configure the access point to scan only the DCA channels supported by its country of operation, enter this command:

config ap monitor-mode tracking-opt *Cisco_AP*

Note To specify the exact channels to be scanned, enter this command and the command in Step 6.

Note To disable tracking optimization for this access point, enter this command: **config ap monitor-mode no-optimization** *Cisco_AP*.

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 To re-enable the access point radio, enter this command:

config 802.11b enable *Cisco_AP*

Step 8 To save your changes, enter this command:

save config

Step 9 To see a summary of all access points in monitor mode, enter 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    Tracking        1, 6, NA, NA
```

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 location accuracy.

Using the controller CLI, follow these steps to configure probe request filtering and rate limiting.

Step 1 To enable or disable the filtering of probe requests forwarded from an access point to the controller, enter this command:

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 To limit the number of probe requests sent to the controller per client per access point radio in a given interval, enter this command:

config advanced probe limit *num_probes interval*

- *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 To save your changes, enter this command:

save config

Step 4 To view the probe request forwarding configuration, enter this command:

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

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

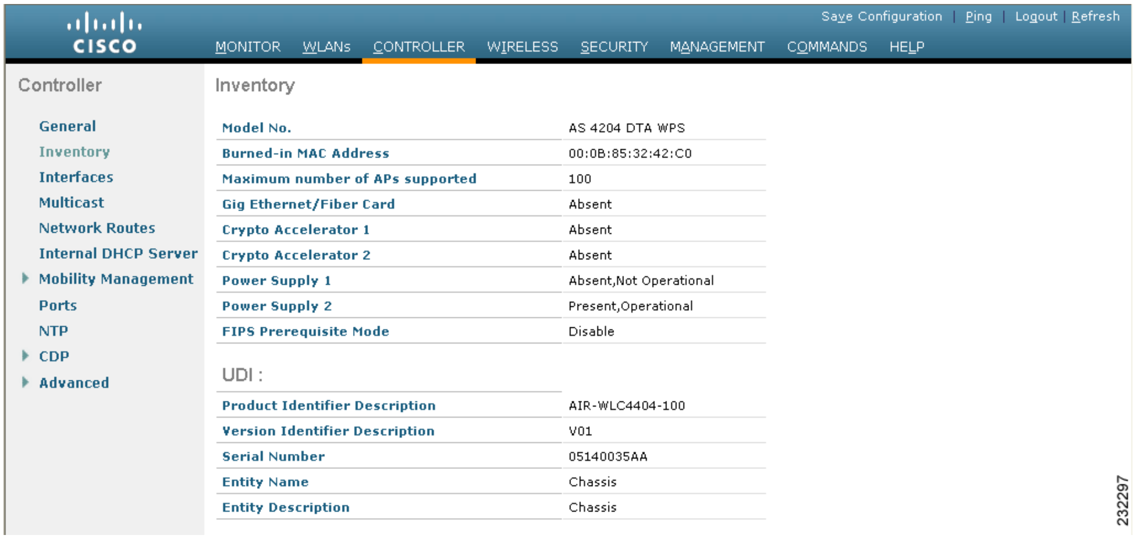
The UDI is burned into the EEPROM of controllers and lightweight access points at the factory. It can be retrieved through either the GUI or the CLI.

Using the GUI to Retrieve the Unique Device Identifier on Controllers and Access Points

Follow these steps to retrieve the UDI on controllers and access points using the GUI.

Step 1 Click **Controller** > **Inventory** to open the Inventory page (see Figure 7-21).

Figure 7-21 Inventory Page



Inventory

Model No.	AS 4204 DTA WPS
Burned-in MAC Address	00:0B:85:32:42:C0
Maximum number of APs supported	100
Gig Ethernet/Fiber Card	Absent
Crypto Accelerator 1	Absent
Crypto Accelerator 2	Absent
Power Supply 1	Absent,Not Operational
Power Supply 2	Present,Operational
FIPS Prerequisite Mode	Disable

UDI :

Product Identifier Description	AIR-WLC4404-100
Version Identifier Description	V01
Serial Number	05140035AA
Entity Name	Chassis
Entity Description	Chassis

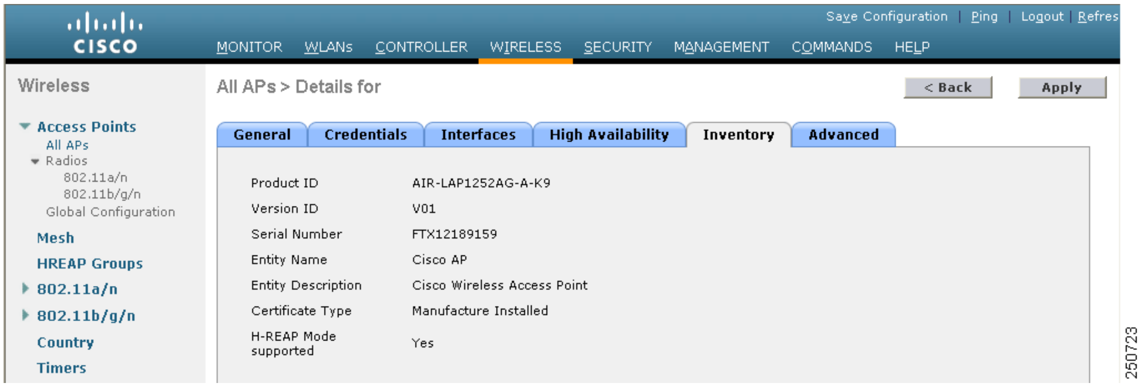
This page shows the five data elements of the controller UDI.

Step 2 Click **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 3 Click the name of the desired access point.

Step 4 Click the **Inventory** tab to open the All APs > Details for (Inventory) page (see Figure 7-22).

Figure 7-22 All APs > Details for (Inventory) Page



Product ID AIR-LAP1252AG-A-K9
Version ID V01
Serial Number FTX12189159
Entity Name Cisco AP
Entity Description Cisco Wireless Access Point
Certificate Type Manufacture Installed
H-REAP Mode supported Yes

This page shows the inventory information for the access point.

Using the CLI to Retrieve the Unique Device Identifier on Controllers and Access Points

Enter these commands to retrieve the UDI on controllers and access points using the CLI:

- **show inventory**—Shows the UDI string of the controller. Information similar to the following appears:

```
NAME: "Chassis"    , DESCR: "Cisco Wireless Controller"
PID: WS-C3750G-24PS-W24,  VID: V01,  SN: FLS0952H00F
```

- **show inventory ap** *ap_id*—Shows the UDI string of the access point specified.

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 fields 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 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), etc.] 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. Therefore, 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 6-39 for more information on CCX.

Note CCX is not supported on the AP1030.

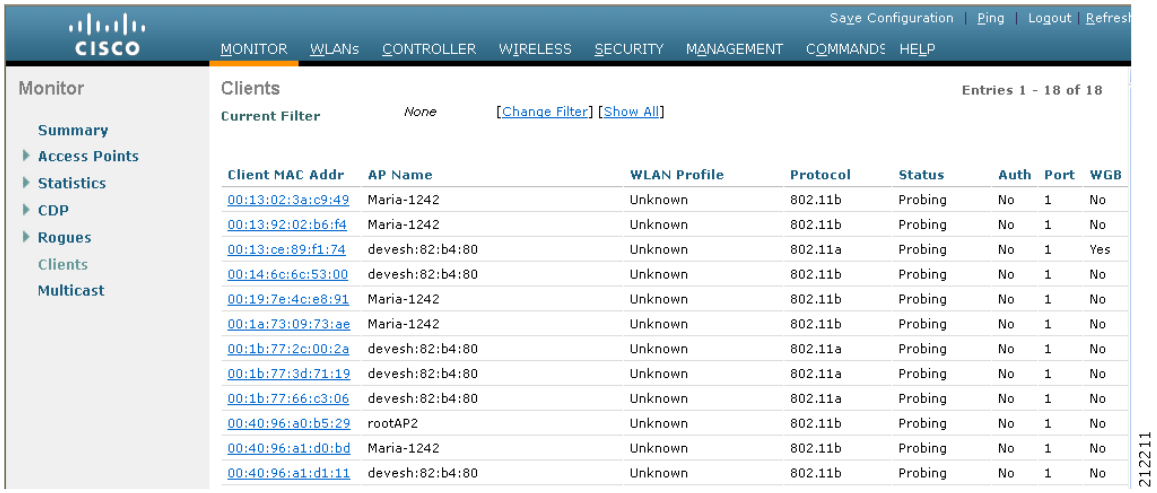
Follow the instructions in this section to perform a link test using either the GUI or the CLI.

Using the GUI to Perform a Link Test

Follow these steps to run a link test using the GUI.

Step 1 Click **Monitor** > **Clients** to open the Clients page (see Figure 7-23).

Figure 7-23 Clients Page


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Access Points
Statistics
CDP
Rogues
Clients
Multicast
212211

Clients

Entries 1 - 18 of 18

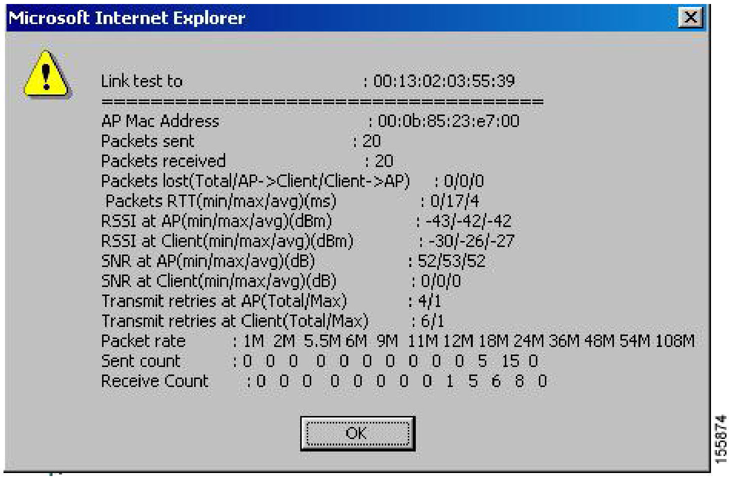
Current Filter None [Change Filter] [Show All]

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:13:02:3a:c9:49	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:13:92:02:b6:f4	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:13:ce:89:f1:74	devesh:82:b4:80	Unknown	802.11a	Probing	No	1	Yes
00:14:6c:6c:53:00	devesh:82:b4:80	Unknown	802.11b	Probing	No	1	No
00:19:7e:4c:e8:91	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:1a:73:09:73:ae	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:1b:77:2c:00:2a	devesh:82:b4:80	Unknown	802.11a	Probing	No	1	No
00:1b:77:3d:71:19	devesh:82:b4:80	Unknown	802.11a	Probing	No	1	No
00:1b:77:66:c3:06	devesh:82:b4:80	Unknown	802.11a	Probing	No	1	No
00:40:96:a0:b5:29	rootAP2	Unknown	802.11b	Probing	No	1	No
00:40:96:a1:d0:bd	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:40:96:a1:d1:11	devesh:82:b4:80	Unknown	802.11b	Probing	No	1	No

Step 2 Hover your cursor over the blue drop-down arrow for the desired client and choose **LinkTest**. A link test page appears (see Figure 7-24).

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 7-24 Link Test Page



```
Link test to                              : 00:13:02:03:55:39
====================================================
AP Mac Address                            : 00:0b:85:23:e7:00
Packets sent                            : 20
Packets received                          : 20
Packets lost(Total/AP->Client/Client->AP)     : 0/0/0
 Packets RTT(min/max/avg)(ms)                 : 0/17/4
RSSI at AP(min/max/avg)(dBm)                  : -43/-42/-42
RSSI at Client(min/max/avg)(dBm)              : -30/-26/-27
SNR at AP(min/max/avg)(dB)                   : 52/53/52
SNR at Client(min/max/avg)(dB)                : 0/0/0
Transmit retries at AP(Total/Max)             : 4/1
Transmit retries at Client(Total/Max)         : 6/1
Packet rate        : 1M  2M  5.5M 6M  9M  11M 12M 18M 24M 36M 48M 54M 108M
Sent count         : 0   0   0    0   0   0   0   0   0   0   5   15  0
Receive Count        : 0   0   0    0   0   0   0   0   1   5   6   8   0
```

This page shows the results of the CCX link test.

Note If the client and/or controller does not support CCX v4 or later, the controller performs a ping link test on the client instead, and a much more limited link test page appears.

Step 3 Click **OK** to exit the link test page.

Using the CLI to Perform a Link Test

Use these commands to run a link test using the CLI.

1. To run a link test, enter this command:

   linktest *ap_mac*

   When CCX v4 or later 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
     Transmit rate:  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
     Transmit rate:  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    8     0
```

   When CCX v4 or later 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
```

2. To adjust the link-test parameters that are applicable to both the CCX link test and the ping test, enter these commands from config mode:

   config > **linktest frame-size** *size_of_link-test_frames*

   config > **linktest num-of-frame** *number_of_link-test_request_frames_per_test*

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 hybrid-REAP access points, for which the link could be a slow or unreliable WAN connection.

Note Link latency is supported for use only with hybrid-REAP access points in connected mode. Hybrid-REAP 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 network link speed and controller processing loads. The access point timestamps the outgoing echo requests to the controller and the echo requests 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.

You can configure link latency for a specific access point using the controller GUI or CLI or for all access points joined to the controller using the CLI.

Using the GUI to Configure Link Latency

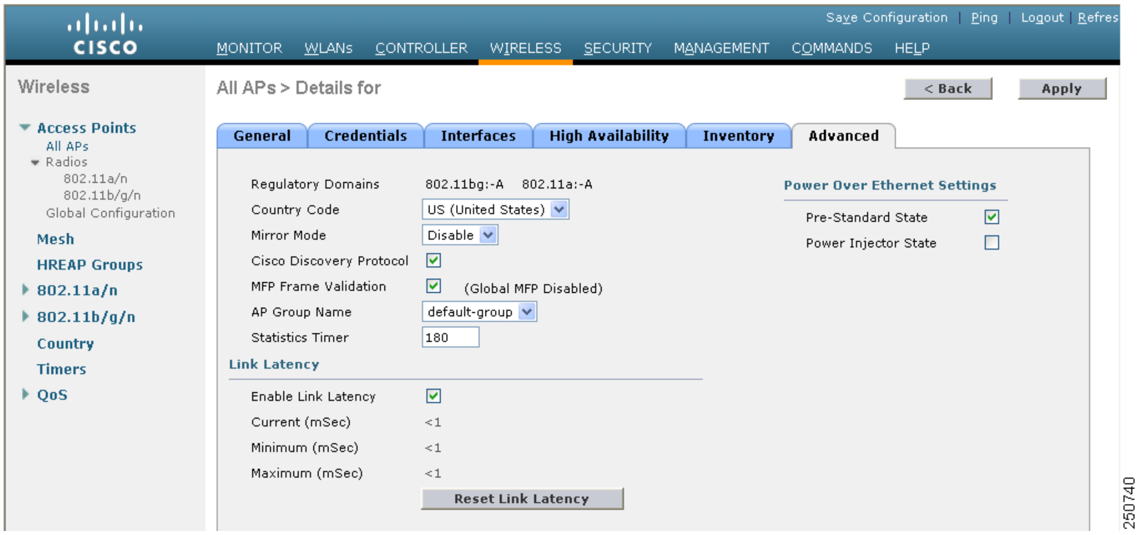
Using the controller GUI, follow these steps to configure link latency.

Step 1 Click **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 Click the **Advanced** tab to open the All APs > Details for (Advanced) page (see Figure 7-25).

Figure 7-25 All APs > Details for (Advanced) Page



All APs > Details for

Regulatory Domains 802.11bg:-A 802.11a:-A
Country Code US (United States)
Mirror Mode Disable
Cisco Discovery Protocol ☑
MFP Frame Validation ☑ (Global MFP Disabled)
AP Group Name default-group
Statistics Timer 180

Link Latency
Enable Link Latency ☑
Current (mSec) <1
Minimum (mSec) <1
Maximum (mSec) <1

Power Over Ethernet Settings
Pre-Standard State ☑
Power Injector State □

Step 4 Check the **Enable Link Latency** check box to enable link latency for this access point or uncheck 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 unchecked.

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, click the **Advanced** tab again. The link latency results appear below the Enable Link Latency check box:

- **Current**—The current round-trip time (in milliseconds) of CAPWAP heartbeat 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 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 from the access point to the controller and back.

Step 9 To clear the current, minimum, and maximum link 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, click the **Advanced** tab. The updated statistics appear in the Minimum and Maximum fields.

Using the CLI to Configure Link Latency

Using the controller CLI, follow these steps to configure link latency.

Step 1 To enable or disable link latency for a specific access point or for all access points currently associated to the controller, enter this command:

config ap link-latency {**enable** | **disable**} {*Cisco_AP* | **all**}

The default value is disabled.

Note The **config 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 To view the link latency results for a specific access point, enter this command:

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 To clear the current, minimum, and maximum link latency statistics on the controller for a specific access point, enter this command:

config ap link-latency reset *Cisco_AP*

Step 4 To view the results of the reset, enter this command:

show ap config general *Cisco_AP*

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.

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 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, refer to this URL:
http://www.cisco.com/en/US/prod/switches/epoe.html

Table 7-3 shows the maximum transmit power settings for 1250 series access points using PoE.

Table 7-3 Maximum Transmit Power Settings for 1250 Series Access Points Using PoE

Radio Band	Data Rates	Number of Transmitters	Cyclic Shift Diversity (CSD)	Maximum Transmit Power (dBm)[1]		
				802.3af Mode (15.4 W)	ePoE Power Optimized Mode (16.8 W)	ePoE Mode (20 W)
2.4 GHz	802.11b	1	—	20	20	20
	802.11g	1	—	17	17	17
	802.11n MCS 0-7	1	Disabled	17	17	17
		2	Enabled (default)	Disabled	14 (11 per Tx)	20 (17 per Tx)
	802.11n MCS 8-15	2	—	Disabled	14 (11 per Tx)	20 (17 per Tx)
5 GHz	802.11a	1	—	17	17	17
	802.11n MCS 0-7	1	Disabled	17	17	17
		2	Enabled (default)	Disabled	20 (17 per Tx)	20 (17 per Tx)
	802.11n MCS 8-15	2	—	Disabled	20 (17 per Tx)	20 (17 per Tx)

[1] Maximum transmit power varies by channel and according to individual country regulations. Refer to the product documentation for specific details.

Note 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.

You can configure PoE through either the controller GUI or CLI.

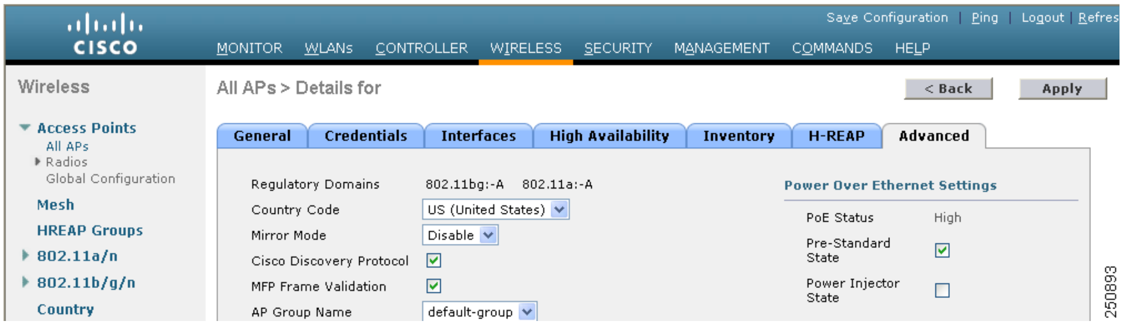
Using the GUI to Configure Power over Ethernet

Using the controller GUI, follow these steps to configure PoE.

Step 1 Click **Wireless > Access Points > All APs** and then the name of the desired access point.

Step 2 Click the **Advanced** tab to open the All APs > Details for (Advanced) page (see Figure 7-26).

Figure 7-26 All APs > Details for (Advanced) Page


Save Configuration | Ping | Logout | Refres
cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Wireless
Access Points
All APs
Radios
Global Configuration
Mesh
HREAP Groups
802.11a/n
802.11b/g/n
Country
< Back
Apply
General Credentials Interfaces High Availability Inventory H-REAP Advanced
250893

All APs > Details for

Regulatory Domains 802.11bg:-A 802.11a:-A
Country Code US (United States)
Mirror Mode Disable
Cisco Discovery Protocol ☑
MFP Frame Validation ☑
AP Group Name default-group

Power Over Ethernet Settings
PoE Status High
Pre-Standard State ☑
Power Injector State □

The PoE Status field shows the power level at which the access point is operating: High (20 W), Medium (16.8 W), or Medium (15.4 W). This field is not configurable. The controller auto-detects the access point's power source and displays the power level here.

Note This field 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:

- Check the **Pre-Standard State** check box if the access point is being powered by a high-power Cisco switch. These switches provide more than the traditional 6 Watts of power but do not support the intelligent power management (IPM) feature. These switches include:
  - 2106 controller,
  - WS-C3550, WS-C3560, WS-C3750,
  - C1880,
  - 2600, 2610, 2611, 2621, 2650, 2651,
  - 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691,
  - 2811, 2821, 2851,
  - 3620, 3631-telco, 3640, 3660,
  - 3725, 3745,
  - 3825, and 3845.
- Uncheck the **Pre-Standard State** check box if power is being provided by a power injector or by a switch not on the above list.

Step 4 Check 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 check this check box.

Step 5 If you checked 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 box 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 field. If you want the access point to find the switch MAC address, leave the Injector Switch MAC Address field blank.

  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. It is acceptable to use this option if your network does not contain any older Cisco 6-Watt switches that could be overloaded if connected directly to a 12-Watt 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-Watt switch, an overload occurs.

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

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

Using the CLI to Configure Power over Ethernet

Using the controller CLI, enter these commands to configure and view PoE settings.

- If your network contains any older Cisco 6-Watt switches that could be accidentally overloaded if connected directly to a 12-Watt 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 issuing this command. Otherwise, this command will fail. See the "Configuring Cisco Discovery Protocol" section on page 4-69 for information on enabling CDP.

- To remove the safety checks and allow the access point to be connected to any switch port, enter this command:

  config ap power injector enable {*Cisco_AP* | **all**} **override**

  It is acceptable to use this command if your network does not contain any older Cisco 6-Watt switches that could be overloaded if connected directly to a 12-Watt 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 wish to automatically detect it using the installed option, enter this command:

  config ap power injector enable {*Cisco_AP* | **all**} *switch_port_mac_address*

- To view the PoE settings for a specific access point, enter 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 field shows "degraded mode" if the access point is not operating at full power.

- To view the controller's trap log, enter this command:

  show traplog

  If the access point is not operating at full power, the trap contains "PoE Status: degraded operation."

Configuring Flashing LEDs

Controller software release 4.0 or later enables you to flash the LEDs on an access point in order to locate it. All IOS lightweight access points support this feature.

Use these commands to configure LED flashing from the Privileged Exec mode of the controller.

Note The output of these commands is sent only to the controller console, regardless of whether the commands were issued on the console or in a TELNET/SSH CLI session.

1. To enable the controller to send commands to the access point from its CLI, enter this command:

   debug ap enable *Cisco_AP*

2. To cause a specific access point to flash its LEDs for a specified number of seconds, enter this command:

   debug ap command "led flash *seconds***"** *Cisco_AP*

   You can enter a value between 1 and 3600 seconds for the *seconds* parameter.

3. To disable LED flashing for a specific access point, enter 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

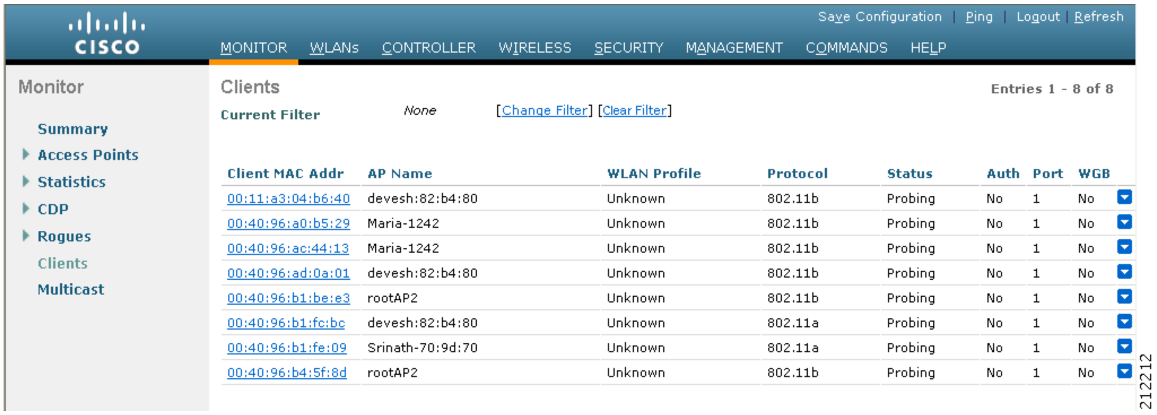
You can use the controller GUI or CLI to view information about the clients that are associated to the controller's access points.

Using the GUI to View Clients

Using the GUI, follow these steps to view client information.

Step 1 Click **Monitor > Clients** to open the Clients page (see Figure 7-27).

Figure 7-27 Clients Page



Clients

Entries 1 - 8 of 8

Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:11:a3:04:b6:40	devesh:82:b4:80	Unknown	802.11b	Probing	No	1	No
00:40:96:a0:b5:29	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:40:96:ac:44:13	Maria-1242	Unknown	802.11b	Probing	No	1	No
00:40:96:ad:0a:01	devesh:82:b4:80	Unknown	802.11b	Probing	No	1	No
00:40:96:b1:be:e3	rootAP2	Unknown	802.11b	Probing	No	1	No
00:40:96:b1:fc:bc	devesh:82:b4:80	Unknown	802.11a	Probing	No	1	No
00:40:96:b1:fe:09	Srinath-70:9d:70	Unknown	802.11a	Probing	No	1	No
00:40:96:b4:5f:8d	rootAP2	Unknown	802.11b	Probing	No	1	No

This page lists all of the clients that are associated to the controller's access points. It provides the following information for each client:

- 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 802.11n(5). If the 802.11n client associates to an 802.11b/g radio with 802.11n enabled, then the client type shows as 802.11n (2.4).

- 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

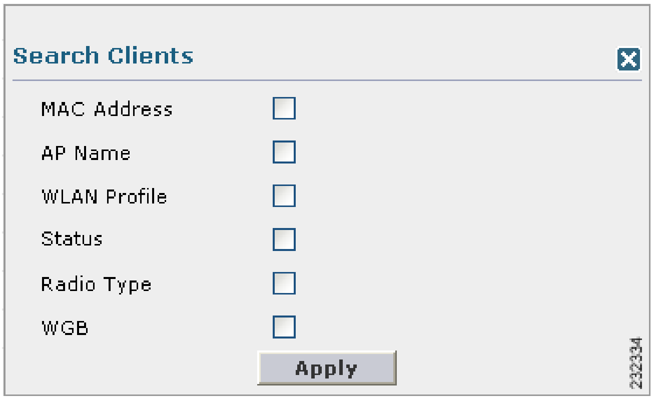
Note Refer to the "Cisco Workgroup Bridges" section on page 7-34 for more information on the WGB status.

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 To create a filter to display only clients that meet certain criteria (such as MAC address, status, or radio type), follow these steps:

a. Click **Change Filter** to open the Search Clients page (see Figure 7-28).

Figure 7-28 Search Clients Page


Search Clients

MAC Address □
AP Name □
WLAN Profile □
Status □
Radio Type □
WGB □

b. Check 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.

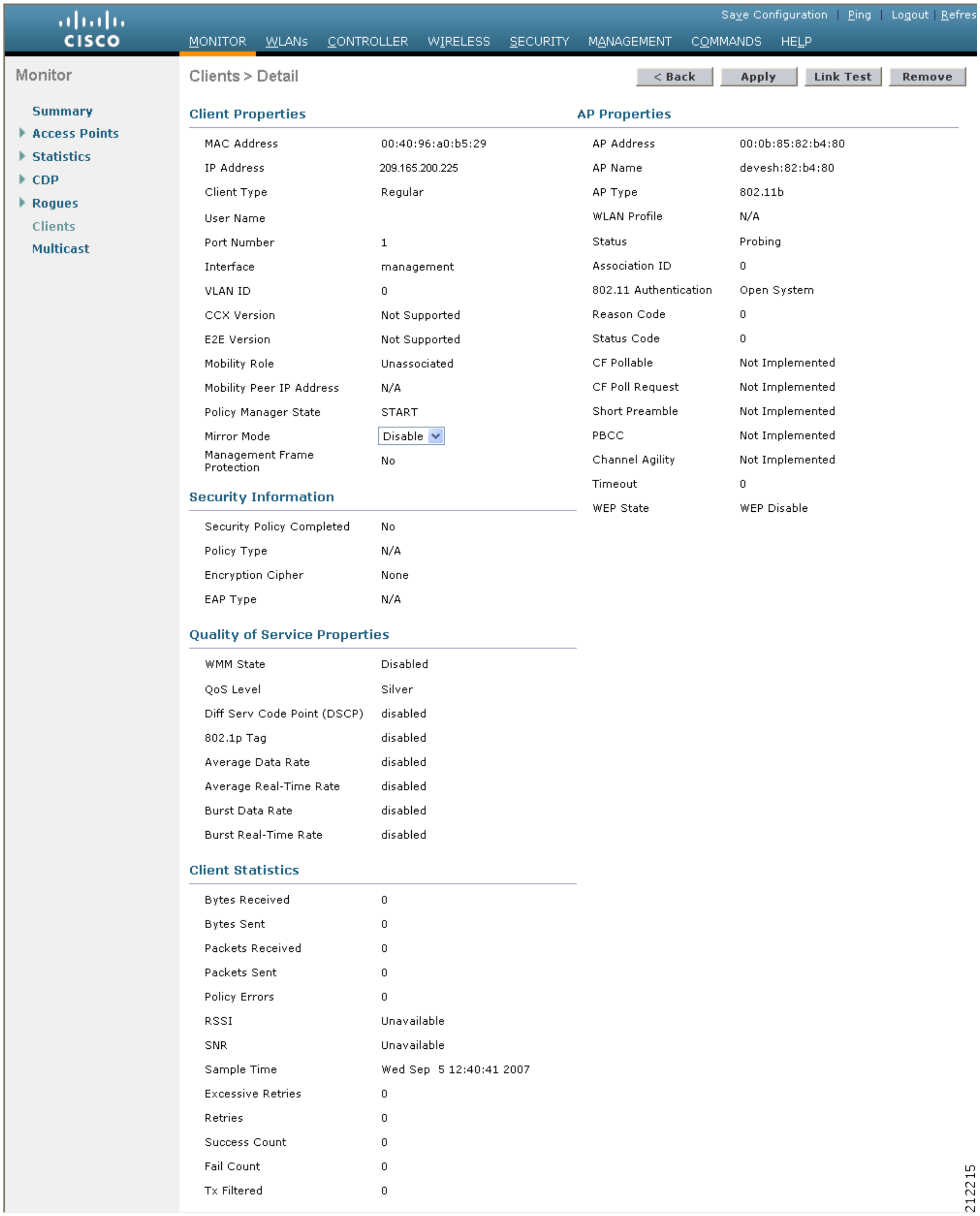
- **AP Name**—Enter the name of an access point.
- **WLAN Profile**—Enter the name of a WLAN.
- **Status**—Check the **Associated**, **Authenticated**, **Excluded**, **Idle**, and/or **Probing** check boxes.
- **Radio Type**—Choose **802.11a**, **802.11b**, **802.11g**, **802.11n**, or **Mobile**.
- **WGB**—Shows 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 **Show All**.

Step 3 To view detailed information for a specific client, click the MAC address of the client. The Clients > Detail page appears (see Figure 7-29).

Figure 7-29 Clients > Detail Page



Clients > Detail

Client Properties

MAC Address	00:40:96:a0:b5:29
IP Address	209.165.200.225
Client Type	Regular
User Name	
Port Number	1
Interface	management
VLAN ID	0
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Unassociated
Mobility Peer IP Address	N/A
Policy Manager State	START
Mirror Mode	Disable
Management Frame Protection	No

AP Properties

AP Address	00:0b:85:82:b4:80
AP Name	devesh:82:b4:80
AP Type	802.11b
WLAN Profile	N/A
Status	Probing
Association ID	0
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Disable

Security Information

Security Policy Completed	No
Policy Type	N/A
Encryption Cipher	None
EAP Type	N/A

Quality of Service Properties

WMM State	Disabled
QoS Level	Silver
Diff Serv Code Point (DSCP)	disabled
802.1p Tag	disabled
Average Data Rate	disabled
Average Real-Time Rate	disabled
Burst Data Rate	disabled
Burst Real-Time Rate	disabled

Client Statistics

Bytes Received	0
Bytes Sent	0
Packets Received	0
Packets Sent	0
Policy Errors	0
RSSI	Unavailable
SNR	Unavailable
Sample Time	Wed Sep 5 12:40:41 2007
Excessive Retries	0
Retries	0
Success Count	0
Fail Count	0
Tx Filtered	0

This page shows the following information:

- The general properties of the client
- The security settings of the client
- The QoS properties of the client
- Client statistics
- The properties of the access point to which the client is associated

Using the CLI to View Clients

Use these CLI commands to view client information.

- To see the clients associated to a specific access point, enter this command:

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

  Information similar to the following appears:

```
MAC Address        AP Id   Status         WLAN Id Authenticated
-----------------  ------  -------------  ---------  -------------
00:13:ce:cc:8e:b8   1     Associated      1          No
```

- To see a summary of the clients associated to the controller’s access points, enter this command:

  show client summary

  Information similar to the following appears:

```
Number of Clients................................ 6

MAC Address       AP Name           Status        WLAN Auth Protocol Port Wired
----------------- ----------------- ------------- ---- ---- -------- ---- -----

00:13:ce:cc:8e:b8 Maria-1242        Probing       N/A  No   802.11a 1    No
00:40:96:a9:a0:a9 CJ-AP1            Probing       N/A  No   802.11a 1    No
00:40:96:ac:44:13 CJ-AP1            Probing       N/A  No   802.11a 1    No
00:40:96:b1:fe:06 CJ-AP1            Probing       N/A  No   802.11a 1    No
00:40:96:b1:fe:09 CJ-AP1          Probing     N/A  No   802.11a 1    No
```

- To see detailed information for a specific client, enter 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
...
```

CHAPTER 8

Controlling Mesh Access Points

This chapter describes Cisco indoor and outdoor mesh access points and explains how to connect them to the controller and manage access point settings. It contains these sections:

- Cisco Aironet Mesh Access Points, page 8-2
- Architecture Overview, page 8-6
- Adding Mesh Access Points to the Mesh Network, page 8-10
- Configuring Advanced Features, page 8-32
- Viewing Mesh Statistics and Reports, page 8-39
- Converting Indoor Access Points to Mesh Access Points (1130AG, 1240AG), page 8-48
- Changing MAP and RAP Roles for Indoor Mesh Access Points (1130AG, 1240AG), page 8-49
- Converting Indoor Mesh Access Points to Non-Mesh Lightweight Access Points (1130AG, 1240AG), page 8-50
- Configuring Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers, page 8-51

Cisco Aironet Mesh Access Points

Controller software release 5.2 supports these Cisco Aironet mesh access points:

- Cisco Aironet 1520 series outdoor mesh access points
  - Cisco 1520 Series consists of the 1522 dual-radio mesh access point and the 1524 multi-radio mesh access point.

Note Refer to the *Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide* for details on the physical installation and initial configuration of the mesh access points at the following link:
http://www.cisco.com/en/US/products/ps8368/tsd_products_support_series_home.html

- Cisco Aironet 1130AG and 1240AG series indoor mesh access points

Note AP1130 and AP1240 must be converted to operate as indoor mesh access points. Refer to the "Converting Indoor Access Points to Mesh Access Points (1130AG, 1240AG)" section on page 8-48.

Note All features discussed in this chapter apply to indoor (1130, 1240) and outdoor mesh access points (1522, 1524) unless noted otherwise. *Mesh access point* or *MAP* is hereafter used to address both indoor and outdoor mesh access points.

Note Cisco Aironet 1505 and 1510 access points are not supported in this release.

Note Refer to the *Release Notes for Cisco Wireless LAN Controllers and Mesh Access Points for Release 5.2.x* for mesh feature summary, operating notes and software upgrade steps for migrating from 4.1.19x.xx mesh releases to controller release 5.2 at:
http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html.

Access Point Roles

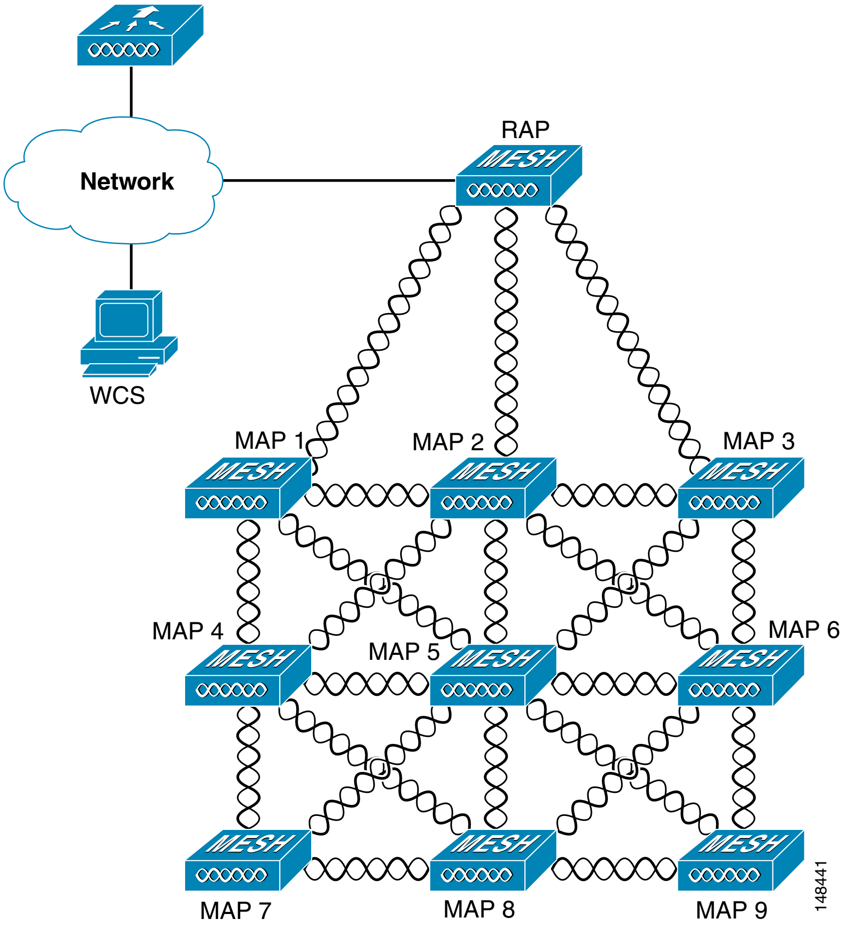
Access points within a mesh network operate as either a root access point (RAP) or a mesh access point (MAP).

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 8-1 shows the relationship between RAPs and MAPs in a mesh network.

Figure 8-1 Simple Mesh Network Hierarchy



Network Access

Wireless mesh networks can simultaneously carry two different traffic types: 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:

- MAC authentication–Mesh access points are added to a reference-able database to ensure they are allowed access to a given controller and the mesh network. Refer to "Adding Mesh Access Points to the Mesh Network" section on page 8-10.
- External RADIUS authentication–Mesh access points can be externally authorized and using a RADIUS server such as Cisco ACS (4.1 and later) that supports the client authentication type of EAP-FAST with certificates. Refer to the "Configuring RADIUS Servers" section on page 8-14.

Network Segmentation

Membership to the wireless LAN mesh network for mesh access points is controlled by:

- Bridge group name–Mesh access points can be placed in like bridge groups to manage membership or provide network segmentation. Refer to "Using the GUI to Configure Antenna Gain" section on page 8-22.

Deployment Modes

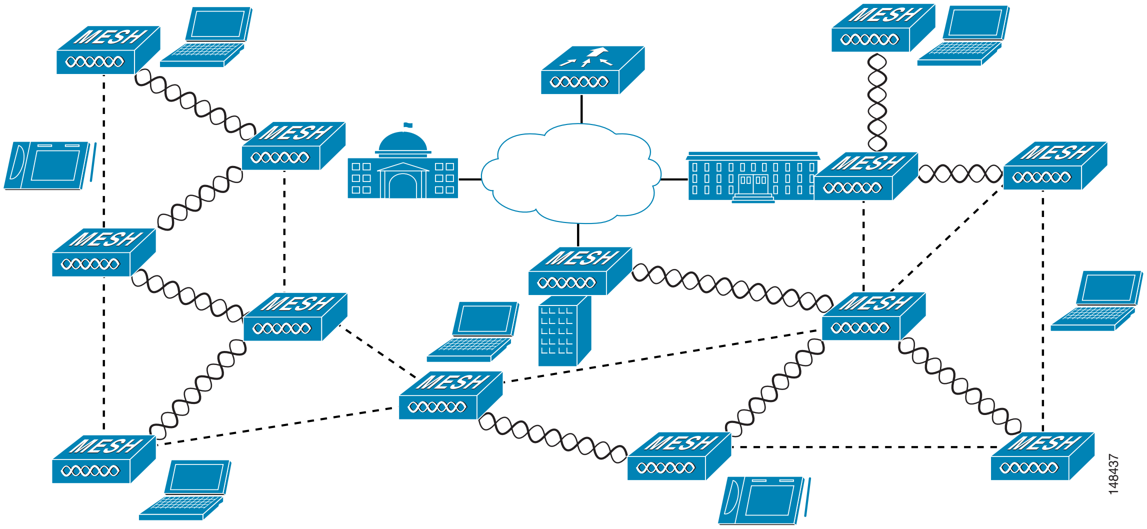
Mesh access points support multiple deployment modes, including the following:

- Wireless mesh
- WLAN backhaul
- Point-to-multipoint wireless bridging
- Point-to-point wireless bridging

Cisco Wireless Mesh Network

In a Cisco wireless outdoor mesh network, multiple mesh access points comprise a network that provides secure, scalable outdoor wireless LANs. Figure 8-2 shows an example mesh deployment.

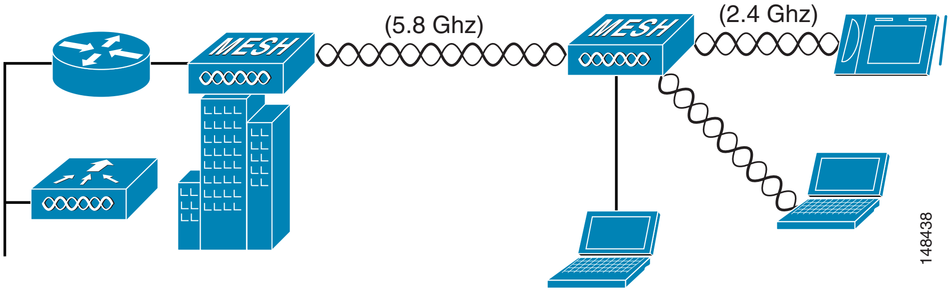
Figure 8-2 Wireless Mesh Deployment



Wireless Backhaul

Mesh access points can provide a simple wireless backhaul solution, which provides 802.11b/g services to wireless LAN and wired clients. This configuration is basically a wireless mesh with one MAP. Figure 8-3 shows an example of this deployment type.

Figure 8-3 Wireless Backhaul Deployment



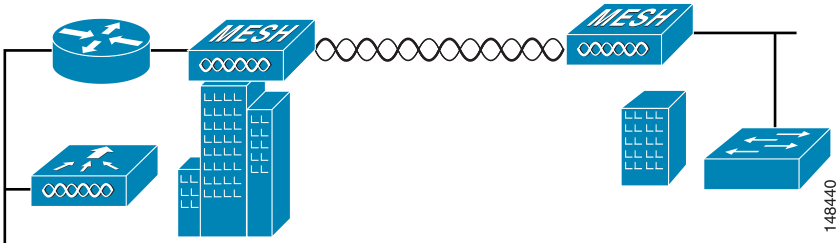
Point-to-Point Wireless Bridging

Mesh access points can support a point-to-point bridging application. In this deployment, mesh access points extend a Layer 2 network by using the backhaul radio to bridge two segments of a switched network (see Figure 8-4). This is fundamentally a wireless mesh network with one MAP and no wireless LAN clients.

Client access can 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, you must enable the bridging feature on the RAP and on all MAPs in that segment. Also 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. If improperly configured, it can take down your mesh deployment.

Figure 8-4 Wireless Point-to-Point Bridge Deployment

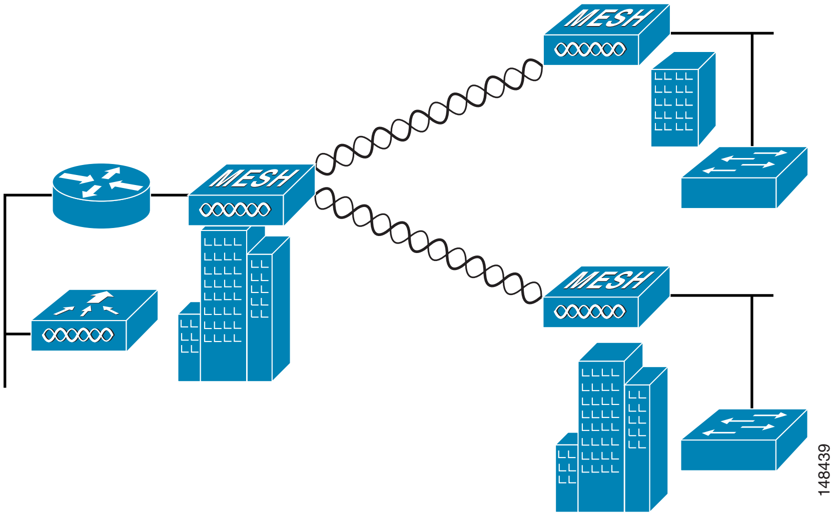


Point-to-Multipoint Wireless Bridging

Mesh access points support point-to-multipoint bridging applications. Specifically, a RAP acting as a root bridge connects to multiple MAPs as non-root bridges with their associated wired LANs. By default, bridging 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. Refer to the "Configuring Ethernet Bridging and Ethernet VLAN Tagging" section on page 8-25 for configuration details.

Figure 8-5 shows a simple point-to-multipoint deployment with one RAP and two MAPs. This configuration is fundamentally a wireless mesh network with no wireless LAN clients. Client access can be provided with Ethernet bridging enabled; however, if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access.

Figure 8-5 Wireless Point-to-Multipoint Bridge Deployment



Architecture Overview

CAPWAP

CAPWAP is the provisioning and control protocol used by the controller to manage access points (mesh and non-mesh) in the network. This protocol replaces LWAPP in controller software release 5.2.

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 link quality and the number of hops.

Ease of deployment, fast convergence, and minimal resource consumption are also key components of AWPP.

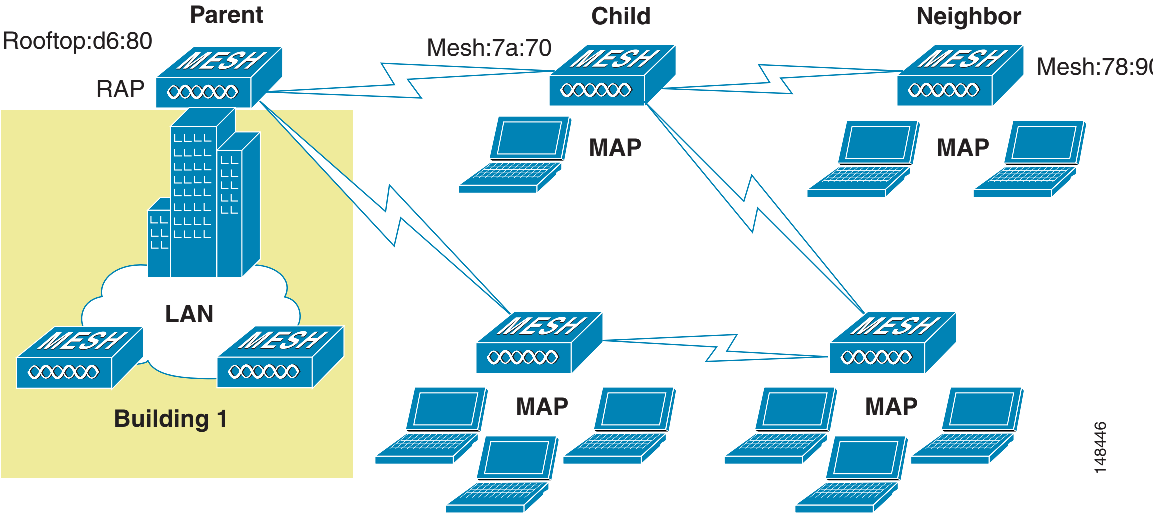
The goal of AWPP is to find the best path back to a RAP for each MAP that is part of the RAP's bridge group. To do this, the MAP actively solicits for neighbor MAPs. During the solicitation, the MAP learns all of the available neighbors back to a RAP, determines which neighbor offers the best path, and then synchronizes with that neighbor.

Mesh Neighbors, Parents, and Children

Relationships among access points with the mesh network are labelled as parent, child or neighbor (see Figure 8-6).

- A parent access point offers the best route back to the RAP based on its ease values. A parent can be either the RAP itself or another MAP.
  - Ease is calculated using the SNR and link hop value of each neighbor. Given multiple choices, generally an access point with a higher ease value is selected.
- A child access point selects the parent access point as its best route back to the RAP.
- A neighbor access point is within 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.

Figure 8-6 Parent, Child and Neighbor Access Points



Wireless Mesh Constraints

When designing and building a wireless mesh network here are a few system characteristics to consider. Some of these apply to the backhaul network design and others to the CAPWAP controller design:

- Recommended backhaul is 24 Mbps
  - 24 Mbps is chosen as the optimal backhaul rate because it aligns with the maximum coverage of the WLAN portion of the client WLAN of the MAP; that is, the distance between MAPs using 24 Mbps backhaul should allow for seamless WLAN client coverage between the MAPs.
  - A lower bit rate might allow a greater distance between mesh access points, 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 mesh access points or results in a reduced SNR between mesh access points, limiting mesh reliability and interconnection.
  - The wireless mesh backhaul bit rate is set on the controller.

Note The backhaul bit rate is set on the **Wireless > 802.11an > Network** page within the 802.11an global parameters section.

- The required minimum LinkSNR for backhaul links per data rate is shown in Table 8-1.

Table 8-1 Backhaul Data Rates and Minimum LinkSNR Requirements

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

- The required minimum LinkSNR is driven by the data rate and the following formula: Minimum SNR + fade margin. Table 8-2 summarizes the calculation by data rate.
  - Minimum SNR refers to an ideal state of non-interference, non-noise and a system packet error rate (PER) of no more than 10%
  - Typical fade margin is approximately 9 to 10 dB
  - We do not recommend using data rates greater than 24 Mbps in municipal mesh deployments as the SNR requirements do not make the distances practical

Table 8-2 Minimum Required LinkSNR Calculations by Data Rate

Date Rate	Minimum SNR (dB) +	Fade Margin =	Minimum Required LinkSNR (dB)
6	5	9	14
9	6	9	15
12	7	9	16
18	9	9	18
24	13	9	22
36	17	9	26

- Number of backhaul hops is limited to eight, but three to four is recommended

  The number of hops is recommended to be limited to three–four primarily to maintain sufficient backhaul throughput, because each mesh AP uses the same radio for transmission and reception of backhaul traffic. This 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 of how many MAPs per RAP you can configure. However, it is suggested that you limit this 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 (see Table 8-3).

Table 8-3 Mesh Access Point Support by Controller Model

Controller Model	Local AP Support (non-mesh)	Maximum Possible Mesh AP Support	RAPs	MAPs[1]	Total Mesh AP Support
4404	100	150	1	149	150
			50	100	150
			75	50	125
			100	0	100
2106	6	11[2]	1	10	11
			2	8	10
			3	6	9
			4	4	8
			5	2	7
			6	0	6
2112	12	12	1	11[3]	12
			3	9	12
			6	6	12
			9	3	12
			12	0	12
2125	25	25	1	24[3]	25
			5	20	25
			10	15	25
			15	10	25
			20	5	25
			25	0	25
WiSM	300	375	1	374	375
			100	275	375
			250	100	350
			300	0	300

[1] Number of MAPs supported on a mesh network is equal to the ((local AP support - number of RAPs) x 2). Local AP support is the total number of non-mesh APs supported on the controller model.

[2] For 2106 controllers, the mesh access point limit is equal to [(local AP support - 1) x 2) +1].

[3] For 2112 and 2125 controllers, the number of MAPs = (Total number of local APs - number of RAPs).

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 onwards.

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. Layer 3 mode is recommended for large deployments.

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

1. Add the MAC address of the MAP to the controller's MAC filter. Refer to "Adding MAC Addresses of Mesh Access Points to the Controller Filter List" section on page 8-10.
    a. To configure external authentication of MAC addresses using an external RADIUS server refer to "Configuring External Authentication and Authorization Using a RADIUS Server" section on page 8-13.
2. Configure the DCA channels for the mesh access points. Refer to the "Using the GUI to Configure Dynamic Channel Assignment" section on page 11-12 for details.
3. Define the role (RAP or MAP) for the mesh access point. Refer to the "Defining the Mesh Access Point Role" section on page 8-16.
4. Configure a primary, secondary, and tertiary controller for each MAP. Refer to the "Verifying that Access Points Join the Controller"and "Configuring Backup Controllers" sections in Chapter 7.
5. Configure global mesh parameters. Refer to "Configuring Global Mesh Parameters" section on page 8-16.
6. Configure bridging parameters. Refer to "Configuring Ethernet Bridging and Ethernet VLAN Tagging" section on page 8-25.
    a. Configure Bridge Group Names.
    b. Assign IP addresses to MAPs unless using DHCP.

       If using DHCP, configure Option 43 and Option 60. Refer to the *Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide.*
7. Configure mobility groups (if desired) and assign controllers. Refer to Chapter 12, "Configuring Mobility GroupsWireless Device Access."
8. Configure advanced features such as using voice and video in the network. Refer to "Configuring Advanced Features" section on page 8-32.

Adding MAC Addresses of Mesh Access Points to the Controller Filter List

You must enter the 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 addressed need be configured.

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

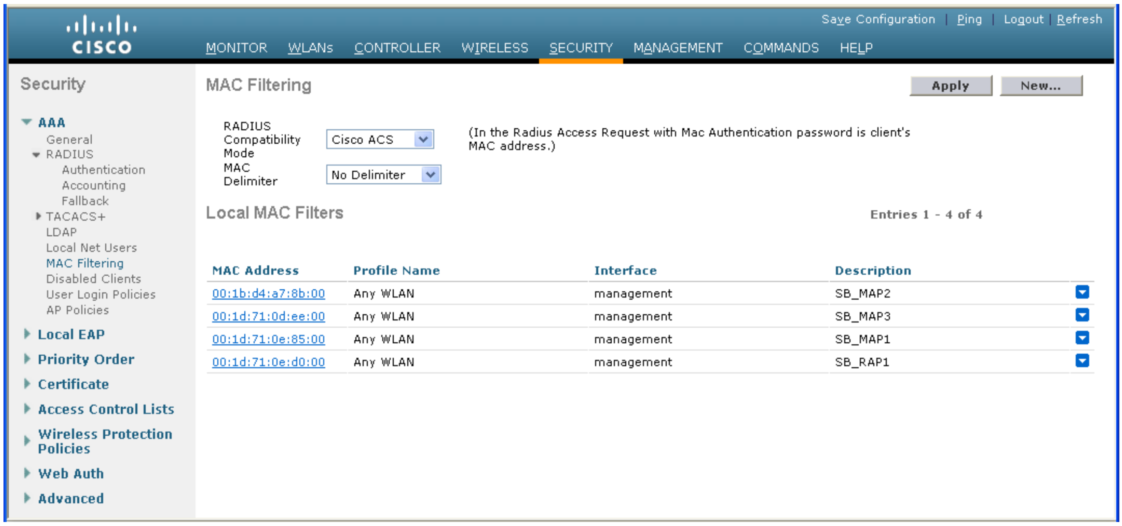
Note You can also download the list of access point MAC addresses and push them to the controller using the Cisco Wireless Control System (WCS). Refer to the *Cisco Wireless Control System Configuration Guide, Release 5.2* for instructions.

Using the GUI to Add MAC Addresses of Mesh Access Points to the Controller Filter List

Using the controller GUI, follow these steps to add a MAC filter entry for the access point on the controller.

Step 1 Click **Security** > **AAA** > **MAC Filtering** to open the MAC Filtering page (see Figure 8-7).

Figure 8-7 MAC Filtering Page



MAC Filtering

RADIUS Compatibility Mode: Cisco ACS

(In the Radius Access Request with Mac Authentication password is client's MAC address.)

MAC Delimiter: No Delimiter

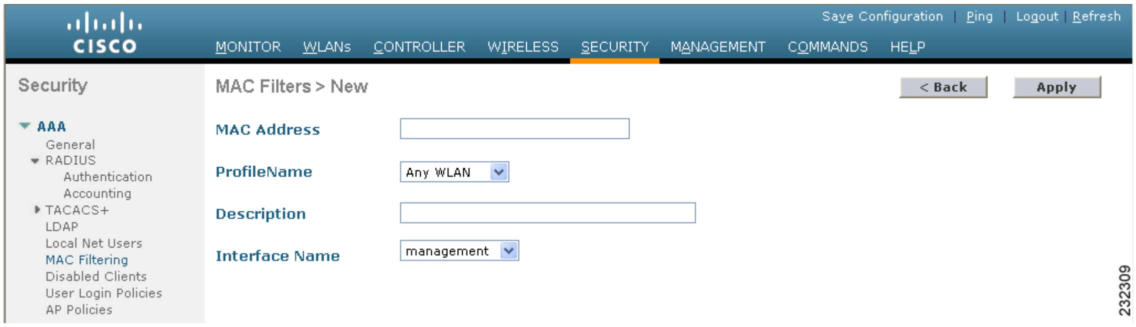
Local MAC Filters

Entries 1 - 4 of 4

MAC Address	Profile Name	Interface	Description
00:1b:d4:a7:8b:00	Any WLAN	management	SB_MAP2
00:1d:71:0d:ee:00	Any WLAN	management	SB_MAP3
00:1d:71:0e:85:00	Any WLAN	management	SB_MAP1
00:1d:71:0e:d0:00	Any WLAN	management	SB_RAP1

Step 2 Click **New** to open the MAC Filters > New page (see Figure 8-8).

Figure 8-8 MAC Filters > New Page



MAC Filters > New

MAC Address	
ProfileName	Any WLAN
Description	
Interface Name	management

Step 3 In the MAC Address field, enter the MAC address of the mesh access point.

Note For 1522 and 1524 outdoor mesh access points, enter the BVI MAC address of the mesh access point into the controller as a MAC filter. For 1130 and 1240 indoor mesh access points, enter the Ethernet MAC address. If the required MAC address does not appear on the exterior of the mesh access point, enter the following command from the access point console to determine the BVI and Ethernet MAC addresses: **sh int | i Hardware**.

Step 4 From the Profile Name drop-down box, choose **Any WLAN**.

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

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

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

Step 7 Click **Apply** to commit your changes. The 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 access points to the list.

Using the CLI to Add MAC Addresses of Mesh Access Points to the Controller Filter List

Using the controller CLI, follow these steps to add a MAC filter entry for the access point on the controller.

Step 1 To add the MAC address of an 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

Configuring External Authentication and Authorization Using a RADIUS Server

Controller software release 5.2 supports external authorization and authentication of mesh access points using a RADIUS server such as Cisco ACS (4.1 and later). The RADIUS server must support the client authentication type of EAP-FAST with certificates.

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

- Configure the RADIUS server to be used as an AAA server on the controller.
- Configure the controller 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, refer to the "Adding a Username to a RADIUS Server" section on page 8-14.
- Configure EAP-FAST on the RADIUS server and install the certificates.

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

Configuring RADIUS Servers

For details on configuring ACS and non-ACS servers, usernames and importing EAP-FAST certificates, refer to the "Configuring the RADIUS Server" section in Chapter 6 of this configuration guide.

Note For additional configuration details on Cisco ACS servers, refer to the following links:

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

http://www.cisco.com/en/US/products/sw/secursw/ps4911/tsd_products_support_series_home.html (UNIX)

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 IOS-based mesh access points (1130, 1240, 1522, 1524), in addition to adding the MAC address to the user list, you need to enter the *platform_name_string–Ethernet_MAC_address* (for example, c1240-001122334455). The controller first sends the MAC address as user name; if this first attempt fails, then the controller sends the *platform_name_string–Ethernet_MAC_address* as user name.

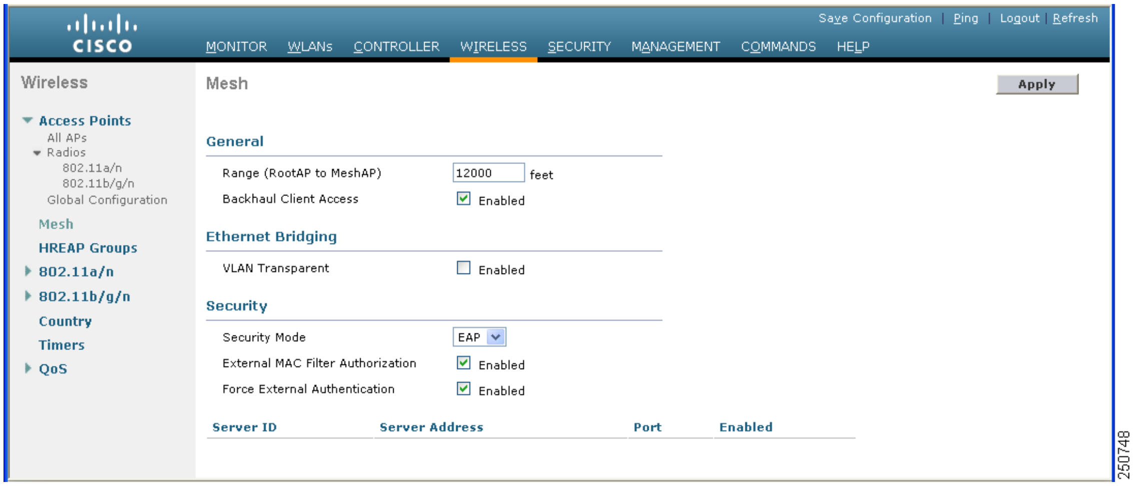
Note If you only enter the *platform_name_string–Ethernet_MAC_address* to the user list, you will see a first-try failure log on the AAA server; however, the IOS-based mesh access point will still be authenticated.

Using the GUI to Enable External Authentication of Mesh Access Points

Using the controller GUI, follow these steps to enable external authentication for a mesh access point.

Step 1 Click **Wireless** > **Mesh** to open the Mesh page (see Figure 8-9).

Figure 8-9 Mesh Page



Mesh

General

Range (RootAP to MeshAP) 12000 feet

Backhaul Client Access ☑ Enabled

Ethernet Bridging

VLAN Transparent □ Enabled

Security

Security Mode EAP

External MAC Filter Authorization ☑ Enabled

Force External Authentication ☑ Enabled

Server ID	Server Address	Port	Enabled

Step 2 Choose **EAP** from the Security Mode drop-down box.

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

Step 4 Click **Apply** to commit your changes.

Step 5 Click **Save Configuration** to save your changes.

Using the CLI to Enable External Authentication of Mesh Access Points

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

config mesh security eap

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

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

config mesh security force-ext-auth enable (Optional)

Using the CLI to View Security Statistics

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

show mesh security-stats *Cisco_AP*

Command shows packet error statistics and a count of failures, timeouts, and association and authentication successes as well as reassociations and reauthentications for the specified access point and its child.

Defining the Mesh Access Point Role

By default, the 152x mesh access points are shipped with a radio role set to MAP. You must reconfigure a mesh access point to act as a RAP.

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

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

The radio role can also be changed using the controller GUI.

Configuring Global Mesh Parameters

This section provides instructions for configuring the access point to establish a connection with the controller including:

- Setting the maximum range between RAP and MAP (not applicable to 1130 and 1240 indoor mesh access points)
- Enabling a backhaul to carry client traffic
- Defining whether 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).

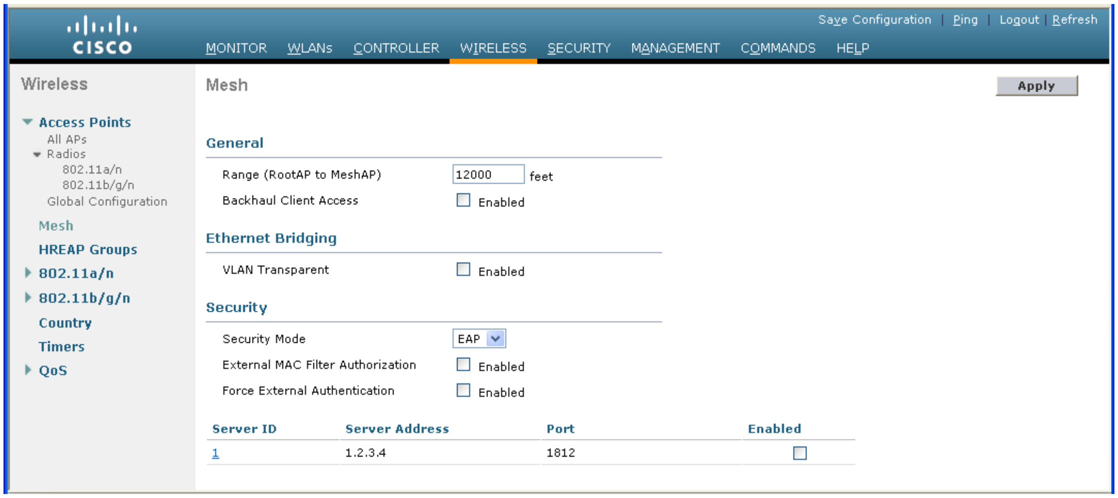
You can configure the necessary mesh parameters using the controller GUI or CLI. All parameters are applied globally.

Using the GUI to Configure Global Mesh Parameters

Using the controller GUI, follow these steps to configure global mesh parameters.

Step 1 Click **Wireless** > **Mesh** to open the Mesh page (see Figure 8-10).

Figure 8-10 Mesh Page



Mesh

General

Range (RootAP to MeshAP) 12000 feet

Backhaul Client Access □ Enabled

Ethernet Bridging

VLAN Transparent □ Enabled

Security

Security Mode EAP

External MAC Filter Authorization □ Enabled

Force External Authentication □ Enabled

Server ID	Server Address	Port	Enabled
1	1.2.3.4	1812	□

Step 2 Modify the mesh parameters as appropriate. Table 8-4 describes each parameter.

Table 8-4 Global Mesh Parameters

Parameter	Description
Range (RootAP to MeshAP)	The optimum distance (in feet) that should exist between the root access point (RAP) and the mesh access point (MAP). This global parameter applies to all access points when they join the controller and all existing access points in the network. **Range:** 150 to 132,000 feet **Default:** 12,000 feet **Note** After this feature is enabled, all mesh access points reboot.
Backhaul Client Access	When this feature is enabled, 1520 series (152x) mesh access points allow wireless client association over the 802.11a radio. Therefore, a 152x mesh access point can carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio. When this feature is disabled, the 152x carries backhaul traffic over the 802.11a radio and allows client association only over the 802.11b/g radio. **Default:** Disabled **Note** After this feature is enabled, all mesh access points reboot.

Table 8-4 Global Mesh Parameters (continued)

Parameter	Description
VLAN Transparent	This feature determines how a mesh access point handles VLAN tags for Ethernet bridged traffic. **Note** Refer to the "Configuring Ethernet Bridging and Ethernet VLAN Tagging" section on page 8-25 for overview and additional configuration details. If this parameter is enabled, then VLAN tags are not handled and packets are bridged as if they are untagged. If this parameter is disabled, all packets are tagged non-VLAN transparent or VLAN-opaque and all tagged packets are dropped. Uncheck the check box to enable the VLAN Tagging feature. **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. **Note** Refer to "Configuring Ethernet Bridging and Ethernet VLAN Tagging" section on page 8-25 for more details. **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

Table 8-4 Global Mesh Parameters (continued)

Parameter	Description
External MAC Filter Authorization	MAC filtering uses the local MAC filter on the controller by default. When external MAC filter authorization is enabled, if the MAC address is not found in the local MAC filter, then the MAC address in the external RADIUS server is used. This protects your network against rogue mesh access points by preventing access points that are not defined on the external server from joining. Before you employ external authentication within the mesh network, the following configuration is required: • The RADUIS 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 (1240, 1522, 1524), the platform name of the mesh access point is located in front of the Ethernet address within the certificate; therefore, the username for external RADIUS servers is *platform_name_string–Ethernet MAC address* such as *c1240-001122334455*. • 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 8-4 Global Mesh Parameters (continued)

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

Step 3 Click **Apply** to commit your changes.

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

Using the CLI to Configure Global Mesh Parameters

Using the controller CLI, follow these steps to configure global mesh parameters.

Note Refer to the "Using the GUI to Configure Global Mesh Parameters" section on page 8-16 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 access points in the network, enter this command:

config mesh range *feet*

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

Step 2 To enable or disable client association on the primary backhaul (802.11a) of an 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 3 To enable or disable VLAN transparent, enter this command:

config mesh ethernet-bridging vlan-transparent {enable | disable}

Step 4 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 MAC address filter in an external RADIUS server for authentication instead of the controller (local), enter these commands:

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

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

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

config mesh security eap

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

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

config mesh security force-ext-auth enable

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

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

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

config mesh security force-ext-auth enable

Step 5 To save your changes, enter this command:

save config

Using the CLI to View Global Mesh Parameter Settings

Use these commands to obtain information on global mesh settings:

- **show mesh client-access**—Shows the status of the client-access backhaul as either enabled or disabled. When this option is enabled, mesh access points are able to associate with 802.11a wireless clients over the 802.11a backhaul. This client association is in addition to the existing communication on the 802.11a backhaul between the root and mesh access points.

```
controller >show mesh client-access
Backhaul with client access status: enabled
```

- **show mesh env** {**summary** | *Cisco_AP*}—Shows the temperature, heater status, and Ethernet status for either all access points (summary) or a specific access point (*Cisco_AP*). The access point name, role (RootAP or MeshAP), and model are also shown.
  - The temperature is shown in both Fahrenheit and Celsius.
  - The heater status is ON or OFF.
  - The Ethernet status is UP or DOWN.

Note Battery status appears as N/A (not applicable) in the **show mesh env** *Cisco_AP* status display because it is not provided for access points.

```
controller > show mesh env summary

AP Name             Temperature(C/F)  Heater  Ethernet  Battery
------------------  ----------------  ------  --------  -------
SB_RAP1              39/102           OFF     UpDnNANA  N/A
SB_MAP1              37/98            OFF     DnDnNANA  N/A
SB_MAP2              42/107           OFF     DnDnNANA  N/A
SB_MAP3              36/96            OFF     DnDnNANA  N/A
```

```
controller >show mesh env SB_RAP1


AP Name.......................................... SB_RAP1
AP Model......................................... AIR-LAP1522AG-A-K9
AP Role.......................................... RootAP

Temperature...................................... 39 C, 102 F
Heater........................................... OFF
Backhaul......................................... GigabitEthernet0

GigabitEthernet0 Status.......................... UP
    Duplex....................................... FULL
    Speed........................................ 100
    Rx Unicast Packets........................... 988175
    Rx Non-Unicast Packets....................... 8563
    Tx Unicast Packets........................... 106420
    Tx Non-Unicast Packets....................... 17122
GigabitEthernet1 Status.......................... DOWN
  POE Out........................................ OFF

Battery.......................................... N/A
```

Configuring Local Mesh Parameters

After configuring global mesh parameters, you must configure the following local mesh parameters:

- Antenna Gain
  - Refer to the "Configuring Antenna Gain" section on page 8-22.
- Workgroup Bridge Groups
  - Refer to the "Using the GUI to Configure Antenna Gain" section on page 8-22.

Configuring Antenna Gain

You must configure the antenna gain for the access point to match that of the antenna installed using the controller GUI or controller CLI.

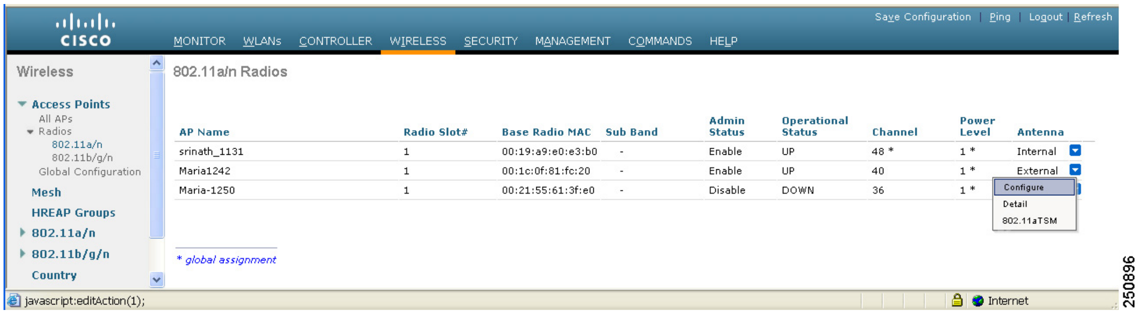
Note Refer to the "External Antennas" section of the *Cisco Aironet 1520 Series Outdoor Mesh Access Points Getting Started Guide* for a summary of supported antennas and their antenna gains at http://www.cisco.com/en/US/docs/wireless/access_point/1520/quick/guide/ap1520qsg.html

Using the GUI to Configure Antenna Gain

Using the controller GUI, follow these steps to configure the antenna gain.

Step 1 Click **Wireless** > **Access Points** > **Radios** > **802.11a/n** to open the 802.11a/n Radios page (see Figure 8-11).

Figure 8-11 802.11a/n Radios Page



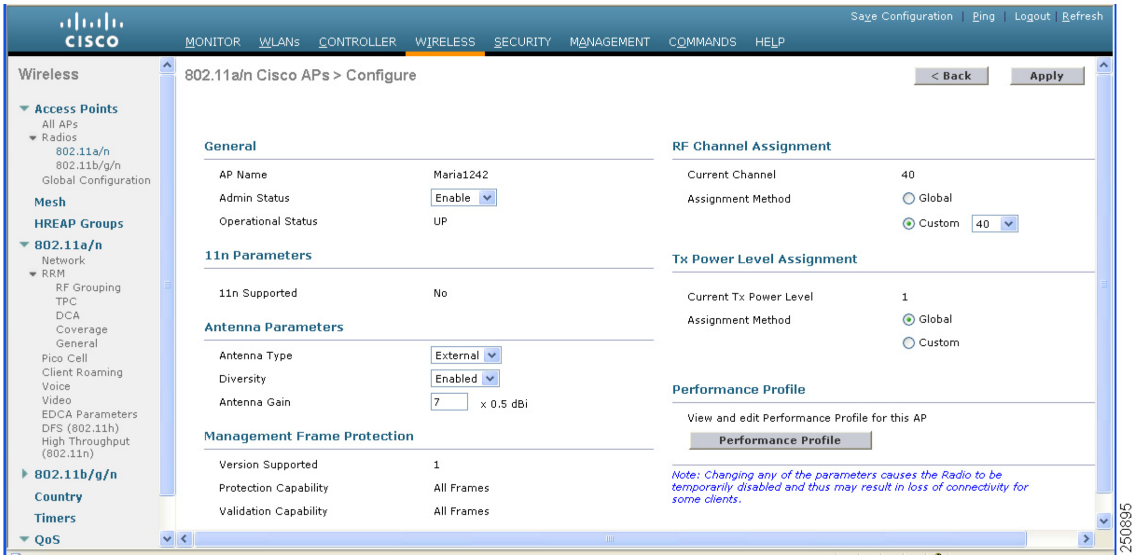
802.11a/n Radios

AP Name	Radio Slot#	Base Radio MAC	Sub Band	Admin Status	Operational Status	Channel	Power Level	Antenna
srinath_1131	1	00:19:a9:e0:e3:b0	-	Enable	UP	48 *	1 *	Internal
Maria1242	1	00:1c:0f:81:fc:20	-	Enable	UP	40	1 *	External
Maria-1250	1	00:21:55:61:3f:e0	-	Disable	DOWN	36	1 *	

* global assignment

Step 2 Hover your cursor over the blue drop-down arrow for the mesh access point antenna that you want to configure and choose **Configure**. The 802.11a/n Cisco APs > Configure page appears (see Figure 8-12).

Figure 8-12 802.11a/n Cisco APs > Configure Page



802.11a/n Cisco APs > Configure

General

AP Name: Maria1242
Admin Status: Enable
Operational Status: UP

11n Parameters

11n Supported: No

Antenna Parameters

Antenna Type: External
Diversity: Enabled
Antenna Gain: 7 x 0.5 dBi

Management Frame Protection

Version Supported: 1
Protection Capability: All Frames
Validation Capability: All Frames

RF Channel Assignment

Current Channel: 40
Assignment Method: ○ Global ● Custom 40

Tx Power Level Assignment

Current Tx Power Level: 1
Assignment Method: ● Global ○ Custom

Performance Profile

View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

Step 3 Under the Antenna Parameters section, enter the antenna gain in 0.5-dBm units in the Antenna Gain field. For example, 2.5 dBm = 5.

Note Only external antennas have configurable gain settings. The value that you enter must match the value specified by the vendor for that antenna.

Step 4 Click **Apply** to commit your changes.

Step 5 Click **Save Configuration** to save your changes.

Using the CLI to Configure Antenna Gain

Using the controller CLI, follow these steps to configure the antenna gain.

Step 1 To configure the antenna gain for the 802.11a backhaul radio, enter this command:

config 802.11a antenna extAntGain *antenna_gain Cisco_AP*

where *antenna_gain* is in 0.5-dBm units (for example, 2.5 dBm = 5).

Step 2 To save your changes, enter this command:

save config

Workgroup Bridge Groups on Mesh Access Points

A workgroup bridge (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 mesh access point using Internet Access Point Protocol (IAPP) messaging. The mesh access point treats the WGB as a wireless client.

When configured as a WGB, the 1130, 1240, and 1310 autonomous access points as well as the series 3200 mobile access router (MAR) can associate with mesh access points. The mesh access points can be configured as RAPs or MAPs. WGB association is supported on both the 2.4-GHz (802.11b) and 5-GHz (802.11a) radio on the 1522, and the 2.4-GHz (802.11b) and 4.9-GHz (public safety radio) on the 1524.

Note Refer to the “Cisco Workgroup Bridges” section in Chapter 7 of this manual for configuration details.

Supported Workgroup Modes and Capacities

- The 1130, 1240, 1310 autonomous access point must be running Cisco IOS release 12.4(3g)JA or later (on 32-MB access points) or Cisco IOS release 12.3(8)JEB or later (on 16-MB access points). Cisco IOS releases prior to 12.4(3g)JA and 12.3(8)JEB are not supported.

  Note If your mesh access point has two radios, you can only configure workgroup bridge mode on one of the radios. Cisco recommends that you disable the second radio. Workgroup bridge mode is not supported on access points with three radios such as 1524.

- Client mode WGB (BSS) is supported; however, infrastructure WGB is not supported.
- Mesh access points can support up to 200 clients including wireless clients, WGBs, and wired clients behind the associated WGBs.
- WGBs operating with Cisco IOS release 12.4(3g)JA 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).

Client Roaming

High-speed roaming of Cisco Compatible Extension (CX), version 4 (v4) clients is supported at speeds up to 70 mph in outdoor mesh deployments of 1522 and 1524 mesh access points. An application example 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**—This feature 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**—This feature 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**—This feature 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.

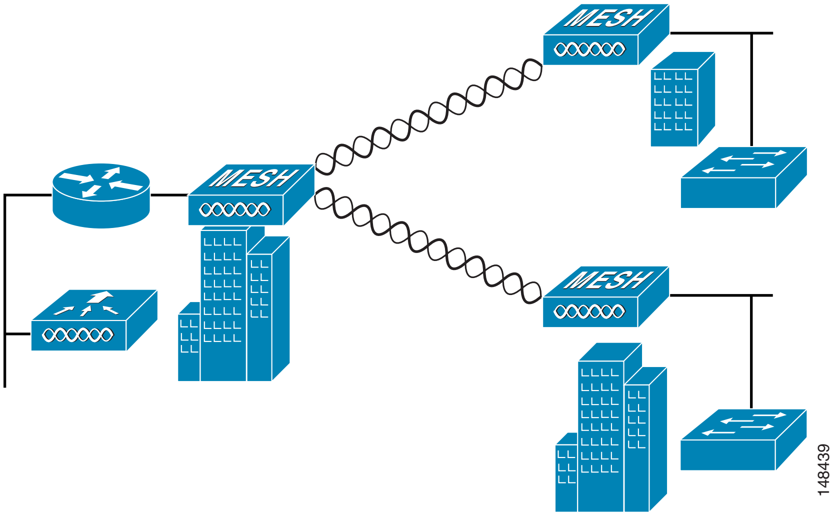
Configuring Ethernet Bridging and Ethernet VLAN Tagging

Ethernet bridging is used in two mesh network scenarios:

- Point-to-point and point-to-multipoint bridging between MAPs (untagged packets). A typical trunking application might be bridging traffic between buildings within a campus (Figure 8-13).

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

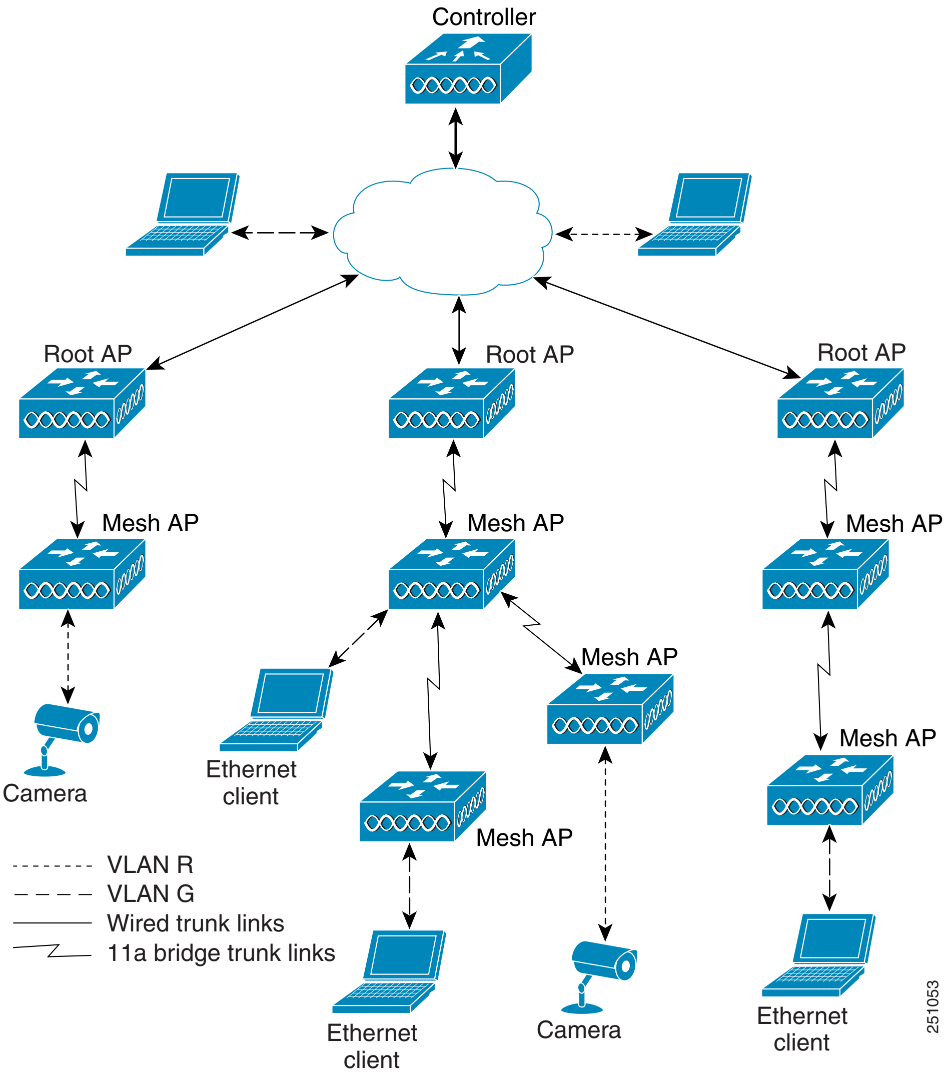
Figure 8-13 Point-to-Multipoint Bridging



- 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 using Ethernet VLAN tagging is 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 (see Figure 8-14).

Figure 8-14 Ethernet VLAN Tagging



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 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). Refer to "Configuring Global Mesh Parameters" section on page 8-16.
  - VLAN transparent is enabled by default. To set as non-VLAN transparent you must uncheck the VLAN transparent option in the global mesh parameters window.
- VLAN configuration on a mesh access point is only applied if all the uplink mesh access points are able to support that VLAN.
  - If uplink access points are not able to support the VLAN, then the configuration is stored rather than applied.
- VLAN tagging can only be configured on Ethernet interfaces.
  - On 152x mesh access points, 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.
- 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 configuration is required to support VLAN tagging on any 802.11a backhaul Ethernet interface within the mesh network.
  - This includes the RAP uplink Ethernet port. The required configuration happens 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 an 152x access point. VLANs can be configured on ports 0 (PoE-in), 1 (PoE-out) and 3 (fiber).
- If bridging between two MAPs, enter the distance (mesh range) between the two access points that are bridging. (Not applicable to applications in which you are forwarding traffic connected to the MAP to the RAP, access mode)
- Up to 16 VLANs are supported on each sector. Therefore, the cumulative number of VLANs supported by a RAP's children (MAPs) cannot exceed 16.
- Ethernet ports on access points function as either *access* or *trunk* ports within an Ethernet tagging deployment.
- Access Mode– In this mode only untagged packets are accepted. All packets are tagged with a user-configured VLAN called access-VLAN. For this mode to take effect, the global VLAN mode should be non-VLAN transparent.
  - This option is used 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 always 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. For this mode to take effect, the global VLAN mode should be non-VLAN transparent.
  - This option is used for bridging applications such as forwarding traffic between two MAPs resident on separate buildings within a campus.
- The switch port connected to the RAP must be a trunk.
  - The trunk port on the switch and the RAP trunk port must match.
- A configured VLAN on a MAP Ethernet port cannot function as a Management VLAN.
- 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.

Note You cannot bridge VLAN ID 1 when using VLAN-Opaque Ethernet bridging because VLAN 1 is the internal native VLAN within a mesh network. This setting cannot be changed.

Using the GUI to Enable Ethernet Bridging and VLAN Tagging

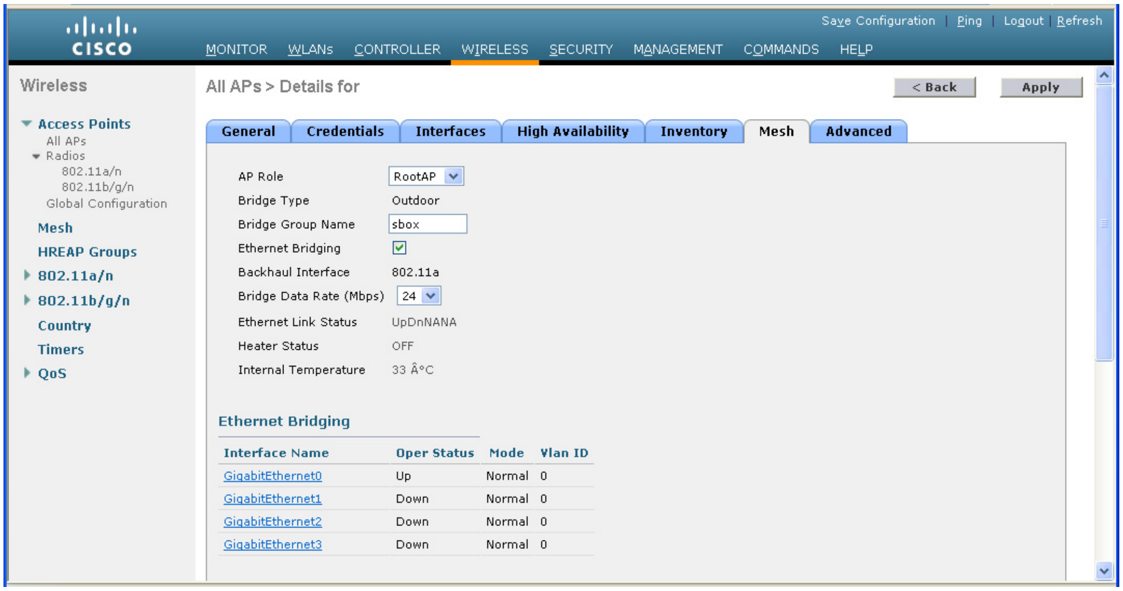
Using the controller GUI, follow these steps to enable Ethernet bridging on a RAP or MAP.

Step 1 Click **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 Ethernet bridging.

Step 3 Click the **Mesh** tab to open the All APs > Details for (Mesh) page (see Figure 8-15).

Figure 8-15 All APs > Details for (Mesh) Page



All APs > Details for

AP Role	RootAP
Bridge Type	Outdoor
Bridge Group Name	sbox
Ethernet Bridging	☑
Backhaul Interface	802.11a
Bridge Data Rate (Mbps)	24
Ethernet Link Status	UpDnNANA
Heater Status	OFF
Internal Temperature	33 Â°C

Ethernet Bridging

Interface Name	Oper Status	Mode	Vlan ID
GigabitEthernet0	Up	Normal	0
GigabitEthernet1	Down	Normal	0
GigabitEthernet2	Down	Normal	0
GigabitEthernet3	Down	Normal	0

Step 4 Choose one of the following options from the AP Role drop-down box.

- **MeshAP**—Choose this option if the 1520 series access point has a wireless connection to the controller. This is the default setting.
- **RootAP**—Choose this option if the 1520 series access point has a wired connection to the controller.

Note You must set at least one mesh access point to RootAP in the mesh network.

Step 5 To assign this access point to a bridge group, enter a name for the group in the Bridge Group Name field.

Step 6 Check the **Ethernet Bridging** check box to enable Ethernet bridging or uncheck it to disable this feature.

Step 7 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 8 Perform one of the following to configure the Ethernet ports:

- If you are configuring a MAP access port, follow these steps:

  a. Click **gigabitEthernet1** (port 1-PoE out).

  b. Select **access** from the mode drop-down menu.

  c. Enter a VLAN ID. The VLAN ID can be any value between 2 and 4095.

  Note You cannot bridge VLAN ID 1 when using VLAN-Opaque Ethernet bridging because VLAN 1 is the internal native VLAN within a mesh network. This setting cannot be changed.

  Note A maximum of 16 VLANs are supported across all of a RAP's subordinate MAPs.

- If you are configuring a RAP or MAP trunk port, follow these steps:

  a. Click **gigabitEthernet0** (port 0-PoE in).

  b. Select **trunk** from the mode drop-down menu.

  c. Enter a native VLAN ID for *incoming* traffic. The native VLAN ID can be any value between 2 and 4095. Do not assign any value assigned to a user-VLAN (access).

  d. Enter a trunk VLAN ID for *outgoing* packets:

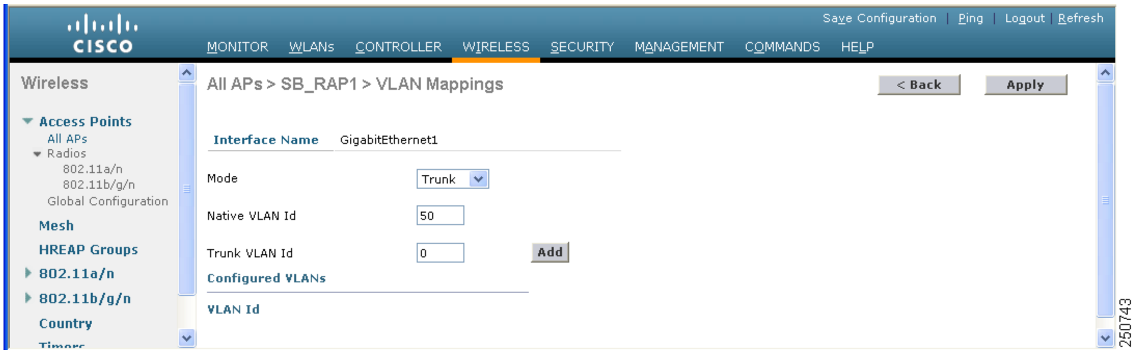
  e. If forwarding *untagged* packets, do not change the default trunk VLAN ID value of zero. (MAP-to-MAP bridging, campus environment)

  f. If forwarding *tagged* packets, enter a VLAN ID (2 to 4095) that is not already assigned. (RAP to switch on wired network).

  g. 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 window.

  Note To remove a VLAN from the list, select the Remove option from the arrow drop-down to the right of the desired VLAN.

Figure 8-16 All APs > AP > VLAN Mappings Page



All APs > SB_RAP1 > VLAN Mappings

Interface Name GigabitEthernet1

Mode Trunk

Native VLAN Id 50

Trunk VLAN Id 0

Step 9 Click **Apply** to commit your changes.

Step 10 At the **Wireless > Mesh** page, select the appropriate backhaul rate from the bridge data rate drop-down menu. The default value is 24 Mbps for the 802.11a backhaul interface.

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Table 8-5 describes display-only parameters on the mesh page.

Table 8-5 Display Parameters for Access Points

Parameter	Description
Bridge type	Displays either outdoor (152x access points) or indoor (1130 or 1240 access points)
Backhaul Interface	Displays the radio band that this MAP uses to transfer data to other MAPs. The only possible value is 802.11a.
Ethernet Link Status	Displays the up or down status of the Ethernet link of the AP152x. The Up or Down (Dn) status of the four Ethernet ports is reported in the following format: port0:port1:port2:port3. For example, *UpDnDnDn* indicates that port0 is Up and ports 1, 2, and 3 are Down (Dn). **Note** If *NA* displays in the status string, then the port has no wired connection to that port.
Heater Status	Displays status of either ON or OFF.
Internal Temperature	Displays the internal temperature of the 1522 and 1524.

Using the CLI to Configure Ethernet Bridging Parameters

Using the controller CLI, follow these steps to configure Ethernet bridging on a RAP or MAP.

Step 1 To specify that your AP152x has bridge functionality, enter this command:

config ap mode bridge *Cisco_AP*

Step 2 To specify the role of this access point in the mesh network, enter this command:

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

Use the **meshAP** parameter if the access point has a wireless connection to the controller or use the **rootAP** parameter if the access point has a wired connection to the controller.

Note Configuration as a MAP is the default setting.

Step 3 To assign the access point to a bridge group, enter this command:

config ap bridgegroupname set *groupname Cisco_AP*

Step 4 To enable Ethernet bridging on the access point, enter this command:

config mesh ethernet-bridging vlan transparent *disable*

Step 5 To specify the rate (in Mb/s) at which data is shared between access points on the backhaul interface, enter this command:

config ap bhrate *rate Cisco_AP*

The default value is 24 Mb/s for the 802.11a backhaul interface.

Step 6 To save your settings, enter this command:

save config

Using the CLI to Configure Ethernet VLAN Tagging

VLAN ID 1 is not reserved as the default VLAN.

A maximum of 16 VLANs are supported across all of a RAP's subordinate MAPs.

A VLAN ID can be any value between 1 and 4095. Do not assign any value assigned to another VLAN.

- To configure a MAP access port, enter this command:

  config ap ethernet 1 mode access enable *AP1520-MAP 50*

  where *AP1520-MAP* is the variable *Cisco_AP* 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 *AP1520-MAP 60*

  where *AP1520-MAP* is the variable *Cisco_AP* 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 *AP1522-MAP3 65*

    where *AP1522-MAP 3* is the variable *Cisco_AP* and *65* is the variable *vlan ID*

Configuring Advanced Features

- Configuring Voice Parameters in Mesh Networks, page 8-32
- Enabling Mesh Multicast Containment for Video, page 8-37

Configuring Voice Parameters in Mesh Networks

You can configure call admission control (CAC) and QoS on the controller to manage voice quality on the mesh network.

Note Voice is supported only on indoor mesh networks (1130 and 1240 access points).

CAC

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 different network loads, CAC in CCXv4 or later is required.

Note CAC is supported in Cisco Compatible Extensions (CCX) v4 or later. See the "Configuring Cisco Client Extensions" section on page 6-19 for more information on CCX.

All calls on a mesh access point use bandwidth-based CAC. Load-based CAC is not supported.

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 can accommodate a particular call by looking at the bandwidth available and compares it against the bandwidth required for the call. If not enough bandwidth is available to maintain the maximum allowed number of calls with acceptable quality, the access point rejects the call.

QoS and DSCP Marking

QoS 802.11e is supported on the access and backhaul radios of mesh access points. MAPs can prioritize client traffic based on the QoS setting defined on the controller. CAC is implemented on the backhaul.

Mesh access points recognize DSCP markings from devices. DSCP is performed on the originating Cisco 7920 voice handset (client) and the terminating voice handset or terminal. No DSCP marking is performed on the controller, MAP or CAC.

Note QoS only is relevant when there is congestion on the network.

You can configure bandwidth-based CAC and QoS for mesh networks using the controller GUI or CLI. The instructions for configuring these features is the same for both mesh and non-mesh networks with the exception of QoS settings.

- Follow the instructions in the "Configuring Voice and Video Parameters" section on page 4-52 to configure voice and video parameters.
  - Refer to the "Guidelines for Using Voice on the Mesh Network" section on page 8-33 for mesh-specific configuration guidelines for voice including QoS.

The instructions for viewing voice and video details using the CLI are different for mesh and non-mesh access points.

- Follow the instructions in the "Using the CLI to View Voice Details for Mesh Networks" section on page 8-34 to view details for mesh access points.

Guidelines for Using Voice on the Mesh Network

- Voice is only supported on indoor mesh access points, 1130 and 1240.
- 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.
- On the **802.11a** or **802.11b/g/n >** *Global* parameters window:
  - Enable dynamic target power control (DTPC)
  - Disable all data rates less than 11 Mbps
- On the **802.11a** or **802.11b/g/n >** *Voice* parameters window:
  - 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%
  - Set the reserved roaming bandwidth to 6%
  - Enable traffic stream metrics
- On the **802.11a** or **802.11b/g/n >** *EDCA* parameters window:
  - Set the EDCA profile for the interface as voice optimized
  - Disable low latency MAC
- On the **QoS >** *Profile* window:
  - Create a voice profile and select 802.1q as the wired QoS protocol type
- On the **WLANs >** *Edit* > *QoS* window:
  - 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* window:
  - Select CCKM for authorization (*auth*) key management (*mgmt*) if you want to support fast roaming. Refer to the "Client Roaming" section on page 8-24
- On the **x >** ***y*** window:
  - Disable voice active detection (VAD)

Voice Call Support in a Mesh Network

Table 8-6 lists a projected minimum and maximum of voice calls supported by radio type and mesh access point role (RAP or MAP) for planning purposes.

Table 8-6 Projected Voice Call Support on a Mesh Network

Mesh Access Point Role	Radio	Minimum Calls Supported[1]	Maximum Calls Supported[2]
RAP	802.11a	14	18
	802.11b/g/n	14	18
MAP1	802.11a	6	9
	802.11b/g/n	11	18
MAP2	802.11a	4	7
	802.11b/g/n	5	9

[1] Bandwidth of 855 transmit units (TUs) with 50% of the bandwidth reserved for voice calls.

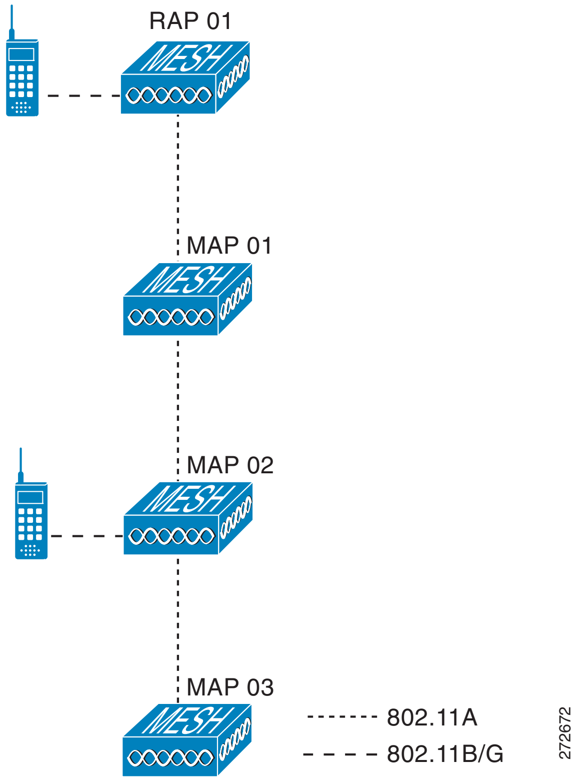
[2] Bandwidth of 1076 TUs with 50% of the bandwidth reserved for voice calls.

Using the CLI to View Voice Details for Mesh Networks

Use the commands in this section to view details on voice calls on the mesh network.

Refer to Figure 8-17 when using the CLI commands and viewing their output.

Figure 8-17 Mesh Network Example



- To view the total number of voice calls and the bandwidth used for voice calls on each root access point, enter this command:

  show mesh cac summary

  Information similar to the following appears:

```
AP Name          Slot#   Radio  BW Used/Max  Calls
------------    -------  -----  -----------  -----
SB_RAP1              0   11b/g     0/23437    0
                     1   11a       0/23437    2
SB_MAP1              0   11b/g     0/23437    0
                     1   11a       0/23437    0
SB_MAP2              0   11b/g     0/23437    0
                     1   11a       0/23437    0
SB_MAP3              0   11b/g     0/23437    0
                     1   11a      0/23437    0
```

- To view the mesh tree topology for the network and the bandwidth utilization (used/maximum available) of voice calls and video links for each access point and radio, enter this command:

  show mesh cac bwused {**voice** | **video**} *Cisco_AP*

  Information similar to the following appears:

```
AP Name       Slot#    Radio      BW Used/Max
------------- -------  -----      -----------
SB_RAP1         0      11b/g       1016/23437
                1      11a         3048/23437
|SB_MAP1        0      11b/g       0/23437
                1      11a         3048/23437
||  SB_MAP2     0      11b/g       2032/23437
                1      11a         3048/23437
||| SB_MAP3     0      11b/g       0/23437
                1      11a         0/23437
```

Note The bars (|) to the left of the AP Name field indicate the number of hops that the mesh access point is away from its root access point (RAP).

Note When the radio type is the same, the backhaul bandwidth used (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 access point radio, enter this command:

  show mesh cac access *Cisco_AP*

Information similar to the following appears:

```
AP Name            Slot#   Radio     Calls
-------------     -------  -----    -----
SB_RAP1             0      11b/g      0
                    1      11a        0
|   SB_MAP1         0      11b/g      0
                    1      11a        0
||  SB_MAP2         0      11b/g      1
                    1      11a        0
||| SB_MAP3         0      11b/g      0
                    1      11a        0
```

Note Each call received by an 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 *Cisco_AP*

  Information similar to the following appears:

```
AP Name            Slot#   Radio     Calls
-------------     -------  -----    -----
SB_RAP1             0      11b/g      0
                    1      11a        1
|   SB_MAP1         0      11b/g      0
                    1      11a        1
||  SB_MAP2         0      11b/g      1
                    1      11a        1
||| SB_MAP3         0      11b/g      0
                    1      11a        0
```

Note The *calls* column for each mesh access point radio in a call path increments by one. For example, for a call that initiates at *map2* (**show mesh cac call path** *SB_MAP2*) and terminates at *rap1* by way of *map1,* one call is added to the *map2* 802.11b/g and 802.11a radio *calls* column*,* one call to the *map1* 802.11a backhaul radio *calls* column, and one call to the *rap1* 802.11a backhaul radio *calls* column.

- To view the mesh tree topology of the network, the voice calls that are rejected at the access point radio because of insufficient bandwidth, and the corresponding access point radio where the rejection occurred, enter this command:

  show mesh cac rejected *Cisco_AP*

Information similar to the following appears:

```
AP Name            Slot#   Radio     Calls
-------------     -------  -----    -----
SB_RAP1             0      11b/g      0
                    1      11a        0
|   SB_MAP1         0      11b/g      0
                    1      11a        0
||  SB_MAP2         0      11b/g      1
                    1      11a        0
||| SB_MAP3         0      11b/g      0
                    1      11a        0
```

Note If a call is rejected at the *map2* 802.11b/g radio, its *calls* column increments by one.

- To view the number of bronze, silver, gold, platinum, and management queues active on the specified access point. The peak and average length of each queue are shown as well as the overflow count.

  show mesh queue-stats *Cisco_AP*

  Information similar to the following appears:

```
Queue Type  Overflows  Peak length  Average length
 ----------  ---------  -----------  --------------
 Silver      0          1            0.000
 Gold        0          4            0.004
 Platinum    0          4            0.001
 Bronze      0          0            0.000
 Management  0          0            0.000
```

  Overflows—The total number of packets dropped because of 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 [mesh access points (MAPs) and root access points (RAPs)] 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:

- **Regular mode**—Data is multicast across the entire mesh network and all its segments by bridging-enabled RAPs and MAPs.
- **In 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. In mode is the default mode.
- **In-out mode**—The RAP and MAP both multicast but in a different manner:
  - If multicast packets are received at a MAP over Ethernet, they are sent to the RAP; however, they are not sent to other MAP Ethernets, and the MAP-to-MAP packets are filtered out of the multicast.
  - If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks. When the in-out mode is in operation, it is important to properly partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment and then sent back into the network.

Note If 802.11b clients need to receive CAPWAP multicasts, then multicast must be enabled globally on the controller as well as on the mesh network (using the **config network multicast global enable** CLI command). If multicast does not need to extend to 802.11b clients beyond the mesh network, the global multicast parameter should be disabled (using the **config network multicast global disable** CLI command).

Using the CLI to Enable Multicast on the Mesh Network

- 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.

Backhaul Client Access (Universal Access) for Indoor and Outdoor Mesh Access Points

You can configure the backhaul for mesh access points (1522, 1240 and 1130) to accept client traffic. When this feature is enabled, mesh access points allow wireless client association over the 802.11a radio. This universal access allows an access point to carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio. When this feature is disabled, backhaul traffic is only transmitted over the 802.11a radio and client association is only allowed over the 802.11b/g radio.

After this feature is enabled, all mesh access points reboot.

Default: Disabled.

Note This parameter is applicable to mesh access points with two radios (1522, 1240 and 1130) *excluding* the 1524.

To enable this feature on the controller, check the Backhaul Client Access check box on the **Wireless > Mesh** window. Refer to “Configuring Global Mesh Parameters” section on page 8-16.

Viewing Mesh Statistics and Reports

Viewing Mesh Statistics for an Access Point

This section explains how to use the controller GUI or CLI to view mesh statistics for specific access points.

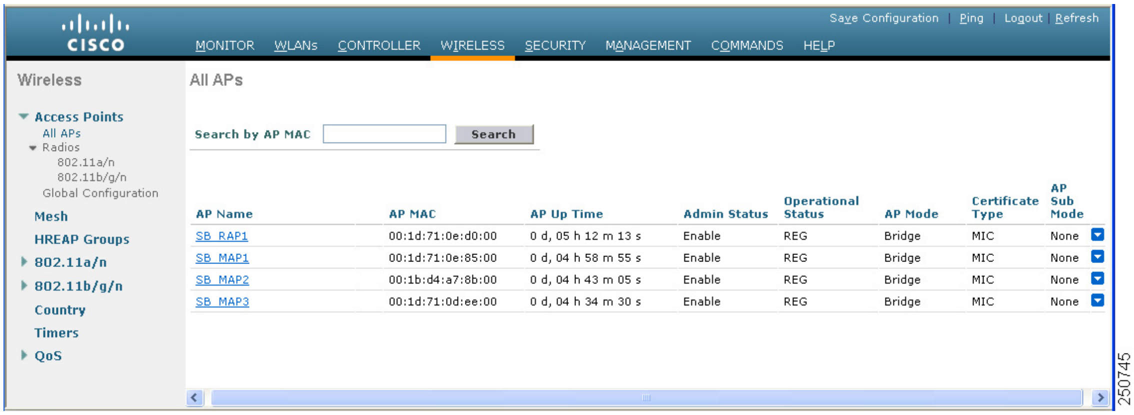
Note You can modify the Statistics Timer interval setting on the All APs > Details page of the controller GUI.

Using the GUI to View Mesh Statistics for an Access Point

Follow these steps to view mesh statistics for a specific access point using the controller GUI.

Step 1 Click **Wireless > Access Points > All APs** to open the All APs page (see Figure 8-18).

Figure 8-18 All APs Page

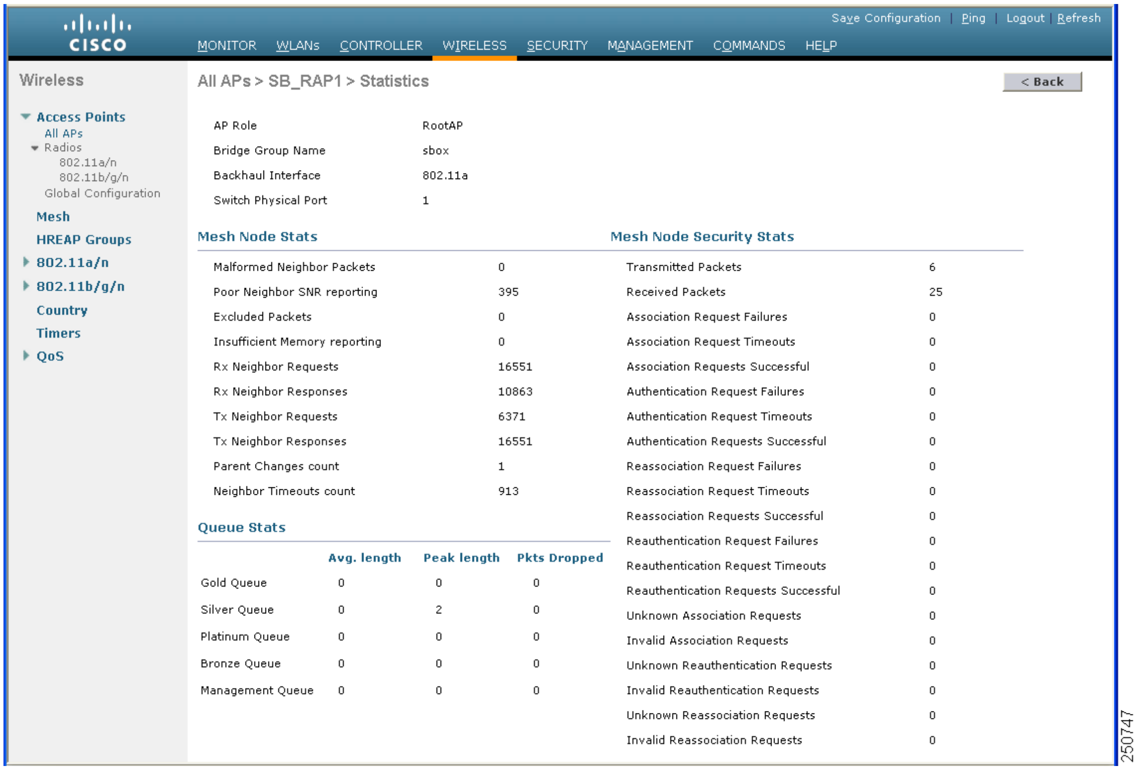


All APs

AP Name	AP MAC	AP Up Time	Admin Status	Operational Status	AP Mode	Certificate Type	AP Sub Mode
SB_RAP1	00:1d:71:0e:d0:00	0 d, 05 h 12 m 13 s	Enable	REG	Bridge	MIC	None
SB_MAP1	00:1d:71:0e:85:00	0 d, 04 h 58 m 55 s	Enable	REG	Bridge	MIC	None
SB_MAP2	00:1b:d4:a7:8b:00	0 d, 04 h 43 m 05 s	Enable	REG	Bridge	MIC	None
SB_MAP3	00:1d:71:0d:ee:00	0 d, 04 h 34 m 30 s	Enable	REG	Bridge	MIC	None

Step 2 To view statistics for a specific access point, hover your cursor over the blue drop-down arrow for the desired access point and choose **Statistics**. The All APs > *Access Point Name* > Statistics page for the access point appears (see Figure 8-19).

Figure 8-19 All APs > Access Point Name > Statistics Page



All APs > SB_RAP1 > Statistics

AP Role	RootAP
Bridge Group Name	sbox
Backhaul Interface	802.11a
Switch Physical Port	1

Mesh Node Stats

Malformed Neighbor Packets	0
Poor Neighbor SNR reporting	395
Excluded Packets	0
Insufficient Memory reporting	0
Rx Neighbor Requests	16551
Rx Neighbor Responses	10863
Tx Neighbor Requests	6371
Tx Neighbor Responses	16551
Parent Changes count	1
Neighbor Timeouts count	913

Queue Stats

	Avg. length	Peak length	Pkts Dropped
Gold Queue	0	0	0
Silver Queue	0	2	0
Platinum Queue	0	0	0
Bronze Queue	0	0	0
Management Queue	0	0	0

Mesh Node Security Stats

Transmitted Packets	6
Received Packets	25
Association Request Failures	0
Association Request Timeouts	0
Association Requests Successful	0
Authentication Request Failures	0
Authentication Request Timeouts	0
Authentication Requests Successful	0
Reassociation Request Failures	0
Reassociation Request Timeouts	0
Reassociation Requests Successful	0
Reauthentication Request Failures	0
Reauthentication Request Timeouts	0
Reauthentication Requests Successful	0
Unknown Association Requests	0
Invalid Association Requests	0
Unknown Reauthentication Requests	0
Invalid Reauthentication Requests	0
Unknown Reassociation Requests	0
Invalid Reassociation Requests	0

This page shows the role of the access point in the mesh network, the name of the bridge group to which the 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 access point. Table 8-7 describes each of the statistics.

Table 8-7 Mesh Access Point Statistics

Statistics	Parameter	Description
Mesh Node Stats	Malformed Neighbor Packets	The number of malformed packets received from the neighbor. Examples of malformed packets include malicious floods of traffic such as malformed or short DNS packets and malformed DNS replies.
	Poor Neighbor SNR Reporting	The number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.
	Excluded Packets	The number of packets received from excluded neighbor mesh access points.
	Insufficient Memory Reporting	The number of insufficient memory conditions.
	Rx Neighbor Requests	The number of broadcast and unicast requests received from the neighbor mesh access points.
	Rx Neighbor Responses	The number of responses received from the neighbor mesh access points.
	Tx Neighbor Requests	The number of unicast and broadcast requests sent to the neighbor mesh access points.
	Tx Neighbor Responses	The number of responses sent to the neighbor mesh access points.
	Parent Changes Count	The number of times a mesh access point (child) moves to another parent.
	Neighbor Timeouts Count	The number of neighbor timeouts.
Queue Stats	Gold Queue	The average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval.
	Silver Queue	The average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval.
	Platinum Queue	The average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval.
	Bronze Queue	The average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval.
	Management Queue	The average and peak number of packets waiting in the management queue during the defined statistics time interval.

Table 8-7 Mesh Access Point Statistics (continued)

Statistics	Parameter	Description
Mesh Node Security Stats	Transmitted Packets	The number of packets transmitted during security negotiations by the selected mesh access point.
	Received Packets	The number of packets received during security negotiations by the selected mesh access point.
	Association Request Failures	The number of association request failures that occur between the selected mesh access point and its parent.
	Association Request Timeouts	The number of association request timeouts that occur between the selected mesh access point and its parent.
	Association Requests Successful	The number of successful association requests that occur between the selected mesh access point and its parent.
	Authentication Request Failures	The number of failed authentication requests that occur between the selected mesh access point and its parent.
	Authentication Request Timeouts	The number of authentication request timeouts that occur between the selected mesh access point and its parent.
	Authentication Requests Successful	The number of successful authentication requests between the selected mesh access point and its parent.
	Reassociation Request Failures	The number of failed reassociation requests between the selected mesh access point and its parent.
	Reassociation Request Timeouts	The number of reassociation request timeouts between the selected mesh access point and its parent.
	Reassociation Requests Successful	The number of successful reassociation requests between the selected mesh access point and its parent.
	Reauthentication Request Failures	The number of failed reauthentication requests between the selected mesh access point and its parent.
	Reauthentication Request Timeouts	The number of reauthentication request timeouts that occur between the selected mesh access point and its parent.
	Reauthentication Requests Successful	The number of successful reauthentication requests that occur between the selected mesh access point and its parent.
	Unknown Association Requests	The number of unknown association requests received by the parent mesh access point from its child. The unknown association requests often occur when a child is an unknown neighbor mesh access point.
	Invalid Association Requests	The number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This state may occur when the selected child is a valid neighbor but is not in a state that allows association.

Table 8-7 Mesh Access Point Statistics (continued)

Statistics	Parameter	Description
Mesh Node Security Stats (continued)	Unknown Reauthentication Requests	The number of unknown reauthentication requests received by the parent mesh access point node from its child. This state may occur when a child mesh access point is an unknown neighbor.
	Invalid Reauthentication Requests	The number of invalid reauthentication requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reauthentication.
	Unknown Reassociation Requests	The number of unknown reassociation requests received by the parent mesh access point from a child. This state may occur when a child mesh access point is an unknown neighbor.
	Invalid Reassociation Requests	The number of invalid reassociation requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reassociation.

Using the CLI to View Mesh Statistics for an Access Point

Use these commands to view mesh statistics for a specific access point using the controller CLI.

- To view packet error statistics; a count of failures, timeouts, association and authentication successes; and reassociations and reauthentications for a specific access point, enter this command:

  show mesh security-stats *Cisco_AP*

  Information similar to the following appears:

```
AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
-----------------------------
x Packets 14, Rx Packets 19, Rx Error Packets 0

Parent-Side Statistics:
--------------------------
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0

Child-Side Statistics:
--------------------------
Association Failures 0
Association Timeouts 0
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Association Failures 0
Re-Association Timeouts 0
```

```
Re-Association Successes 0
Re-Authentication Failures 0
Re-Authentication Timeouts 0
Re-Authentication Successes 0
```

- To view the number of packets in the queue by type, enter this command:

  show mesh queue-stats *Cisco_AP*

  Information similar to the following appears:

```
Queue Type  Overflows  Peak length  Average length
 ----------  ---------  -----------  --------------
 Silver      0          1            0.000
 Gold        0          4            0.004
 Platinum    0          4            0.001
 Bronze      0          0            0.000
 Management  0          0            0.000
```

  Overflows—The total number of packets dropped because of 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 an Access Point

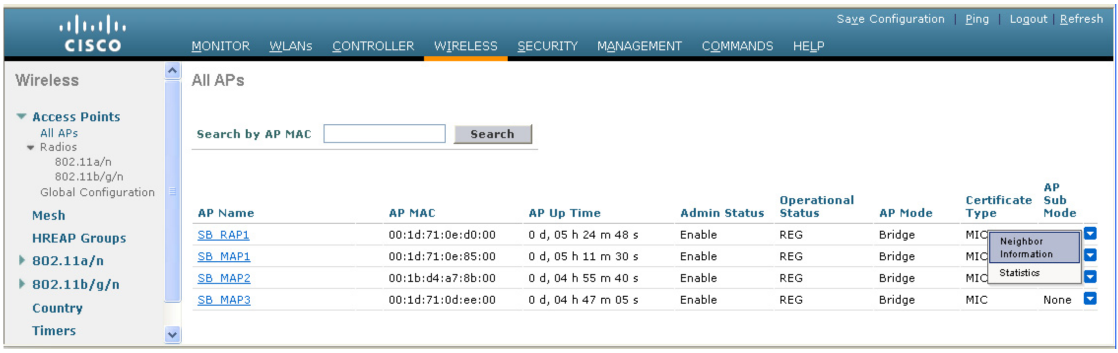
This section explains how to use the controller GUI or CLI to view neighbor statistics for a selected access point. It also describes how to run a link test between the selected access point and its parent.

Using the GUI to View Neighbor Statistics for an Access Point

Using the controller GUI, follow these steps to view neighbor statistics for an access point.

Step 1 Click **Wireless** > **Access Points** > **All APs** to open the All APs page (see Figure 8-20).

Figure 8-20 All APs Page



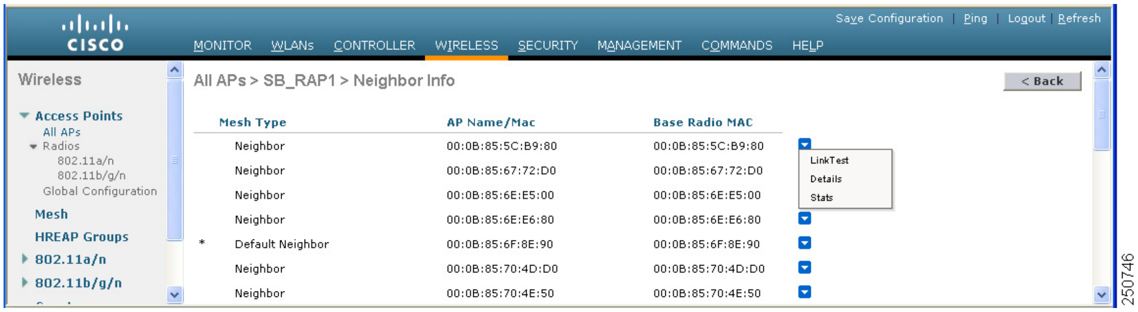
All APs

Search by AP MAC

AP Name	AP MAC	AP Up Time	Admin Status	Operational Status	AP Mode	Certificate Type	AP Sub Mode
SB_RAP1	00:1d:71:0e:d0:00	0 d, 05 h 24 m 48 s	Enable	REG	Bridge	MIC	
SB_MAP1	00:1d:71:0e:85:00	0 d, 05 h 11 m 30 s	Enable	REG	Bridge	MIC	
SB_MAP2	00:1b:d4:a7:8b:00	0 d, 04 h 55 m 40 s	Enable	REG	Bridge	MIC	
SB_MAP3	00:1d:71:0d:ee:00	0 d, 04 h 47 m 05 s	Enable	REG	Bridge	MIC	None

Step 2 To view neighbor statistics for a specific access point, hover your cursor over the blue drop-down arrow for the desired access point and choose **Neighbor Information**. The All APs > *Access Point Name* > Neighbor Info page for the access point appears (see Figure 8-21).

Figure 8-21 All APs > Access Point Name > Neighbor Info Page



All APs > SB_RAP1 > Neighbor Info

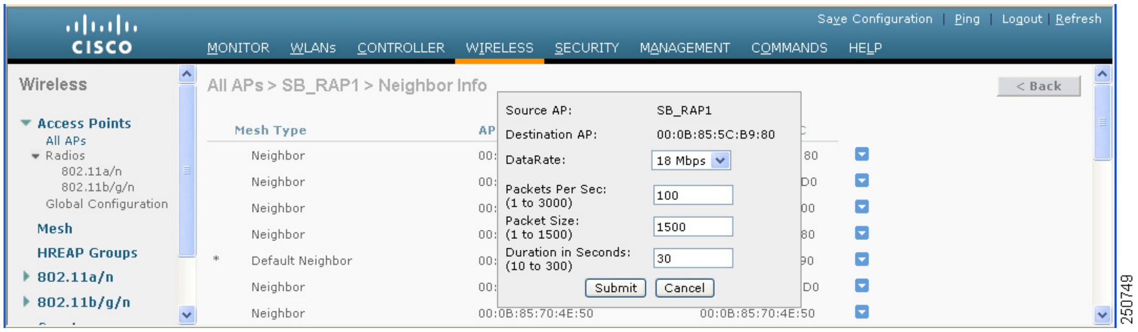
Mesh Type	AP Name/Mac	Base Radio MAC
Neighbor	00:0B:85:5C:B9:80	00:0B:85:5C:B9:80
Neighbor	00:0B:85:67:72:D0	00:0B:85:67:72:D0
Neighbor	00:0B:85:6E:E5:00	00:0B:85:6E:E5:00
Neighbor	00:0B:85:6E:E6:80	00:0B:85:6E:E6:80
* Default Neighbor	00:0B:85:6F:8E:90	00:0B:85:6F:8E:90
Neighbor	00:0B:85:70:4D:D0	00:0B:85:70:4D:D0
Neighbor	00:0B:85:70:4E:50	00:0B:85:70:4E:50

This page lists the parent, children, and neighbors of the access point. It provides each access point's name and radio MAC address.

Step 3 To perform a link test between the access point and its parent or children, follow these steps:

a. Hover your cursor over the blue drop-down arrow of the parent or child and choose **LinkTest**. A pop-up window appears (see Figure 8-22).

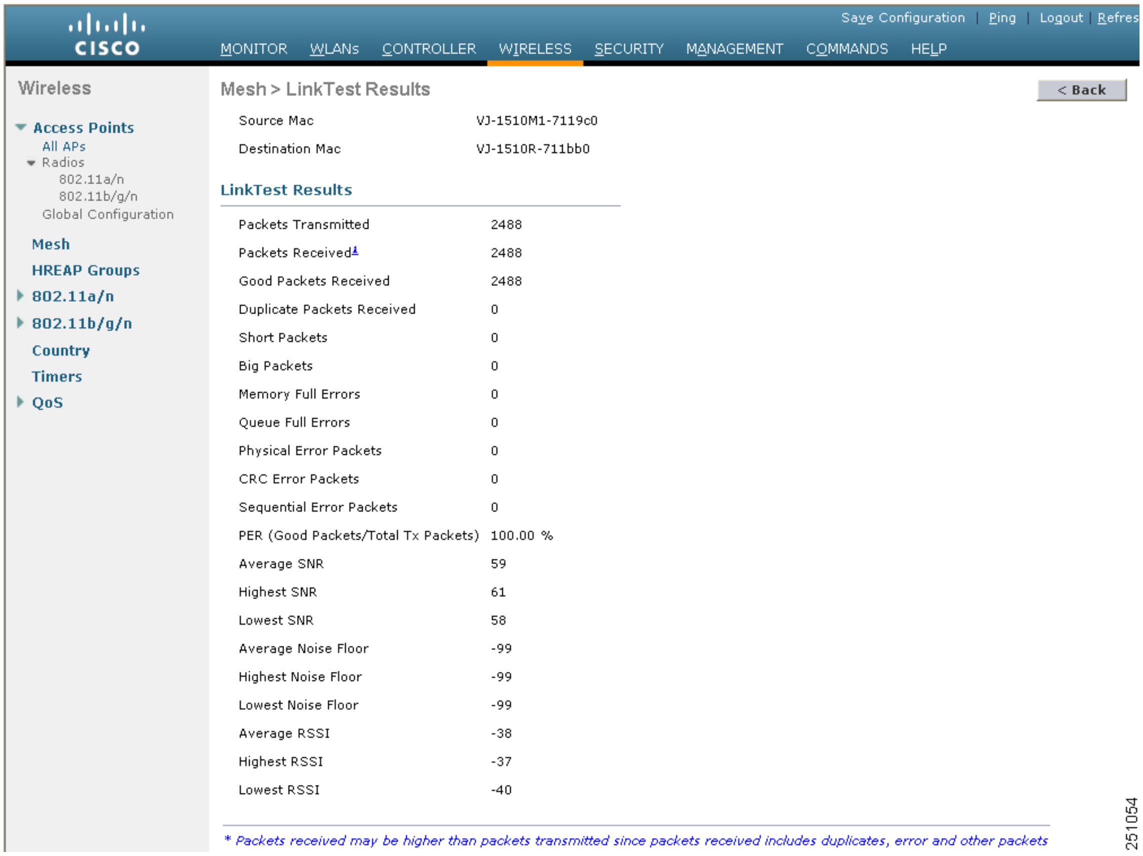
Figure 8-22 Link Test Window



Source AP: SB_RAP1
Destination AP: 00:0B:85:5C:B9:80
DataRate: 18 Mbps
Packets Per Sec: (1 to 3000) 100
Packet Size: (1 to 1500) 1500
Duration in Seconds: (10 to 300) 30

b. Click **Submit** to start the link test. The link test results appear on the Mesh > LinkTest Results page (see Figure 8-23).

Figure 8-23 Mesh > LinkTest Results Page



Mesh > LinkTest Results

Source Mac	VJ-1510M1-7119c0
Destination Mac	VJ-1510R-711bb0

LinkTest Results

Packets Transmitted	2488
Packets Received[1]	2488
Good Packets Received	2488
Duplicate Packets Received	0
Short Packets	0
Big Packets	0
Memory Full Errors	0
Queue Full Errors	0
Physical Error Packets	0
CRC Error Packets	0
Sequential Error Packets	0
PER (Good Packets/Total Tx Packets)	100.00 %
Average SNR	59
Highest SNR	61
Lowest SNR	58
Average Noise Floor	-99
Highest Noise Floor	-99
Lowest Noise Floor	-99
Average RSSI	-38
Highest RSSI	-37
Lowest RSSI	-40

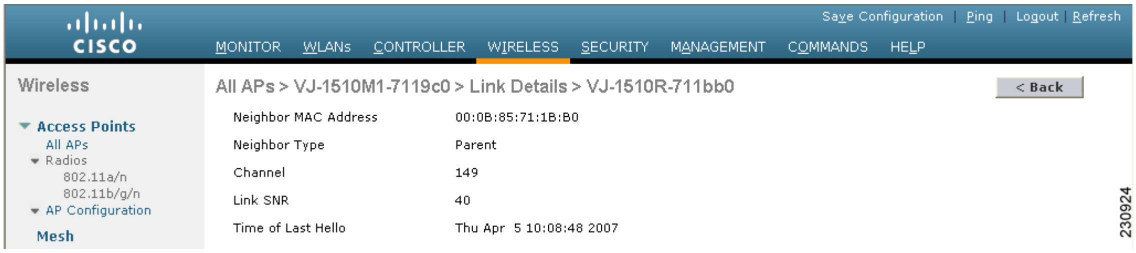
* Packets received may be higher than packets transmitted since packets received includes duplicates, error and other packets

c. Click **Back** to return to the All APs > *Access Point Name* > Neighbor Info page.

Step 4 To view the details for any of the access points on this page, follow these steps:

a. Hover your cursor over the blue drop-down arrow for the desired access point and choose **Details**. The All APs > *Access Point Name* > Link Details > *Neighbor Name* page appears (see Figure 8-24).

Figure 8-24 All APs > Access Point Name > Link Details > Neighbor Name Page



All APs > VJ-1510M1-7119c0 > Link Details > VJ-1510R-711bb0

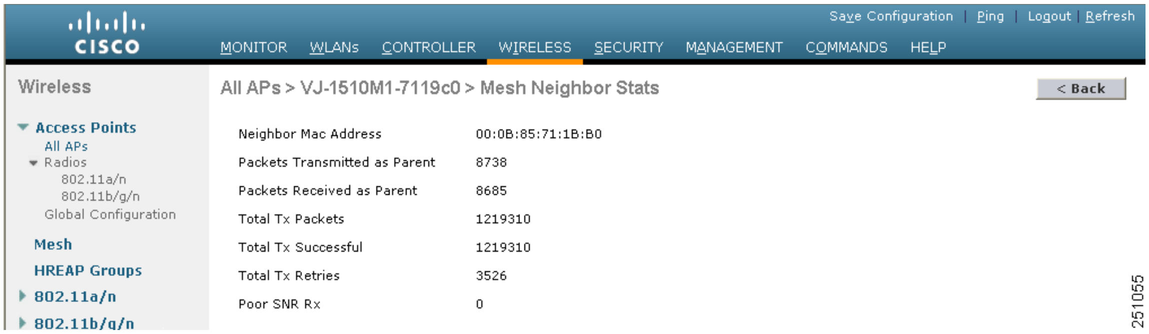
Neighbor MAC Address	00:0B:85:71:1B:B0
Neighbor Type	Parent
Channel	149
Link SNR	40
Time of Last Hello	Thu Apr 5 10:08:48 2007

b. Click **Back** to return to the All APs > *Access Point Name* > Neighbor Info page.

Step 5 To view statistics for any of the access points on this page, follow these steps:

a. Hover your cursor over the blue drop-down arrow for the desired access point and choose **Stats**. The All APs > *Access Point Name* > Mesh Neighbor Stats page appears (see Figure 8-25).

Figure 8-25   All APs > Access Point Name > Mesh Neighbor Stats Page



All APs > VJ-1510M1-7119c0 > Mesh Neighbor Stats

Neighbor Mac Address	00:0B:85:71:1B:B0
Packets Transmitted as Parent	8738
Packets Received as Parent	8685
Total Tx Packets	1219310
Total Tx Successful	1219310
Total Tx Retries	3526
Poor SNR Rx	0

b. Click **Back** to return to the All APs > *Access Point Name* > Neighbor Info page.

Using the CLI to View Neighbor Statistics for an Access Point

Use these commands to view neighbor statistics for a specific access point.

- To view the mesh neighbors for a specific access point, enter this command:

  show mesh neigh {detail | summary} *Cisco_AP*

  Information similar to the following appears when you request a summary display:

```
AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags State
-----------------  ------- ------ -------- -------- ------ -------
mesh-45-rap1       165     15     18       16       0x86b  UPDATED NEIGH PARENT BEACON
00:0B:85:80:ED:D0  149      5      6        5       0x1a60 NEED UPDATE BEACON DEFAULT
00:17:94:FE:C3:5F  149      7      0       0        0x860     BEACON
```

- To view the channel and signal-to-noise ratio (SNR) details for a link between an access point and its neighbor, enter this command:

  show mesh path *Cisco_AP*

  Information similar to the following appears:

```
AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags State
-----------------  ------- ------ -------- -------- ------ -------
mesh-45-rap1       165     15     18       16       0x86b UPDATED NEIGH PARENT BEACON
mesh-45-rap1 is a Root AP.
```

- To view the percentage of packet errors for packets transmitted by the neighbor mesh access point, enter this command:

  show mesh per-stats *Cisco_AP*

  Information similar to the following appears:

```
Neighbor MAC Address 00:0B:85:5F:FA:F0
Total Packets transmitted: 104833
Total Packets transmitted successfully: 104833
Total Packets retried for transmission: 33028

Neighbor MAC Address 00:0B:85:80:ED:D0
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
```

```
Neighbor MAC Address 00:17:94:FE:C3:5F
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
```

Note Packet error rate percentage = 1 – (number of successfully transmitted packets/number of total packets transmitted).

Converting Indoor Access Points to Mesh Access Points (1130AG, 1240AG)

Before you can install an 1130AG or 1240AG indoor access point into an indoor mesh deployment, you must do the following.

1. Convert the autonomous access point (k9w7 image) to a lightweight access point.

   A detailed explanation of this process is located at:

   http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00804fc3dc.html

2. Convert the lightweight access point to either a mesh access point (MAP) or root access point (RAP).

   Indoor mesh access points (1130 and 1240) can function as either a RAP or a MAP. By default, all are configured as MAPs.

   At least one access point within a mesh network must be configured to function as a RAP.

   - To convert the access point to a mesh access point using the CLI, perform one of the following:
     - To convert from a lightweight access point to a mesh access point, enter the following CLI commands:

       config ap mode bridge *Cisco_AP*

       The mesh access point reloads.

     - To convert from a lightweight access point to a RAP, enter the following 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 menu.

        The access point reboots.

     c. At the Mesh panel, select either RootAP or MeshAP from the AP Role drop- down menu.

     d. Click **Apply** and **Save Configuration**.

Changing MAP and RAP Roles for Indoor Mesh Access Points (1130AG, 1240AG)

Cisco 1130 and 1240 series indoor mesh access points can function as either RAPs or MAPs.

Using the GUI to Change MAP and RAP Roles for Indoor Mesh Access Points

Using the controller GUI, follow these steps to change an indoor mesh access point from one role to another.

Step 1 Click **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 box, 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 Cisco recommends 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. It is the responsibility of the user to 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 The recommended power source for MAPs is either a power supply or power injector. PoE is not a recommended power source for MAPs.

Using the CLI to Change MAP and RAP Roles for Indoor Mesh Access Points

Using the controller CLI, follow these steps to change an indoor mesh access point from one role to another.

Step 1 To change the role of an indoor access point from MAP to RAP or from RAP to MAP, enter this command:

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

The access point reboots after you change the role.

Step 2 To save your changes, enter this command:

save config

Converting Indoor Mesh Access Points to Non-Mesh Lightweight Access Points (1130AG, 1240AG)

The access point reboots after entry of the conversion commands (noted below).

Note A Fast Ethernet connection to the controller for the conversion from a mesh (bridge) to non-mesh (local) access point is recommended. If the backhaul is a radio, after the conversion you must enable Ethernet and then reload the access image. After the reload and reboot the backhaul is Fast Ethernet.

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. Consequently, 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 non-mesh lightweight access point using the CLI, enter the following command.

  config ap mode local *Cisco_AP*

  The access point reloads.

- To convert an indoor mesh access point (MAP or RAP) to a non-mesh lightweight access point using the GUI, follow these steps:

  a. Click **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, select **Local** from the AP Mode drop-down menu.

  c. Click **Apply** and **Save Configuration**.

- To convert an indoor mesh access point (MAP or RAP) to a non-mesh lightweight access point using Cisco WCS, follow these steps:

  a. Click **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, select **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, 1524) 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 5.8-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 allows data collected from in-vehicle deployments such as a police cars to 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, refer to Table 8-8.

Table 8-8 Mesh Access Points and MAR 3200 Interoperability

Mesh Access Point Model	MAR Model
1522[1]	c3201[2], c3202[3], c3205[4]
1524	c3201, c3202
1130, 1240 configured as indoor mesh access points with universal access	c3201, c3205

[1] Universal access must be enabled on the 1522 if connecting to a MAR on the 802.11a radio or 4.9-GHz band.

[2] Model c3201 is a MAR with a 802.11b/g radio (2.4 GHz).

[3] Model c3202 is a MAR with a 4-9-GHz sub-band radio.

[4] Model c3205 is a MAR with a 802.11a radio (5.8-GHz sub-band).

Configuration Guidelines

For the 1522 or 1524 mesh access point and Cisco MAR 3200 to interoperate on the public safety network, the following configuration guidelines must be met:

- 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 1524 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.

The default channel width for MAR 3200s is 5 MHz. You must *either* change the channel width to 10 or 20 MHz to enable WGBs to associate with series 1520 mesh access points *or* change the channel on the 1522 or 1524 to a channel in the 5-MHz (channels 1 to 10) or 10-MHz band (channels 11 through 19).

- When using the CLI, you must disable the 802.11a radio prior to configuring its channels. You re-enable the radio after the channels are configured.
- When using the GUI, enabling and disabling of the 802.11a radio for channel configuration is not required.
- Cisco MAR 3200s can scan channels *within* but not across the 5-, 10-, or 20-MHz bands.

Using the GUI to Enable Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers

Using the controller GUI, follow these steps to enable the 1522 and 1524 mesh access points to associate to the Cisco 3200 series MAR.

Step 1 To enable the backhaul for client access, click **Wireless** > **Mesh** to open the Mesh page.

Step 2 Check the **Backhaul Client Access** check box to allow wireless client association over the 802.11a radio.

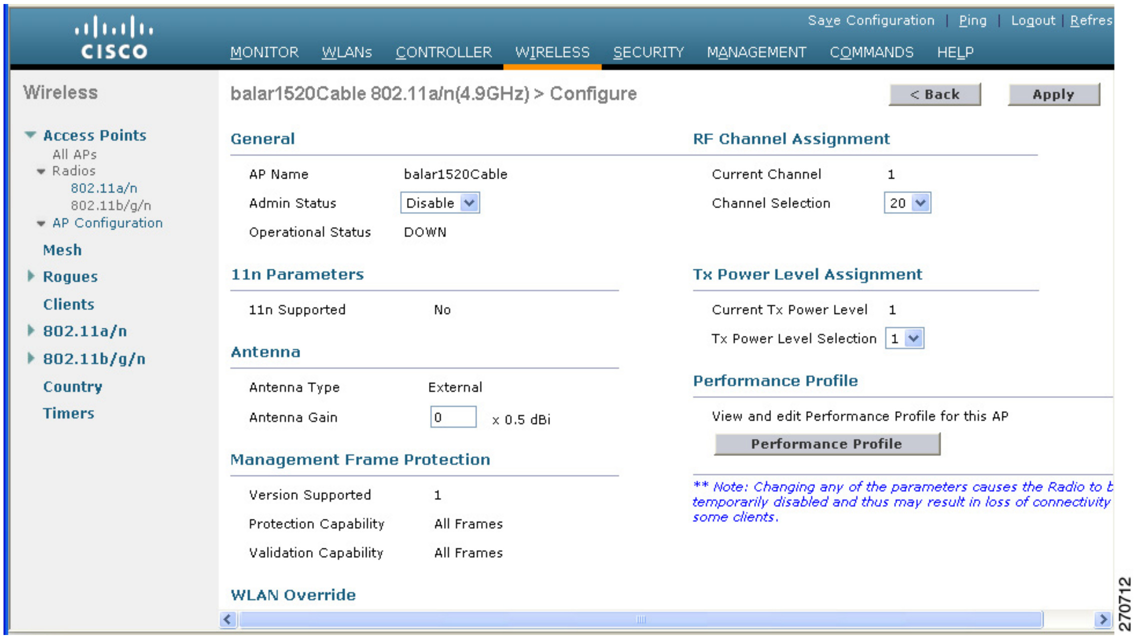
Step 3 Click **Apply** to commit your changes.

Step 4 When prompted to allow a reboot of all the mesh access points on the network, click **OK**.

Step 5 Click **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 (see Figure 8-26).

Figure 8-26 802.11 a/n (4.9GHz) > Configure Page



balar1520Cable 802.11a/n(4.9GHz) > Configure

General

AP Name	balar1520Cable
Admin Status	Disable
Operational Status	DOWN

11n Parameters

11n Supported	No

Antenna

Antenna Type	External
Antenna Gain	0 x 0.5 dBi

Management Frame Protection

Version Supported	1
Protection Capability	All Frames
Validation Capability	All Frames

RF Channel Assignment

Current Channel	1
Channel Selection	20

Tx Power Level Assignment

Current Tx Power Level	1
Tx Power Level Selection	1

Performance Profile

View and edit Performance Profile for this AP

** Note: Changing any of the parameters causes the Radio to b temporarily disabled and thus may result in loss of connectivity some clients.

Step 7 Under the RF Channel Assignment section, choose the **Custom** option for Assignment Method and a channel between 1 and 26.

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your changes.

Using the CLI to Enable Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers

Using the controller CLI, follow these steps to enable the 1522 and 1524 mesh access points to associate to the Cisco 3200 series MAR.

Step 1 To enable client access mode on the 1522 and 1524 mesh access points, enter this command:

config mesh client-access enable

Step 2 To enable 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:

- 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 1524, 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 **config 802.11–a58 enable** *Cisco_MAP* to enable a 5.8-GHz radio.

Note For both the 1522 and 1524 mesh access points, *channel_number* is equal to a value between 1 and 26 (inclusive).

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 (for 1522 access points only)

show ap config 802.11–a49 summary (for 1524 access points only)

Note Enter **show config 802.11-a58 summary** to view configuration details for a 5.8-GHz radio.

CHAPTER 9

Managing Controller Software and Configurations

This chapter describes how to manage configurations and software versions on the controllers. It contains these sections:

- Upgrading Controller Software, page 9-2
- Transferring Files to and from a Controller, page 9-13
- Saving Configurations, page 9-26
- Editing Configuration Files, page 9-27
- Clearing the Controller Configuration, page 9-28
- Erasing the Controller Configuration, page 9-28
- Resetting the Controller, page 9-28

Upgrading 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.

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, 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 5.2.157.0, the WLAN override feature has been removed from both the controller GUI and CLI. If your controller is configured for WLAN override and you upgrade to controller software release 5.2.157.0, 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 for Upgrading Controller Software

Follow these guidelines before upgrading your controller to software release 5.2:

- Make sure you have a TFTP or FTP server available for the software upgrade. Keep these guidelines in mind when setting up a TFTP or FTP server:
  - Controller software release 5.2 is greater than 32 MB; therefore, 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 within WCS. If you attempt to download the 5.2 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 5.2. Table 9-1 shows the upgrade path that you must follow prior to downloading software release 5.2.

Table 9-1 Upgrade Path to Controller Software Release 5.2

Current Software Release	Upgrade Path to 5.2 Software
3.2.78.0 or later 3.2 release	First upgrade to a 4.1 release and then upgrade to 4.2.176.0 before upgrading to 5.2.
4.0.155.5 or later 4.0 release	Upgrade to 4.2.176.0 before upgrading to 5.2.
4.1.171.0 or later 4.1 release	Upgrade to 4.2.176.0 before upgrading to 5.2.
4.1.191.xM or 4.1.192.xM	You can upgrade directly to 5.2.
4.2.61.0, 4.2.99.0, or 4.2.112.0	Upgrade to 4.2.176.0 or to a 5.1 release before upgrading to 5.2.
4.2.130.0	Upgrade to 4.2.176.0 before upgrading to 5.2.
4.2.173.0 or 4.2.176.0	You can upgrade directly to 5.2.
5.0.148.0 or later 5.0 release	You can upgrade directly to 5.2.
5.1.151.0 or later 5.1 release	You can upgrade directly to 5.2.

Note 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 5.2 software. In large networks, it may take some time to download the software on each access point.

- Cisco recommends 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** CLI 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 Field Recovery Image Version field in the output of this command.

Note 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 (5.2.157.0 ER.aes) ensures that the boot software modifications in all of the previous and current boot software ER.aes files are installed.

Caution 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.

Guidelines for Upgrading to Controller Software 5.2 in Mesh Networks

Caution Before upgrading your controller to software release 5.2 in a mesh network, you must comply with the following rules.

Mandatory Boot Variable Update for Networks with 1522 Access Points

If your network is operating with 1520 series access points or you plan to install 1522 access points in your network, you must set the boot variable on the access point before upgrading from software release 4.1.190.5 to 4.1.192.35M or installing a 1520 series access point in a 4.1.192.35M or 5.2 or later network. Updating the boot variable ensures that the 1522 access point joins correctly.

Note You should check the boot variable setting before updating the boot.

- If the boot system image is visible, then no boot variable update is required.
  - If upgrading from software release 4.1.190.5, the system image should read: flash:/c1520-k9w9-mx.124-3g.JMA1/c1520-k9w9-mx.124-3g.JMA1
- If the boot system image is missing, then you must update the boot variable.

Checking the Boot Variable Setting

Follow these steps to check the setting of the boot variable.

Step 1 On the controller CLI, enter these commands for each mesh access point:

debug ap enable *ap_name*

debug ap command "more flash:/env_vars" *Cisco_MAP*

Information similar to the following appears:

```
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: 5G_RADIO_CARRIER_SET=0020
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: 5G_RADIO_ENCRYPTION_CONFIG=02
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: 5G_RADIO_MAX_TX_POWER=65535
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f:
BOOT=flash:/c1520-k9w9-mx.124-3g.JMA1/c1520-k9w9-mx.124-3g.JMA1
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: DEFAULT_ROUTER=11.200.9.20
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: DEVIATION_NUM=0
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: DOT11G_RADIO_MODE=255
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: DOT11_DEVICE_TYPE=4C
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: DOT11_ENCRYPTION_CONFIG=02
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: DOT11_MAX_ASSOCIATION_NUM=2007
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: ENABLE_BREAK=yes
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: FAB_PART_NUM=800-28909-02
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: IP_ADDR=11.200.9.99
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: MAC_ADDR=00:1d:e5:e8:aa:00
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: MAC_ADDR_BLOCK_SIZE=256
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: MANUAL_BOOT=no
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: NETMASK=255.255.0.0
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: NEW_IMAGE=yes
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PCA_ASSY_NUM_800=03 20 00 70 ED 02
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PCA_PART_NUM_73=49 2A A6 02
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PCA_REVISION_NUM=A0
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PCA_REVISION_NUM_800=A0
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PCB_SERIAL_NUM=FHH1101007F
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PEP_PRODUCT_ID=AIR-LAP1521AG-A-K9
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PEP_VERSION_ID=V01
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PRODUCT_MODEL_NUM=AIR-LAP1521AG-A-K9
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: RADIO_CARRIER_SET=00FF
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: RADIO_MAX_TX_POWER=65535
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: SYSTEM_REVISION_NUM_800=A0
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: TOP_ASSY_NUM_800=03 20 00 71 22 02
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: TOP_ASSY_SERIAL_NUM=SJC1101007F
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: param-any=
```

Step 2 To turn off debug access, enter **debug ap disable** *ap_name*.

Note You do not need to turn off the debug access at this point if a boot update is required. Continue to the "Updating the Boot Variable" section on page 9-5.

Updating the Boot Variable

Follow these steps to update the boot variable on a 1520 series access point prior to a software upgrade.

Step 1 On the controller CLI, enter these commands for each mesh access point:

debug ap enable *Cisco_MAP*

debug ap command "debug lwapp con cli" *Cisco_MAP*

debug ap command "test mesh enable telnet" *Cisco_MAP*

show ap config general *Cisco_MAP*

Note Find the IP address for the access point in the **show ap config general** *ap_name* command and continue to Step 2.

Step 2 Telnet to the access point using the IP address identified in Step 1 by entering this command:

telnet *IP_address*

Step 3 From the AP console, enter these commands:

enable

debug lwapp console cli

show version

Look for the system image as noted in the example below:

```
System image file is “flash:/c1520-k9w9-mx.124-3g.JMA1/c1520-k9w9-mx.124-3g.JMA1”
```

Enter the image name (enclosed within quotes) into the **boot system**... command below.

config term

boot system flash:/c1520-k9w9-mx.124-3g.JMA1/c1520-k9w9-mx.124-3g.JMA1

Note The system image entered in the **boot system** *image_name* command must match the version identified in the **show version** command.

exit

Enter the following command to verify that you typed the image string correctly.

more flash:/env_vars *Cisco_MAP*

Step 4 Disconnect Telnet.

Upgrade Compatibility Matrix

Table 2 outlines the upgrade compatibility of controller mesh and non-mesh releases and indicates the intermediate software releases required as part of the upgrade path.

Software Upgrade Notes

- You can upgrade from all mesh releases to controller software release 5.2 without any configuration file loss.

Note If you downgrade to a mesh release, you must then reconfigure the controller. Cisco recommends that you save the configuration from the mesh release before upgrading to release 5.2 for the first time. Then you can reapply the configuration if you need to downgrade.

- You cannot downgrade from controller software release 5.2 to a mesh release (4.1.190.5, 4.1.191.22M, or 4.1.192.xxM) without experiencing a configuration loss.
- Configuration files are in the binary state immediately after upgrade from a mesh release to controller software release 5.2. After reset, the XML configuration file is selected.
- Do not edit XML files.
- Any field with an invalid value is filtered out and set to default by the XML validation engine. Validation occurs during bootup.

Table 2 Upgrade Compatibility Matrix for Controller Mesh and Non-Mesh Releases

Upgrade to	5.2	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	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	3.2.116.21	3.2.78.0	3.1.111.0	3.1.105.0
Upgrade from																									
4.1.192.35M	Y																								
4.1.192.22M	Y	Y																							
4.1.191.24M		Y	–																						
4.1.190.5		Y[1]	Y	–																					
4.1.185.0			Y	Y[2]	–																				
4.1.181.0				Y[2]	Y[2]																				
4.1.171.0				Y[2]	Y[2]	–																			
4.0.219.0					Y[2]	Y[2]	–																		
4.0.217.204			Y[2]		Y[2]	Y[2]	Y[2]	–																	
4.0.217.0					Y[2]	Y[2]	Y[2]	Y[3]	–																
4.0.216.0					Y[2]	Y[2]	Y[2]	Y[3]	Y	–															
4.0.206.0					Y[2]	Y[2]	Y[2]	Y[3]	Y		–														
4.0.179.11									Y		Y[4]	–													
4.0.179.8									Y		Y[4]	Y	–												
4.0.155.5									Y		Y[4]	Y	Y	–											
4.0.155.0									Y		Y[4]	Y	Y	Y	–										
3.2.195.10									Y		Y[4]	Y	Y	Y		–									
3.2.193.5									Y		Y[4]	Y	Y	Y		Y	–								
3.2.171.6									Y		Y[4]	Y	Y	Y		Y		–							
3.2.171.5									Y		Y[4]	Y	Y	Y		Y		Y	–						
3.2.150.10									Y		Y[4]	Y	Y	Y		Y		Y		–					
3.2.150.6									Y		Y[4]	Y	Y	Y		Y		Y		Y	–				
3.2.116.21									Y		Y[4]	Y	Y	Y		Y		Y		Y		–			
3.2.78.0									Y		Y[4]	Y	Y	Y		Y		Y		Y		Y	–		
3.1.111.0																Y		Y		Y		Y	Y	–	
3.1.105.0																Y		Y		Y		Y	Y	Y	–
3.1.59.24																Y		Y		Y		Y	Y	Y	Y

1. You can upgrade directly from software release 4.1.190.5 to 4.1.192.35M; however, upgrading to 4.1.191.24M before upgrading to 4.1.192.35M is highly recommended.
2. CUSTOMERS WHO REQUIRE DYNAMIC FREQUENCY SELECTION (DFS) FUNCTIONALITY SHOULD NOT USE THIS RELEASE. This release does not provide DFS functionality fixes found in release 4.0.217.204. Additionally, this release is not supported in ETSI-compliant countries or Singapore.
3. Release 4.0.217.204 provides fixes for DFS on 1510 series access points. This functionality is needed only in countries where DFS rules apply.

4. An upgrade to 4.0.206.0 is not allowed in the following country codes when operating with the following access points: Australia (1505 and 1510), Brazil (1505 and 1510), Hong Kong (1505 and 1510), India (1505 and 1510), Japan (1510), Korea (1505 and 1510), Mexico (1505 and 1510), New Zealand (1505 and 1510), and Russia (1505 and 1510). Note: The 1505 mesh access point is not supported in release 5.0 and later. The 1510 mesh access point is supported only in mesh releases 4.1.190.5, 4.1.191.22M, and 4.1.192.xxM.

Using the GUI to Upgrade Controller Software

Follow these steps to upgrade the controller software using the GUI.

Note Do not install the 5.2 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; then install the other file and reboot the controller.

Step 1 Upload your controller configuration files to a server to back them up.

Note Cisco highly recommends that you back up your controller's configuration files prior to upgrading the controller software. See the "Uploading and Downloading Configuration Files" section on page 9-21 for instructions.

Step 2 Follow these steps to obtain the 5.2 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:

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

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

b. Click **Wireless Software**.

c. Click **Wireless LAN Controllers**.

d. Click **Standalone Controllers** or **Integrated Controllers and Controller Modules**.

e. Click a controller series.

f. If necessary, click a controller model.

g. If you chose Standalone Controllers in Step d., click **Wireless LAN Controller Software**.

h. If you chose Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM) in Step e., click **Wireless Services Modules (WiSM) Software**.

i. Click 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 and new hardware platform support as well as bug fixes.
- **Maintenance Deployment (MD)**—These software releases provide bug fixes and ongoing software maintenance.
- **Deferred (DF)**—These software releases have been deferred. Cisco recommends that you migrate to an upgraded release.

j. Click 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 5.2 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.

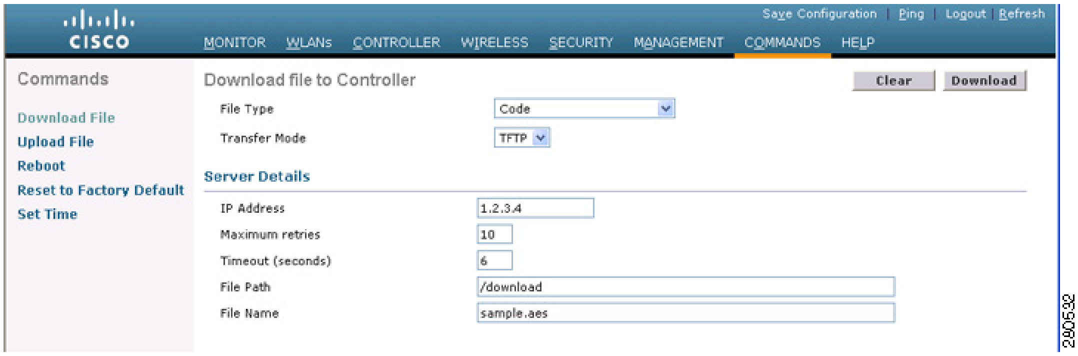
Step 4 Disable the controller 802.11a and 802.11b/g networks.

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.

Step 7 Click **Commands** > **Download File** to open the Download File to Controller page (see Figure 9-1).

Figure 9-1 Download File to Controller Page



Download file to Controller

File Type: Code

Transfer Mode: TFTP

Server Details

IP Address: 1.2.3.4

Maximum retries: 10

Timeout (seconds): 6

File Path: /download

File Name: sample.aes

Step 8 From the File Type drop-down box, choose **Code**.

Step 9 From the Transfer Mode drop-down box, choose **TFTP** or **FTP**.

Step 10 In the IP Address field, enter the IP address of the TFTP or FTP server.

Step 11 If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields 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 in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the software in the Timeout field.

Step 12 In the File Path field, enter the directory path of the software.

Step 13 In the File Name field, enter the name of the controller software file (*filename*.aes).

Step 14 If you are using an FTP server, follow these steps:

a. In the Server Login Username field, enter the username to log into the FTP server.

b. In the Server Login Password field, enter the password to log into the FTP server.

c. In the Server Port Number field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 15 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Step 16 After the download is complete, click **Reboot**.

Step 17 If prompted to save your changes, click **Save and Reboot**.

Step 18 Click **OK** to confirm your decision to reboot the controller.

Step 19 After the controller reboots, repeat Step 7 to Step 18 to install the remaining file (either the 5.2 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 20 Re-enable the WLANs.

Step 21 For Cisco WiSMs, re-enable the controller port channel on the Catalyst switch.

Step 22 Re-enable your 802.11a and 802.11b/g networks.

Step 23 If desired, reload your latest configuration file to the controller.

Step 24 To verify that the 5.2 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 25 To verify that the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file is installed on your controller, enter the **show sysinfo** command on the controller CLI and look at the Field Recovery Image Version field.

Note If you do not install the 5.2.157.0 ER.aes file, the Field Recovery Image Version field shows "N/A."

Using the CLI to Upgrade Controller Software

Follow these steps to upgrade the controller software using the CLI.

Note Do not install the 5.2 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; then install the other file and reboot the controller.

Step 1 Upload your controller configuration files to a server to back them up.

Note Cisco highly recommends that you back up your controller's configuration files prior to upgrading the controller software. See the "Uploading and Downloading Configuration Files" section on page 9-21 for instructions.

Step 2 Follow these steps to obtain the 5.2 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:

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

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

b. Click **Wireless Software**.

c. Click **Wireless LAN Controllers**.

d. Click **Standalone Controllers**, **Wireless Integrated Routers**, or **Wireless Integrated Switches**.

e. Click the name of a controller.

f. Click **Wireless LAN Controller Software**.

g. Click 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 5.2 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 **ping** *server-ip-address* to verify that the controller can contact the TFTP or FTP server.

Step 9 Enter **transfer download start** and 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 Enter these commands to change the download settings, if necessary:

- **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 Solarwinds 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 Enter **transfer download start** to view the updated settings and 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.
```

Step 12 Enter **reset system** to save the code update to non-volatile NVRAM and reboot the controller. The controller completes the bootup process.

Step 13 After the controller reboots, repeat Step 9 to Step 12 to install the remaining file (either the 5.2 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 14 Enter **config wlan enable** *wlan_id* to re-enable the WLANs.

Step 15 For Cisco WiSMs, re-enable the controller port channel on the Catalyst switch.

Step 16 Re-enable your 802.11a and 802.11b/g networks.

Step 17 If desired, reload your latest configuration file to the controller.

Step 18 To verify that the 5.2 controller software is installed on your controller, enter **show sysinfo** and look at the Product Version field.

Step 19 To verify that the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file is installed on your controller, enter the **show sysinfo** command on the controller CLI and look at the Field Recovery Image Version field.

Note If you do not install the 5.2.157.0 ER.aes file, the Field Recovery Image Version field shows "N/A."

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 Device Certificates, page 9-13
- Downloading CA Certificates, page 9-16
- Uploading PACs, page 9-19
- Uploading and Downloading Configuration Files, page 9-21

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 wish to use your own vendor-specific device certificate, it must be downloaded to the controller.

Note See the "Configuring Local EAP" section on page 5-38 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. Keep these guidelines in mind 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 All certificates downloaded to the controller must be in PEM format.

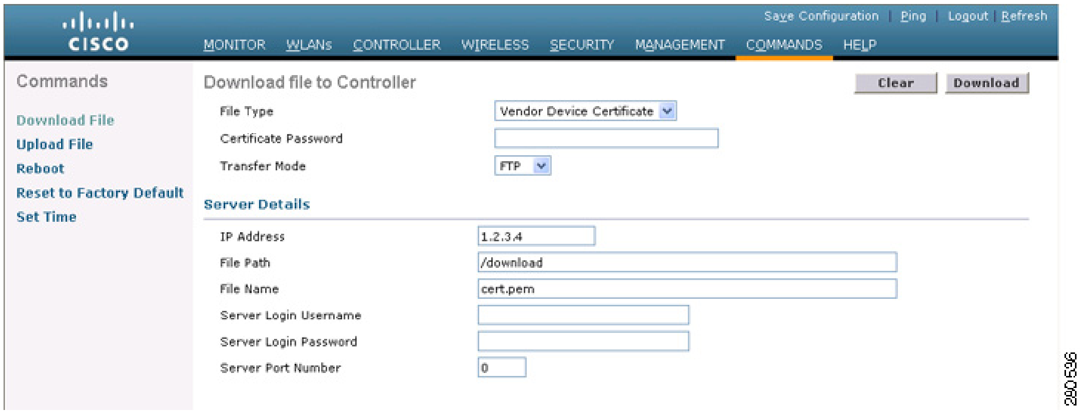
Using the GUI to Download Device Certificates

Follow these steps to download a device certificate to the controller using the controller GUI.

Step 1 Copy the device certificate to the default directory on your TFTP or FTP server.

Step 2 Click **Commands** > **Download File** to open the Download File to Controller page (see Figure 9-2).

Figure 9-2 Download File to Controller Page


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Commands
Download File
Upload File
Reboot
Reset to Factory Default
Set Time
Clear
Download
280536

Download file to Controller

File Type: Vendor Device Certificate

Certificate Password:

Transfer Mode: FTP

Server Details

IP Address: 1.2.3.4

File Path: /download

File Name: cert.pem

Server Login Username:

Server Login Password:

Server Port Number: 0

Step 3 From the File Type drop-down box, choose **Vendor Device Certificate**.

Step 4 In the Certificate Password field, enter the password that was used to protect the certificate.

Step 5 From the Transfer Mode drop-down box, choose **TFTP** or **FTP**.

Step 6 In the IP Address field, enter the IP address of the TFTP or FTP server.

Step 7 If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields 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 certificate in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout field.

Step 8 In the File Path field, enter the directory path of the certificate.

Step 9 In the File Name field, enter the name of the certificate.

Step 10 If you are using an FTP server, follow these steps:

a. In the Server Login Username field, enter the username to log into the FTP server.

b. In the Server Login Password field, enter the password to log into the FTP server.

c. In the Server Port Number field, 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, click **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.

Using the CLI to Download Device Certificates

Follow these steps to download a device certificate to the controller using the controller CLI.

Step 1 Log into the controller CLI.

Step 2 Enter **transfer download mode** {**tftp** | **ftp**}.

Step 3 Enter **transfer download datatype eapdevcert**.

Step 4 Enter **transfer download certpassword** *password*.

Step 5 Enter **transfer download serverip** *server-ip-address*.

Step 6 Enter **transfer download path** *server-path-to-file*.

Step 7 Enter **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*

Note The default value for the *port* parameter is 21.

Step 10 Enter **transfer download start** to view the updated settings; then answer **y** when prompted to confirm the current settings and start the download process. This example shows the download command output:

```
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/username/
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 Enter **reset system** to reboot the controller.

Step 12 After the controller reboots, enter **show certificates local-auth** to verify that the certificate is installed.

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 wish to use your own vendor-specific CA certificate, it must be downloaded to the controller.

Note See the "Configuring Local EAP" section on page 5-38 for information on configuring local EAP.

Follow the instructions in this section to download CA certificates 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. Keep these guidelines in mind 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 All certificates downloaded to the controller must be in PEM format.

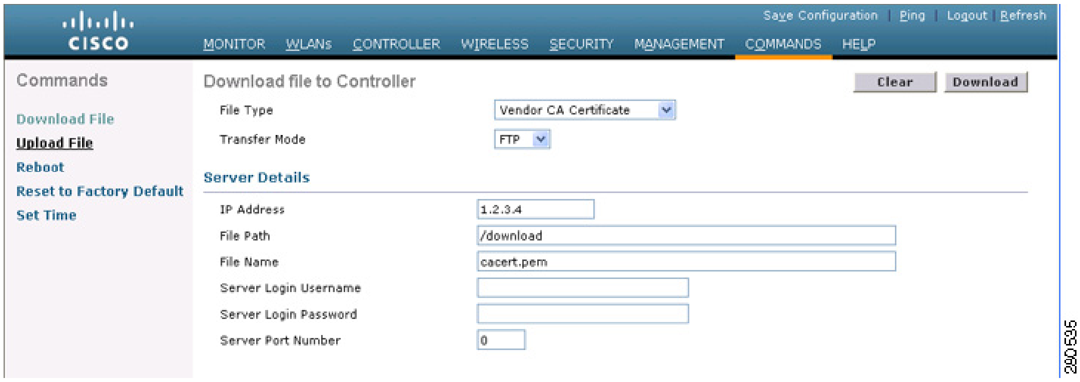
Using the GUI to Download CA Certificates

Follow these steps to download a CA certificate to the controller using the controller GUI.

Step 1 Copy the CA certificate to the default directory on your TFTP or FTP server.

Step 2 Click **Commands** > **Download File** to open the Download File to Controller page (see Figure 9-3).

Figure 9-3 Download File to Controller Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Commands
Download File
Upload File
Reboot
Reset to Factory Default
Set Time
Clear
Download
290535

Download file to Controller

File Type: Vendor CA Certificate

Transfer Mode: FTP

Server Details

IP Address: 1.2.3.4

File Path: /download

File Name: cacert.pem

Server Login Username:

Server Login Password:

Server Port Number: 0

Step 3 From the File Type drop-down box, choose **Vendor CA Certificate**.

Step 4 From the Transfer Mode drop-down box, choose **TFTP** or **FTP**.

Step 5 In the IP Address field, enter the IP address of the TFTP or FTP server.

Step 6 If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields 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 certificate in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout field.

Step 7 In the File Path field, enter the directory path of the certificate.

Step 8 In the File Name field, enter the name of the certificate.

Step 9 If you are using an FTP server, follow these steps:

a. In the Server Login Username field, enter the username to log into the FTP server.

b. In the Server Login Password field, enter the password to log into the FTP server.

c. In the Server Port Number field, 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, click **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.

Using the CLI to Download CA Certificates

Follow these steps to download a CA certificate to the controller using the controller CLI.

Step 1 Log into the controller CLI.

Step 2 Enter **transfer download mode** {**tftp** | **ftp**}.

Step 3 Enter **transfer download datatype eapcacert**.

Step 4 Enter **transfer download serverip** *server-ip-address*.

Step 5 Enter **transfer download path** *server-path-to-file*.

Step 6 Enter **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 Enter **transfer download start** to view the updated settings; then answer **y** when prompted to confirm the current settings and start the download process. This example shows the download command output:

```
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 Enter **reset system** to reboot the controller.

Step 11 After the controller reboots, enter **show certificates local-auth** to verify that the certificate is installed.

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 5-38 for information on configuring local EAP.

Follow the instructions in this section to generate and load PACs from the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP or FTP server available for the PAC upload. Keep these guidelines in mind when setting up a TFTP or FTP server:

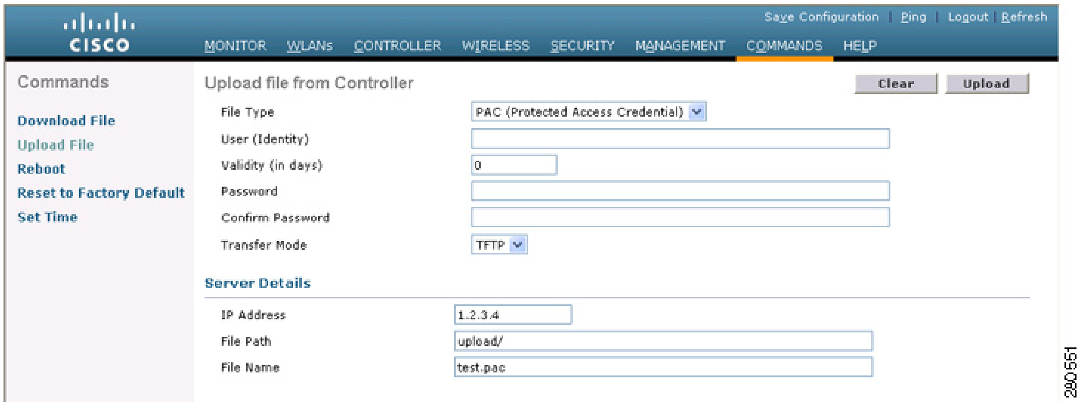
- If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are uploading through the distribution system network port, the TFTP or FTP server 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.

Using the GUI to Upload PACs

Follow these steps to upload a PAC from the controller using the controller GUI.

Step 1 Click **Commands** > **Upload File** to open the Upload File from Controller page (see Figure 9-4).

Figure 9-4 Upload File from Controller Page



Upload file from Controller

File Type: PAC (Protected Access Credential)
User (Identity):
Validity (in days): 0
Password:
Confirm Password:
Transfer Mode: TFTP

Server Details

IP Address: 1.2.3.4
File Path: upload/
File Name: test.pac

Step 2 From the File Type drop-down box, choose **PAC (Protected Access Credential)**.

Step 3 In the User field, enter the name of the user who will use the PAC.

Step 4 In the Validity field, enter the number days for the PAC to remain valid. The default setting is zero (0).

Step 5 In the Password and Confirm Password fields, enter a password to protect the PAC.

Step 6 From the Transfer Mode drop-down box, choose **TFTP** or **FTP**.

Step 7 In the IP Address field, enter the IP address of the TFTP or FTP server.

Step 8 In the File Path field, enter the directory path of the PAC.

Step 9 In the File Name field, 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 field, enter the username to log into the FTP server.

b. In the Server Login Password field, enter the password to log into the FTP server.

c. In the Server Port Number field, 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.

Using the CLI to Upload PACs

Follow these steps to upload a PAC from the controller using the controller CLI.

Step 1 Log into the controller CLI.

Step 2 Enter **transfer upload mode** {**tftp** | **ftp**}.

Step 3 Enter **transfer upload datatype pac**.

Step 4 Enter **transfer upload pac** *username validity password.*

Step 5 Enter **transfer upload serverip** *server-ip-address*.

Step 6 Enter **transfer upload path** *server-path-to-file*.

Step 7 Enter **transfer upload filename** *manual*.pac.

Step 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.

Step 9 Enter **transfer upload start** to view the updated settings; then answer **y** when prompted to confirm the current settings and start the upload process. This example shows the upload command output:

```
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

Cisco recommends that you upload your controller's configuration file to a server to back it up. If you ever experience some loss of configuration, you can then download the saved configuration to the controller.

In controller software release 4.2 or later, the controller's bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in binary format. Therefore, you cannot download a binary configuration file onto a controller running software release 4.2 or later. However, when you upgrade a controller from a previous software release to 4.2 or later, the configuration file is migrated and converted to XML.

Note Controller software release 5.2 enables you to read and modify the configuration file. See the "Editing Configuration Files" section on page 9-27 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

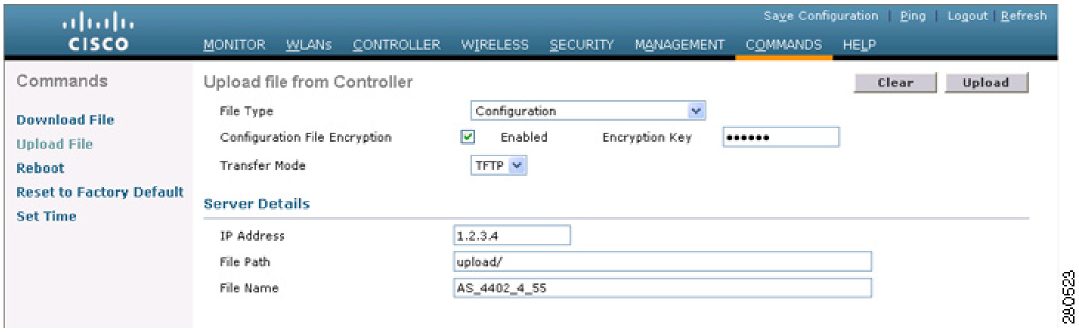
You can upload configuration files using either the GUI or the CLI.

Using the GUI to Upload Configuration Files

Using the controller GUI, follow these steps to upload a configuration file to a server.

Step 1 Click **Commands** > **Upload File** to open the Upload File from Controller page (see Figure 9-5).

Figure 9-5 Upload File from Controller Page



Upload file from Controller

File Type	Configuration		
Configuration File Encryption	☑ Enabled	Encryption Key	••••••
Transfer Mode	TFTP		

Server Details

IP Address	1.2.3.4
File Path	upload/
File Name	AS_4402_4_55

Step 2 From the File Type drop-down box, choose **Configuration**.

Step 3 To encrypt the configuration file, check the **Configuration File Encryption** check box and enter the encryption key in the Encryption Key field.

Step 4 From the Transfer Mode drop-down box, choose **TFTP** or **FTP**.

Step 5 In the IP Address field, enter the IP address of the TFTP or FTP server.

Step 6 In the File Path field, enter the directory path of the configuration file.

Step 7 In the File Name field, enter the name of the configuration file.

Step 8 If you are using an FTP server, follow these steps:

a. In the Server Login Username field, enter the username to log into the FTP server.

b. In the Server Login Password field, enter the password to log into the FTP server.

c. In the Server Port Number field, 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.

Using the CLI to Upload Configuration Files

Using the controller CLI, follow these steps to upload a configuration file to a server.

Step 1 To specify the transfer mode used to upload the configuration file, 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 config

Step 3 To encrypt the configuration file, enter these commands:

- **transfer encrypt enable**
- **transfer encrypt set-key** *key*, where *key* is the encryption key used to encrypt the file

Step 4 To specify the IP address of the TFTP or FTP server, enter this command:

transfer upload serverip *server-ip-address*

Step 5 To specify the directory path of the configuration file, enter this command:

transfer upload path *server-path-to-file*

Step 6 To specify the name of the configuration file to be uploaded, enter 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 To initiate the upload process, enter this command:

transfer upload start

Step 9 When prompted to confirm the current settings, answer **y**. This example shows the upload command output:

```
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.

Downloading Configuration Files

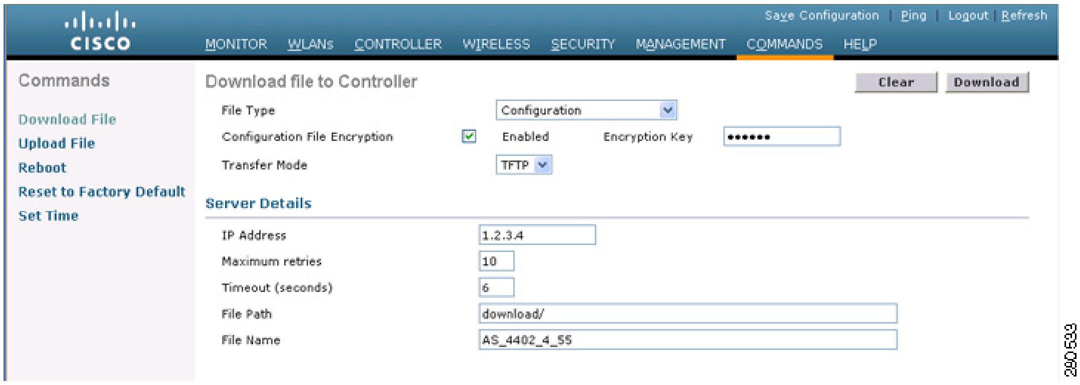
You can download configuration files using either the GUI or the CLI.

Using the GUI to Download Configuration Files

Using the controller GUI, follow these steps to download a configuration file to the controller.

Step 1 Click **Commands** > **Download File** to open the Download File to Controller page (see Figure 9-6).

Figure 9-6 Download File to Controller Page


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Commands
Download File
Upload File
Reboot
Reset to Factory Default
Set Time
Clear
Download
290533

Download file to Controller

File Type	Configuration
Configuration File Encryption	☑ Enabled Encryption Key ••••••
Transfer Mode	TFTP

Server Details

IP Address	1.2.3.4
Maximum retries	10
Timeout (seconds)	6
File Path	download/
File Name	AS_4402_4_55

Step 2 From the File Type drop-down box, choose **Configuration**.

Step 3 If the configuration file is encrypted, check the **Configuration File Encryption** check box and enter the encryption key used to decrypt the file in the Encryption Key field.

Note The key that you enter here should match the one entered during the upload process.

Step 4 From the Transfer Mode drop-down box, choose **TFTP** or **FTP**.

Step 5 In the IP Address field, enter the IP address of the TFTP or FTP server.

Step 6 If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields 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 configuration file in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the configuration file in the Timeout field.

Step 7 In the File Path field, enter the directory path of the configuration file.

Step 8 In the File Name field, 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 field, enter the username to log into the FTP server.

b. In the Server Login Password field, enter the password to log into the FTP server.

c. In the Server Port Number field, 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.

Using the CLI to Download Configuration Files

Using the controller CLI, follow these steps to download a configuration file to the controller.

Note The controller does not support incremental configuration downloads. The configuration file contains all mandatory CLIs (all interface address CLIs, mgmtuser with read-write permission CLIs, and interface port or LAG enable or disable CLIs) required to successfully complete the download. For example, if you download only **config time ntp server** *index server_address* as part of the configuration file, the download fails. Only the CLI 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 To specify the transfer mode used to download the configuration file, enter this command:

transfer download mode {**tftp** | **ftp**}

Step 2 To specify the type of file to be downloaded, enter this command:

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 To specify the IP address of the TFTP or FTP server, enter this command:

transfer download serverip *server-ip-address*

Step 5 To specify the directory path of the configuration file, enter this command:

transfer download path *server-path-to-file*

Step 6 To specify the name of the configuration file to be downloaded, enter this command:

transfer download filename *filename*

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 to specify the username and password used to log into the FTP server and the port number through which the download occurs:

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

Note The default value for the *port* parameter is 21.

Step 9 To view the updated settings, enter this command:

transfer download start

Step 10 When prompted to confirm the current settings and start the download process, answer **y**. This example shows the download command output:

```
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 download fails, repeat this procedure and try again.

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 non-volatile 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 enables 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 CLI format on the server. When you are finished, you download the file back to the controller, where it is reconverted to XML format and saved.

Follow these steps to edit the controller's configuration file.

Step 1 To upload the configuration file to a TFTP or FTP server, perform one of the following:

- Upload the file using the controller GUI. Follow the instructions in the "Using the GUI to Upload Configuration Files" section on page 9-21.
- Upload the file using the controller CLI. Follow the instructions in the "Using the CLI to Upload Configuration Files" section on page 9-22.

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 To download the configuration file to the controller, perform one of the following:

- Download the file using the controller GUI. Follow the instructions in the "Using the GUI to Download Configuration Files" section on page 9-23.
- Download the file using the controller CLI. Follow the instructions in the "Using the CLI to Download Configuration Files" section on page 9-25.

The controller converts the configuration file to 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 "Using the GUI to Upload Configuration Files" section on page 9-21 but choose **Invalid Config** from the File Type drop-down box in Step 2 and skip Step 3.
- Upload the invalid configuration using the controller CLI. Follow the instructions in the "Using the CLI to Upload Configuration Files" section on page 9-22 but enter this command in Step 2: **transfer upload datatype invalid-config** and skip Step 3.

Step 6 The controller does not support the uploading and downloading of port configuration CLI commands. If you want to configure the controller ports, enter these commands to do so now:

- **config port linktrap** {*port* | **all**} {**enable** | **disable**}—Enables or disables the up and down link traps for a specific controller port or for all ports.
- **config port adminmode** {*port* | **all**} {**enable** | **disable**}—Enables or disables the administrative mode for a specific controller port or for all ports.

Step 7 To save your changes, enter this command:

save config

Clearing the Controller Configuration

Follow these steps to clear the active configuration in NVRAM.

Step 1 Enter **clear config** and enter **y** at the confirmation prompt to confirm the action.

Step 2 Enter **reset system**. At the confirmation prompt, enter **n** to reboot without saving configuration changes. When the controller reboots, the configuration wizard starts automatically.

Step 3 Follow the instructions in the "Using the Configuration Wizard" section on page 4-2 to complete the initial configuration.

Erasing the Controller Configuration

Follow these steps to reset the controller configuration to default settings.

Step 1 Enter **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, enter **recover-config** to restore the factory default configuration. The controller reboots and the configuration wizard starts automatically.

Step 3 Follow the instructions in the "Using the Configuration Wizard" section on page 4-2 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.

CHAPTER 10

Managing User Accounts

This chapter explains how to create and manage guest user accounts, describes the web authentication process, and provides instructions for customizing the web authentication login page. It contains these sections:

- Creating Guest User Accounts, page 10-2
- Web Authentication Process, page 10-7
- Choosing the Web Authentication Login Page, page 10-9
- Configuring Wired Guest Access, page 10-23

Creating Guest User Accounts

The controller can provide guest user access on WLANs. The first step in creating guest user accounts is to create a lobby administrator account, 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.

The local user database is limited to a maximum of 2048 entries and is set to a default value of 512 entries (on the Security > General page). This database is shared by local management users (including lobby ambassadors), net users (including guest users), MAC filter entries, and disabled clients. Together these cannot exceed the configured database size.

Creating a Lobby Ambassador Account

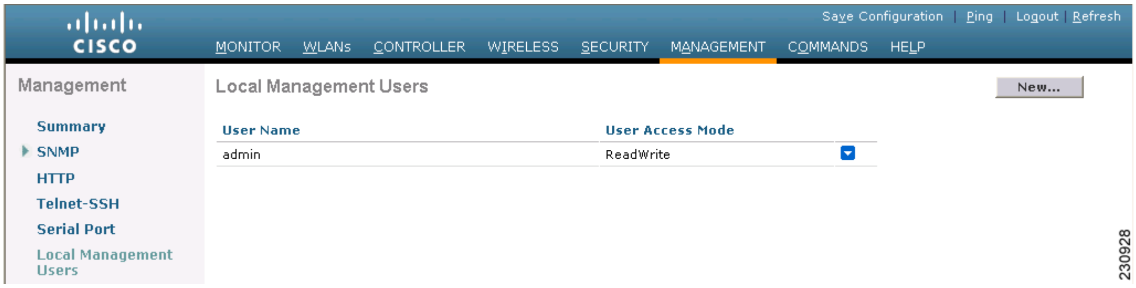
You can create a lobby ambassador account on the controller through either the GUI or the CLI.

Using the GUI to Create a Lobby Ambassador Account

Follow these steps to create a lobby ambassador account using the controller GUI.

Step 1 Click **Management** > **Local Management Users** to open the Local Management Users page (see Figure 10-1).

Figure 10-1 Local Management Users Page



Local Management Users

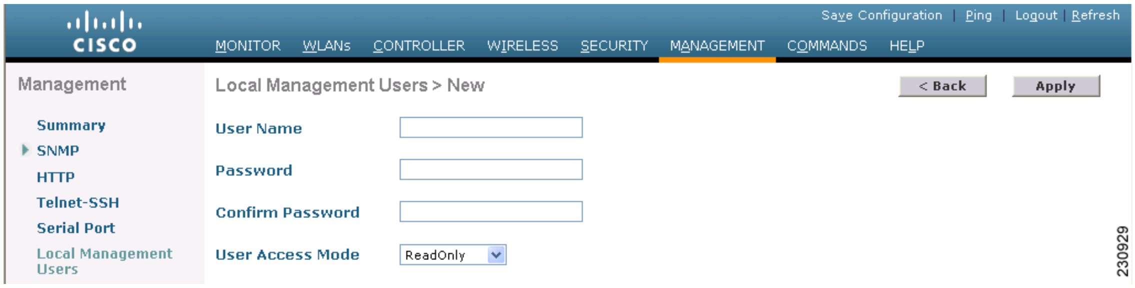
User Name	User Access Mode
admin	ReadWrite

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 To create a lobby ambassador account, click **New**. The Local Management Users > New page appears (see Figure 10-2).

Figure 10-2 Local Management Users > New Page



Local Management Users > New

User Name
Password
Confirm Password
User Access Mode: ReadOnly

Step 3 In the User Name field, 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 fields, enter a password for the lobby ambassador account.

Note Passwords are case sensitive.

Step 5 Choose **LobbyAdmin** from the User Access Mode drop-down box. 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.

Using the CLI to Create a Lobby Ambassador Account

Enter this command to create a lobby ambassador account using the controller CLI:

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.

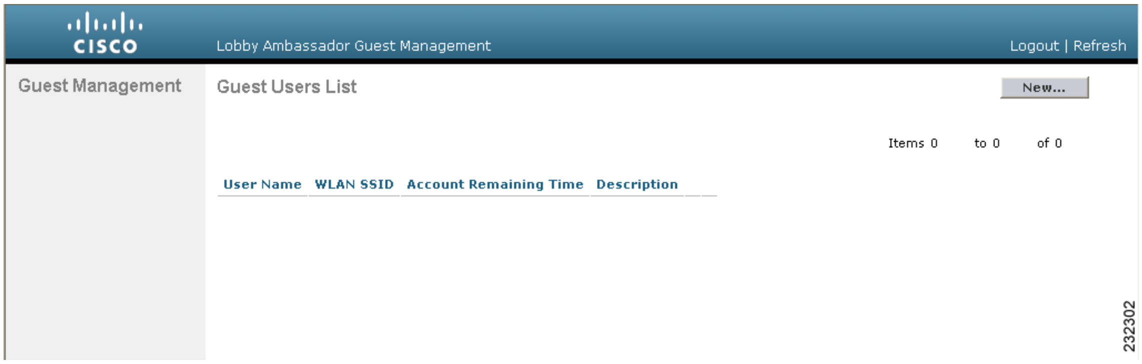
Creating Guest User Accounts as a Lobby Ambassador

A lobby ambassador would follow these steps to create guest user accounts.

Note A lobby ambassador cannot access the controller CLI interface and therefore can create guest user accounts only from the controller GUI.

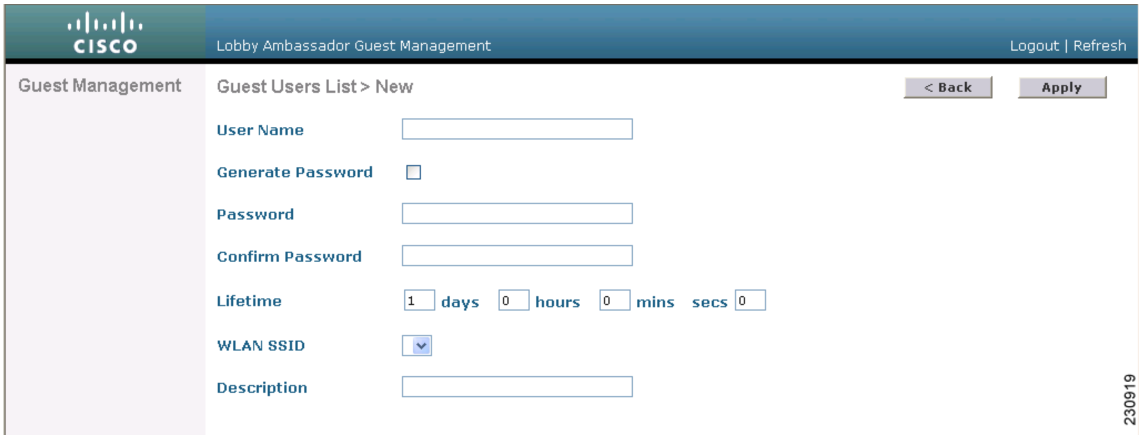
Step 1 Log into the controller as the lobby ambassador, using the username and password specified in the "Creating a Lobby Ambassador Account" section above. The Lobby Ambassador Guest Management > Guest Users List page appears (see Figure 10-3).

Figure 10-3 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 (see Figure 10-4).

Figure 10-4 Lobby Ambassador Guest Management > Guest Users List > New Page



Step 3 In the User Name field, 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, check the **Generate Password** check box. The generated password is entered automatically in the Password and Confirm Password fields.
- If you want to create a password for this guest user, leave the **Generate Password** check box unchecked and enter a password in both the Password and Confirm Password fields.

Note Passwords can contain up to 24 characters and are case sensitive.

Step 5 From the Lifetime drop-down boxes, 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 fields 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 non-zero 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** CLI command to make a guest user account permanent without deleting and recreating it.

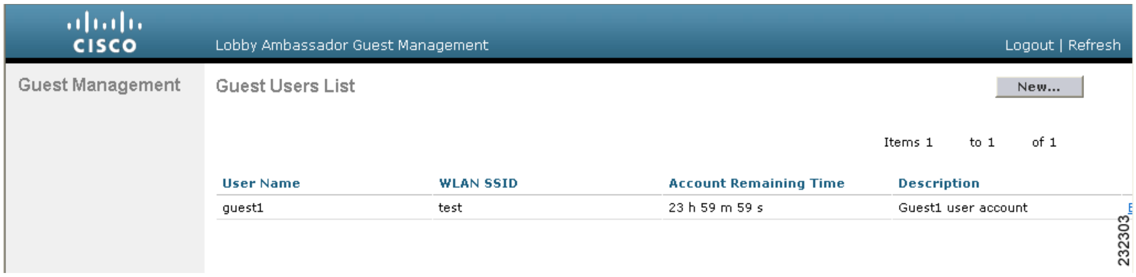
Step 6 From the WLAN SSID drop-down box, choose the SSID that will be used by the guest user. The only WLANs that are listed are those for which Layer 3 web authentication has been configured.

Note Cisco recommends that the system administrator create a specific guest WLAN to prevent any potential conflicts. If a guest account expires and it has a name conflict with an account on the RADIUS server and both are on the same WLAN, the users associated with both accounts are disassociated before the guest account is deleted.

Step 7 In the Description field, 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 (see Figure 10-5).

Figure 10-5 Lobby Ambassador Guest Management > Guest Users List Page



User Name	WLAN SSID	Account Remaining Time	Description
guest1	test	23 h 59 m 59 s	Guest1 user account

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.

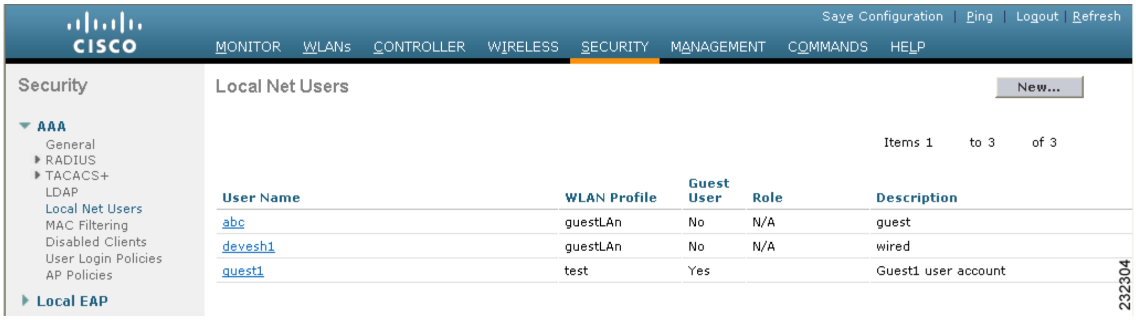
Viewing Guest User Accounts

After a lobby ambassador has created guest user accounts, the system administrator can view them from the controller GUI or CLI.

Using the GUI to View Guest Accounts

To view guest user accounts using the controller GUI, click **Security** > **AAA** > **Local Net Users**. The Local Net Users page appears (see Figure 10-6).

Figure 10-6 Local Net Users Page



User Name	WLAN Profile	Guest User	Role	Description
abc	guestLAn	No	N/A	guest
devesh1	guestLAn	No	N/A	wired
guest1	test	Yes		Guest1 user account

From this page, the system administrator 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.

Using the CLI to View Guest Accounts

To view all of the local net user accounts (including guest user accounts) using the controller CLI, enter this command:

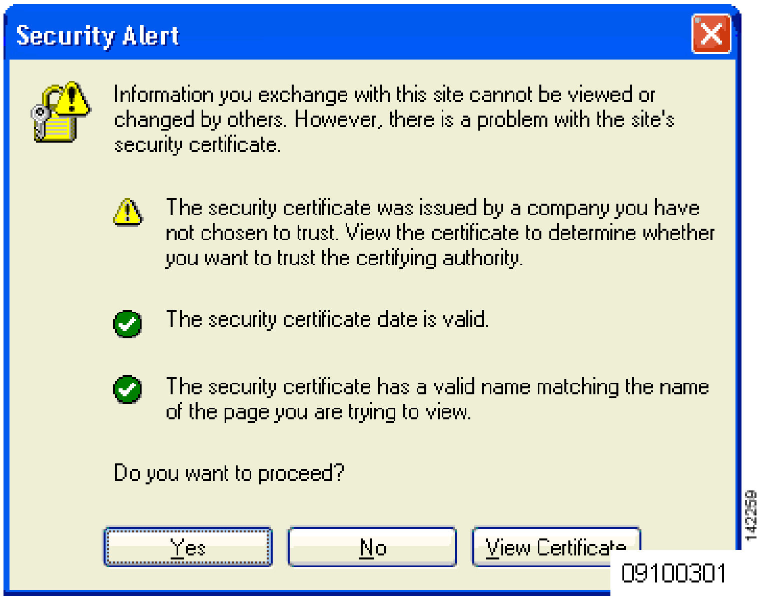
show netuser summary

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. Then when the clients attempt to join the wireless LAN, their users must enter the username and password when prompted by a login page.

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. Figure 10-7 shows a typical security alert.

Figure 10-7 Typical Web-Browser Security Alert



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

✓ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

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 10-8).

To prevent the security alert from appearing, the user can perform 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, check the **Show Physical Stores** check box.

Step 6 Expand the **Trusted Root Certification Authorities** folder and choose **Local Computer**.

Step 7 Click **OK**.

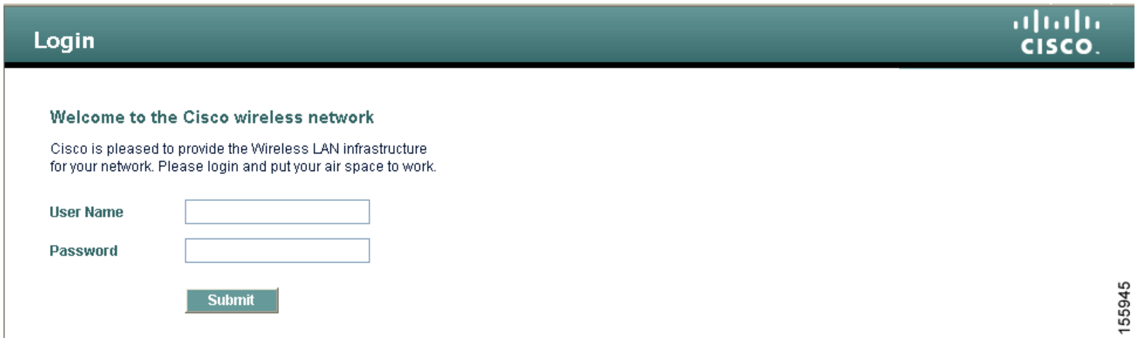
Step 8 Click **Next** > **Finish**.

Step 9 When the "The import was successful" message appears, click **OK**.

Step 10 Because the issuer field is blank on the controller self-signed certificate, open Internet Explorer, click **Tools** > **Internet Options** > **Advanced**, uncheck the **Warn about Invalid Site Certificates** check box under Security, and click **OK**.

Step 11 Reboot the PC. On the next web authentication attempt, the login page appears (see Figure 10-8).Figure 10-8 shows the default web authentication login window.

Figure 10-8 Default Web Authentication Login Page



Login

Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.

User Name

Password

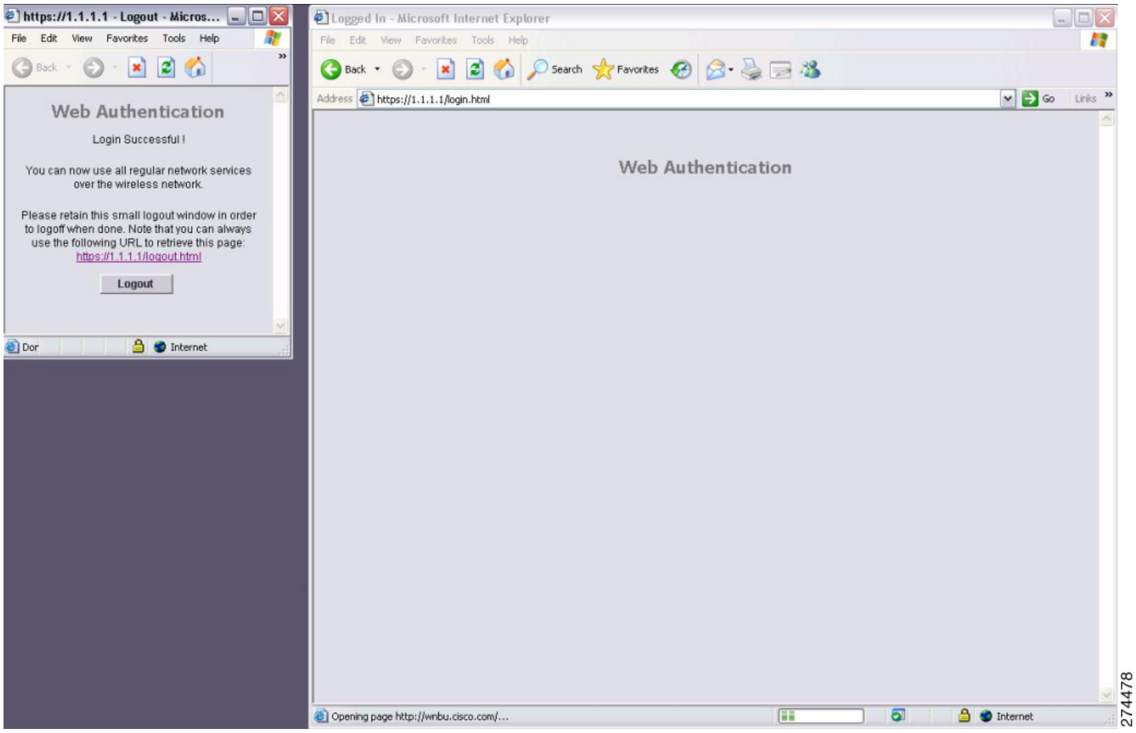
The default login page contains a Cisco logo and Cisco-specific text. You can choose to have the web authentication system display one of the following:

- 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 Web Authentication Login Page" section on page 10-9 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. Figure 10-9 shows a typical successful login page.

Figure 10-9 Successful Login Page



https://1.1.1.1 - Logout - Micros...
File Edit View Favorites Tools Help
Back
Dor
Internet
Logged In - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
Internet
274478

Web Authentication

Login Successful !

You can now use all regular network services over the wireless network.

Please retain this small logout window in order to logoff when done. Note that you can always use the following URL to retrieve this page:
https://1.1.1.1/logout.html

Logout

https://1.1.1.1/login.html

Web Authentication

Opening page http://wnbu.cisco.com/...

The default successful login page contains a pointer to a virtual gateway address URL: https://1.1.1.1/logout.html. The IP address that you set for the controller virtual interface serves as the redirect address for the login page (see Chapter 3 for more information on the virtual interface).

Choosing the Web Authentication Login Page

This section provides instructions for specifying the content and appearance of the web authentication login page. Follow the instructions in one of these sections to choose the web authentication login page using the controller GUI or CLI:

- Choosing the Default Web Authentication Login Page, page 10-10
- Creating a Customized Web Authentication Login Page, page 10-14
- Using a Customized Web Authentication Login Page from an External Web Server, page 10-16
- Downloading a Customized Web Authentication Login Page, page 10-17
- Assigning Login, Login Failure, and Logout Pages per WLAN, page 10-21

Note 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 this command: **config network secureweb cipher-option sslv2 disable**. If you enter this command, users must use a browser that is configured to use a more secure protocol such as SSLv3 or later. The default value is enabled.

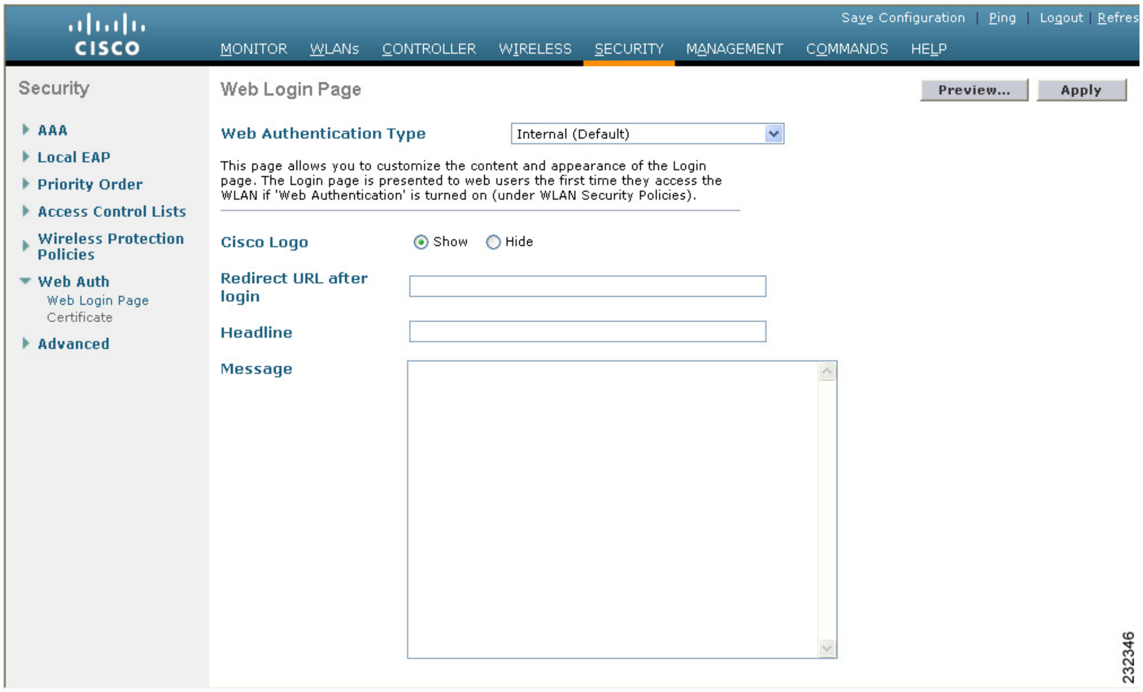
Choosing the Default Web Authentication Login Page

If you want to use the default web authentication login page as is (see Figure 10-8) or with a few modifications, follow the instructions in the GUI or CLI procedure below.

Using the GUI to Choose the Default Web Authentication Login Page

Step 1 Click **Security** > **Web Auth** > **Web Login Page** to open the Web Login page (see Figure 10-10).

Figure 10-10 Web Login Page



Save Configuration | Ping | Logout | Refres
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
Local EAP
Priority Order
Access Control Lists
Wireless Protection Policies
Web Auth
Web Login Page
Certificate
Advanced
Preview...
Apply
232346

Web Login Page

Web Authentication Type: Internal (Default)

This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

Cisco Logo ● Show ○ Hide

Redirect URL after login

Headline

Message

Step 2 From the Web Authentication Type drop-down box, 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 (such as www.AcompanyBC.com) in the Redirect URL After Login field. You can enter up to 254 characters.

Note The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.

Step 6 If you want to create your own headline on the login page, enter the desired text in the Headline field. 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 field. 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.

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.

Using the CLI to Choose the Default Web Authentication Login Page

Step 1 To specify the default web authentication type, enter 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 7. 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 **clear redirecturl**.

Note The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.

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 **clear webtitle**.

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 **clear webmessage**.

Step 7 Enter **save config t**o save your settings.

Step 8 If you want to import your own logo into the web authentication login page, follow these steps:

a. Make sure that you have a Trivial File Transfer Protocol (TFTP) server available for the file download. Keep these guidelines in mind 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. Enter **ping ip-address** to ensure that the controller can contact the TFTP server.

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. To specify the download mode, enter **transfer download mode tftp**.

e. To specify the type of file to be downloaded, enter **transfer download datatype image**.

f. To specify the IP address of the TFTP server, enter **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.

g. To specify the download path, enter **transfer download path** *absolute-tftp-server-path-to-file*.

h. To specify the file to be downloaded, enter **transfer download filename** {*filename.jpg* | *filename.gif* | *filename.png*}.

i. Enter **transfer download start** to view your updated settings and answer **y** to the prompt to confirm the current download settings and start the download. Information similar to the following appears:

```
Mode........................................... TFTP
Data Type...................................... Login Image
TFTP Server IP................................. xxx.xxx.xxx.xxx
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.
```

j. Enter **save config** to save your settings.

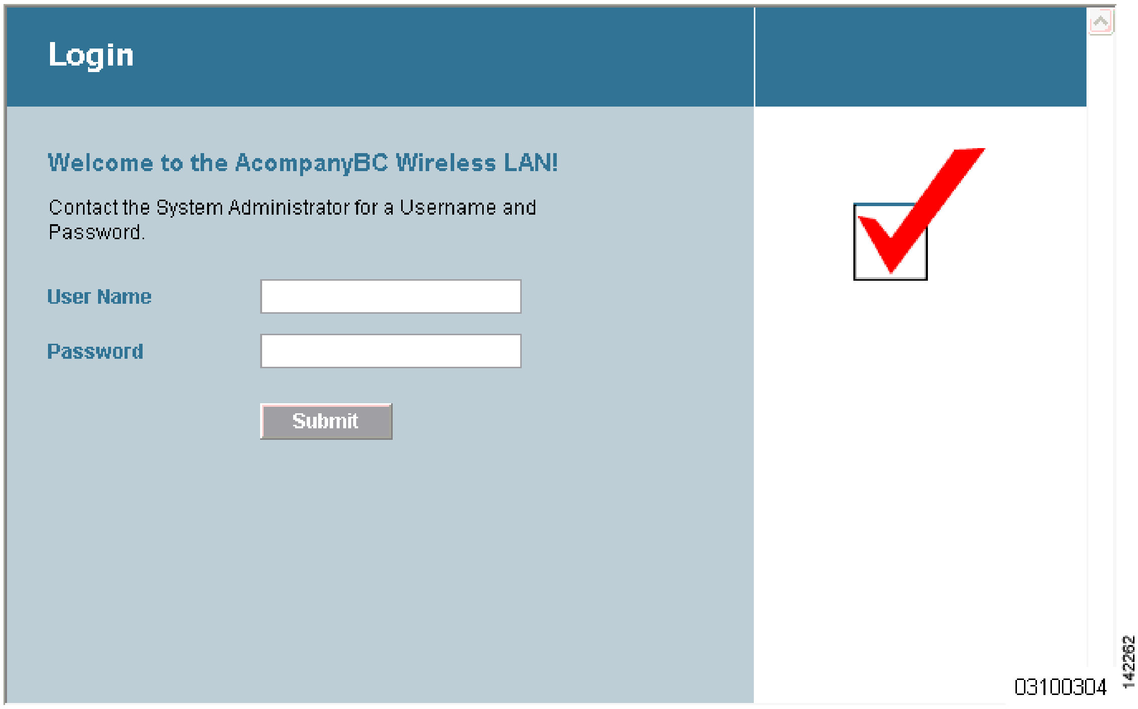
Note If you ever want to remove this logo from the web authentication login page, enter **clear webimage**.

Step 9 Follow the instructions in the "Using the CLI to Verify the Web Authentication Login Page Settings" section on page 10-20 to verify your settings.

Modified Default Web Authentication Login Page Example

Figure 10-11 shows an example of a modified default web authentication login page.

Figure 10-11 Modified Default Web Authentication Login Page Example



Login

Welcome to the AcompanyBC Wireless LAN!

Contact the System Administrator for a Username and Password.

These are the CLI commands 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

```
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 http://www.AcompanyBC.com

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
```

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>
<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 = "";
      var urlStr = "";
      if(equalIndex > 0) {
            equalIndex += searchString.length;
            urlStr = link.substring(equalIndex);
            if(urlStr.length > 0){
               redirectUrl += urlStr;
               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);
      }
      //alert( "AP MAC Address is " + args.ap_mac);
      //alert( "The Switch URL to post user credentials is " + args.switch_url);
      //document.forms[0].action = args.switch_url;

      // 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.");
      }

}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();">
<form method="post" action="https://1.1.1.1/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"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name &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.

These are the available status codes:

- 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, refer to the *External Web Authentication with Wireless LAN Controllers Configuration Example* at this URL: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008067489f.shtml

Using a Customized Web Authentication Login Page from an External Web Server

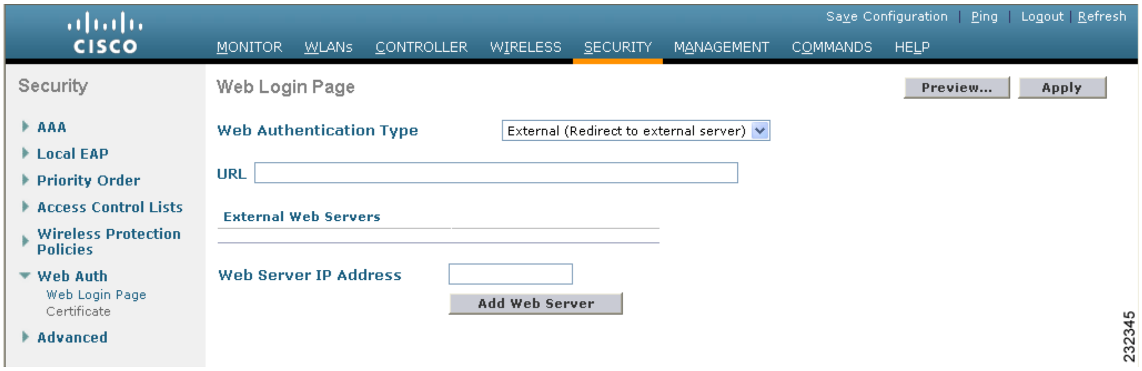
If you want to use a customized web authentication login page that you configured on an external web server, follow the instructions in the GUI or CLI procedure below. When you enable this feature, the user is directed to your customized login page on the external web server.

Note 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. See Chapter 5 for more information on ACLs.

Using the GUI to Choose a Customized Web Authentication Login Page from an External Web Server

Step 1 Click **Security** > **Web Auth** > **Web Login Page** to open the Web Login page (see Figure 10-12).

Figure 10-12 Web Login Page



Web Login Page

Web Authentication Type: External (Redirect to external server)

URL

External Web Servers

Web Server IP Address

Step 2 From the Web Authentication Type drop-down box, choose **External (Redirect to external server)**.

Step 3 In the URL field, 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 field, 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.

Using the CLI to Choose a Customized Web Authentication Login Page from an External Web Server

Step 1 To specify the web authentication type, enter this command:

config custom-web webauth_type external.

Step 2 To specify the URL of the customized web authentication login page on your web server, enter this command:

config custom-web ext-webauth-url *url*

You can enter up to 252 characters for the URL.

Step 3 To specify the IP address of your web server, enter this command:

config custom-web ext-webserver {**add** | **delete**} *server_IP_address*

Step 4 Enter **save config** to save your settings.

Step 5 Follow the instructions in the "Using the CLI to Verify the Web Authentication Login Page Settings" section on page 10-20 to verify your settings.

Downloading a 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, Cisco recommends that you use an application that complies with GNU standards, such as PicoZip, to compress the .tar file for the webauth bundle.

Follow these guidelines when preparing the customized login page:

- Name the login page "login.html." The controller prepares the web authentication URL based on this name. If the does not find this file after the webauth bundle has been untarred, the bundle is discarded, and an error message appears.
- Include input fields 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) are of relative type.

You can download a login page example from Cisco WCS and use it as a starting point for your customized login page. Refer to the "Downloading a Customized Web Auth Page" section in the Using Templates chapter of the *Cisco Wireless Control System Configuration Guide, Release 5.2* for instructions.

If you want to download a customized web authentication login page to the controller, follow the instructions in the GUI or CLI procedure below.

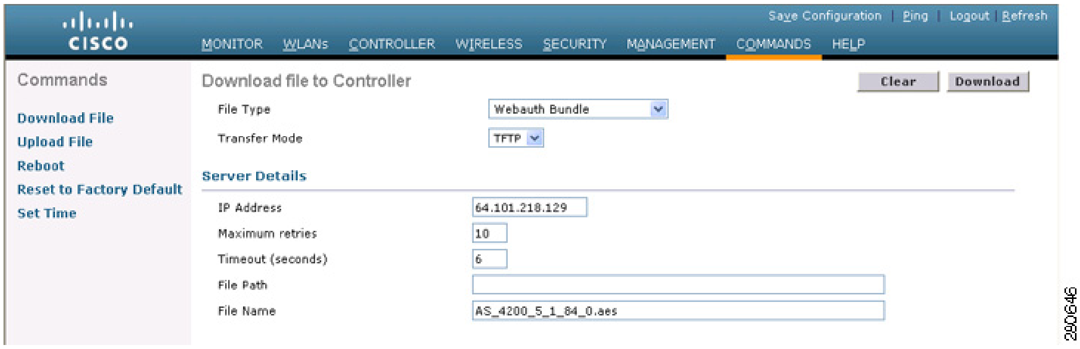
Using the GUI to Download a Customized Web Authentication Login Page

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 8 of the "Using the CLI to Choose the Default Web Authentication Login Page" section on page 10-11.

Step 2 Copy the .tar file containing your login page to the default directory on your TFTP server.

Step 3 Click **Commands** > **Download File** to open the Download File to Controller page (see Figure 10-13).

Figure 10-13 Download File to Controller Page



Download file to Controller

File Type: Webauth Bundle

Transfer Mode: TFTP

Server Details

IP Address: 64.101.218.129

Maximum retries: 10

Timeout (seconds): 6

File Path:

File Name: AS_4200_5_1_84_0.aes

Step 4 From the File Type drop-down box, choose **Webauth Bundle**.

Step 5 From the Transfer Mode drop-down box, choose **TFTP** or **FTP**.

Step 6 In the IP Address field, 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 field.

Range: 1 to 254

Default: 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 field.

Range: 1 to 254 seconds

Default: 6 seconds

Step 9 In the File Path field, enter the path of the .tar file to be downloaded. The default value is "/."

Step 10 In the File Name field, 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 field, enter the username to log into the FTP server.
- **b.** In the Server Login Password field, enter the password to log into the FTP server.
- **c.** In the Server Port Number field, 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 Click **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 14 From the Web Authentication Type drop-down box, 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.

Using the CLI to Download a Customized Web Authentication Login Page

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 8 of the "Using the CLI to Choose the Default Web Authentication Login Page" section on page 10-11.

Step 2 Copy the .tar file containing your login page to the default directory on your TFTP server.

Step 3 To specify the download mode, enter **transfer download mode tftp**.

Step 4 To specify the type of file to be downloaded, enter **transfer download datatype webauthbundle**.

Step 5 To specify the IP address of the TFTP server, enter **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 To specify the download path, enter **transfer download path** *absolute-tftp-server-path-to-file*.

Step 7 To specify the file to be downloaded, enter **transfer download filename** *filename.tar*.

Step 8 Enter **transfer download start** to view your updated settings and answer **y** to the prompt to confirm the current download settings and start the download.

Step 9 To specify the web authentication type, enter **config custom-web webauth_type customized**.

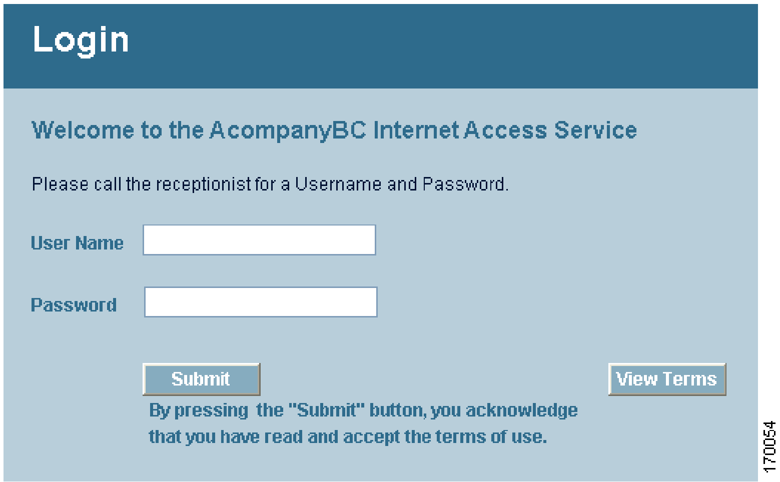
Step 10 Enter **save config** to save your settings.

Step 11 Follow the instructions in the "Using the CLI to Verify the Web Authentication Login Page Settings" section on page 10-20 to verify your settings.

Customized Web Authentication Login Page Example

Figure 10-14 shows an example of a customized web authentication login page.

Figure 10-14 Customized Web Authentication Login Page Example



Login

Welcome to the AcompanyBC Internet Access Service

Please call the receptionist for a Username and Password.

User Name

Password

By pressing the "Submit" button, you acknowledge that you have read and accept the terms of use.

Using the CLI to Verify the Web Authentication Login Page Settings

Enter **show custom-web** 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
```

This example shows the information that appears when the configuration settings have been modified:

```
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....................... Internal
Web Authentication URL........................... Disabled
```

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.

Using the GUI to Assign Login, Login Failure, and Logout Pages per WLAN

Using the controller GUI, follow these steps to assign web login, login failure, and logout pages to a WLAN.

Step 1 Click **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 Click **Security** > **Layer 3**.

Step 4 Make sure that **Web Policy** and **Authentication** are selected.

Step 5 To override the global authentication configuration web authentication pages, check the **Override Global Config** check box.

Step 6 When the Web Auth Type drop-down box 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 boxes 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 box 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, refer to the "Downloading a Customized Web Authentication Login Page" section on page 10-17.

- **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 field.

  You can select 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, click **AAA Servers** and choose up to three RADIUS and LDAP servers using the drop-down boxes.

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 To establish the priority in which the servers are contacted to perform web authentication, follow these steps. 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 the **Up** and **Down** buttons 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.

Using the CLI to Assign Login, Login Failure, and Logout Pages per WLAN

Using the controller CLI, follow these steps to assign web login, login failure, and logout pages to a WLAN.

Step 1 To determine the ID number of the WLAN to which you want to assign a web login, login failure, or logout page, enter 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 this command: **config wlan custom-web loginfailure-page none** *wlan_id*.

- **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 this command: **config wlan custom-web logout-page none** *wlan_id*.

Step 3 If you want wireless guest users to be redirected to an external server before accessing the web login page, enter this command to specify the URL of the external server:

config wlan custom-web ext-webauth-url *ext_web_url wlan_id*

Step 4 If you want to define the order in which web authentication servers are contacted, enter this command:

config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

The default order of server web authentication is local, RADIUS, LDAP.

Note All external servers must be pre-configured on the controller. You can configure them on the RADIUS Authentication Servers page and the LDAP Servers page.

Step 5 To define which web authentication page displays for a wireless guest user, enter this command:

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 To use a WLAN-specific custom web configuration rather than a global custom web configuration, enter this command:

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 To save your changes, enter this command:

save config

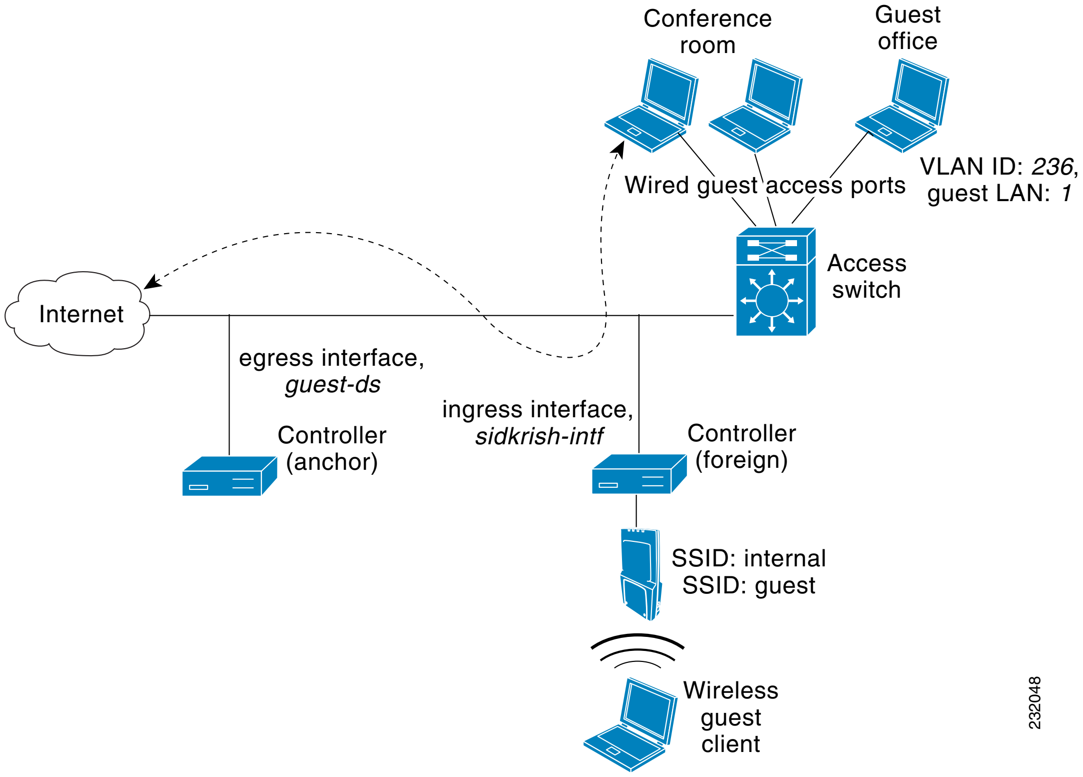
Configuring Wired Guest Access

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.

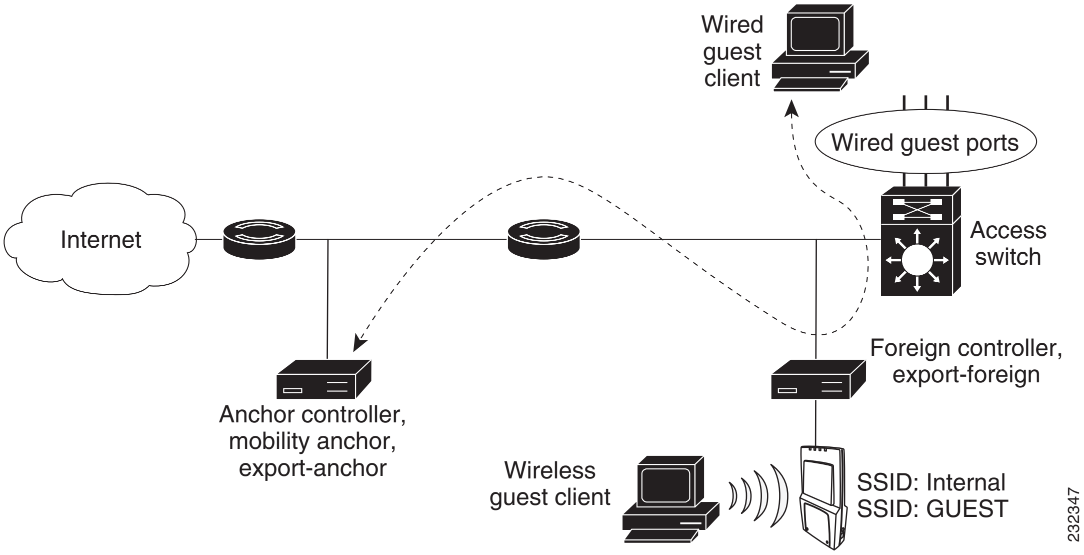
Wired guest access ports initially terminate on a Layer 2 access switch or switch port configured with VLAN interfaces for wired guest access traffic. The wired guest traffic is then trunked from the access switch to a controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch. See Figure 10-15.

Figure 10-15 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 10-16.

Figure 10-16 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, refer to the "Configuring Quality of Service Roles" section on page 4-48.

Configuration Overview

To configure wired guest access on a wireless network, you will 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

Configuration Guidelines

Follow these guidelines before using wired guest access on your network:

- Wired guest access is supported only on the following controllers: 4400 series controllers, the Cisco WiSM, 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.
- Layer 3 web authentication and web passthrough are supported for wired guest access clients. Layer 2 security is not supported.
- Do not attempt to trunk a guest VLAN on the Catalyst 3750G Integrated Wireless LAN Controller Switch to multiple controllers. Redundancy cannot be achieved by doing so.

Using the GUI to Configure Wired Guest Access

Using the controller GUI, follow these steps to configure wired guest user access on your network.

Step 1 To create a dynamic interface for wired guest user access, click **Controller** > **Interfaces**. The Interfaces page appears.

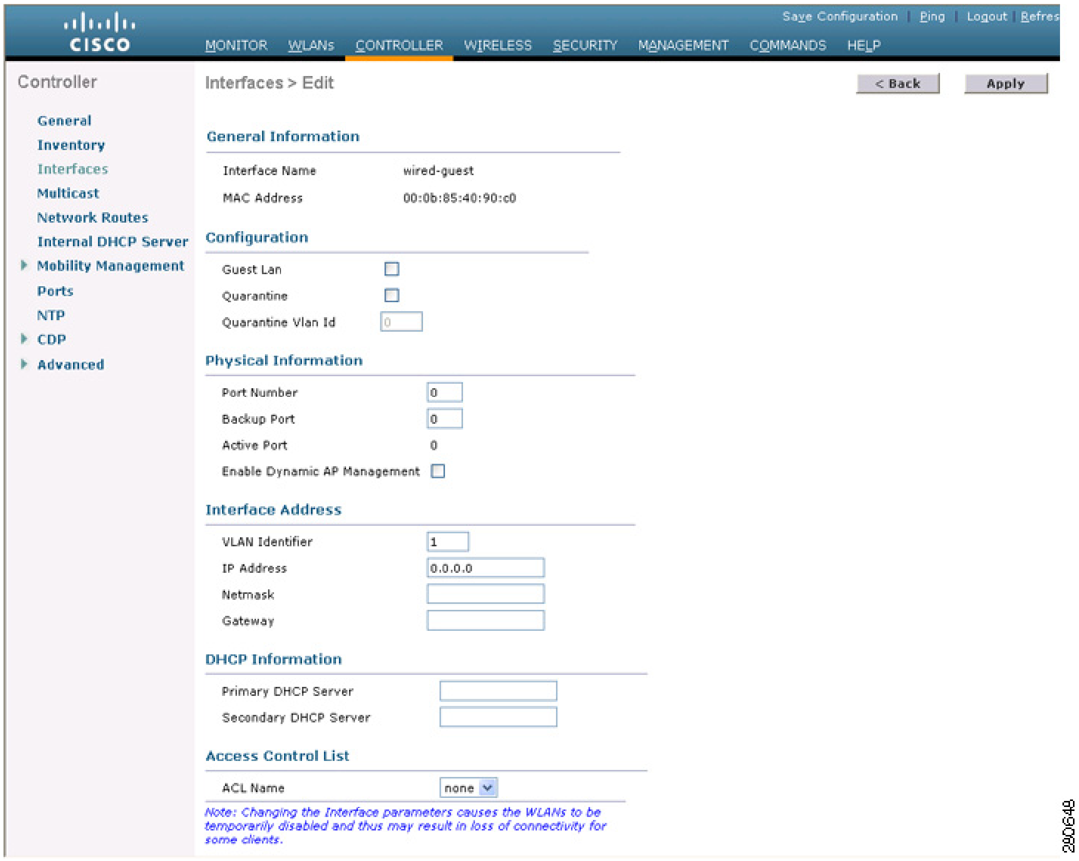
Step 2 Click **New** to open the Interfaces > New page.

Step 3 Enter a name and VLAN ID for the new interface.

Step 4 Click **Apply** to commit your changes.

Step 5 On the Interfaces > Edit page, enter the IP address, netmask, and gateway address for the interface (see Figure 10-17).

Figure 10-17 Interfaces > Edit Page



Interfaces > Edit

General Information

Interface Name	wired-guest
MAC Address	00:0b:85:40:90:c0

Configuration

Guest Lan	□
Quarantine	□
Quarantine Vlan Id	0

Physical Information

Port Number	0
Backup Port	0
Active Port	0
Enable Dynamic AP Management	□

Interface Address

VLAN Identifier	1
IP Address	0.0.0.0
Netmask	
Gateway	

DHCP Information

Primary DHCP Server	
Secondary DHCP Server	

Access Control List

ACL Name	none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

Step 6 In the Port Number field, enter a valid port number. You can enter a number between 0 and 25 (inclusive).

Step 7 Check the **Guest LAN** check box.

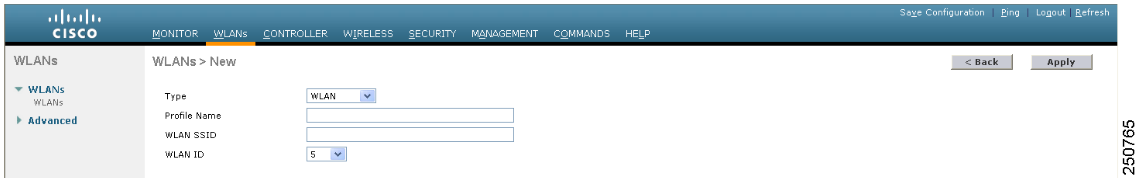
Step 8 Enter an IP address for the primary DHCP server.

Step 9 Click **Apply** to commit your changes.

Step 10 To create a wired LAN for guest user access, click **WLANs**.

Step 11 On the WLANs page, choose **Create New** from the drop-down box and click **Go**. The WLANs > New page appears (see Figure 10-18).

Figure 10-18 WLANs > New Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
250765

WLANs > New

Type WLAN
Profile Name
WLAN SSID
WLAN ID 5

Step 12 From the Type drop-down box, choose **Guest LAN**.

Step 13 In the Profile Name field, enter a name that identifies the guest LAN. Do not use any spaces.

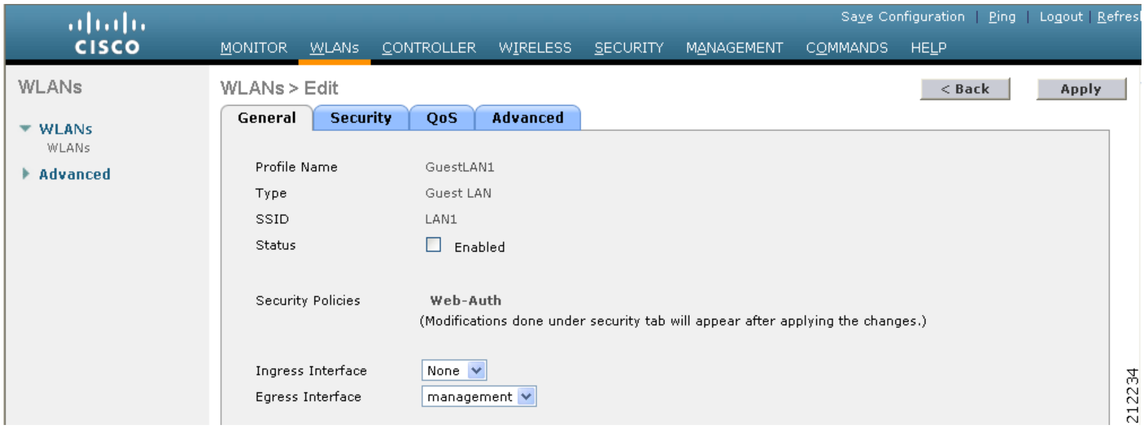
Step 14 In the WLAN SSID field, enter an SSID that identifies the guest LAN. Do not use any spaces.

Step 15 From the WLAN ID drop-down box, 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 16 Click **Apply** to commit your changes. The WLANs > Edit page appears (see Figure 10-19).

Figure 10-19 WLANs > Edit Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
212234

WLANs > Edit

Profile Name GuestLAN1
Type Guest LAN
SSID LAN1
Status □ Enabled

Security Policies Web-Auth
(Modifications done under security tab will appear after applying the changes.)

Ingress Interface None
Egress Interface management

Step 17 Check the **Enabled** check box for the Status parameter.

Step 18 Web authentication (Web-Auth) is the default security policy. If you want to change this to web passthrough, click the **Security** tab after completing Step 19 and Step 20.

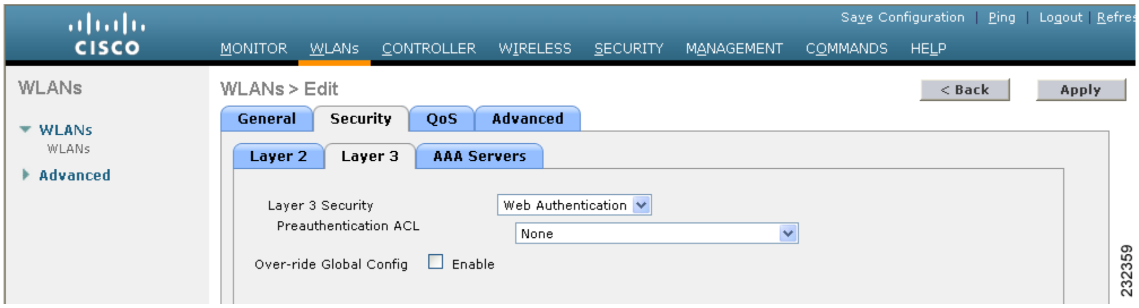
Step 19 From the Ingress Interface drop-down box, choose the VLAN that you created in Step 3. This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 20 From the Egress Interface drop-down box, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.

Note If you have only one controller in the configuration, choose **management** from the Egress Interface drop-down box.

Step 21 If you want to change the authentication method (for example, from web authentication to web passthrough), click **Security** > **Layer 3**. The WLANs > Edit (Security > Layer 3) page appears (see Figure 10-20).

Figure 10-20 WLANs > Edit (Security > Layer 3) Page


CISCO
Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General Security QoS Advanced
Layer 2 Layer 3 AAA Servers
232359

Layer 3 Security: Web Authentication

Preauthentication ACL: None

Over-ride Global Config □ Enable

Step 22 From the Layer 3 Security drop-down box, 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.

Step 23 If you choose the Web Passthrough option, an **Email Input** check box appears. Check this check box if you want users to be prompted for their email address when attempting to connect to the network.

Step 24 To override the global authentication configuration set on the Web Login page, check the **Override Global Config** check box.

Step 25 When the Web Auth Type drop-down box 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 boxes 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 box 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 field.

  You can select 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 26 If you chose External as the web authentication type in Step 25, click **AAA Servers** and choose up to three RADIUS and LDAP servers using the drop-down boxes.

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 27 To establish the priority in which the servers are contacted to perform web authentication, follow these steps. 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 the **Up** and **Down** buttons 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 28 Click **Apply** to commit your changes.

Step 29 Click **Save Configuration** to save your changes.

Step 30 Repeat this process if a second (anchor) controller is being used in the network.

Using the CLI to Configure Wired Guest Access

Using the controller CLI, follow these steps to configure wired guest user access on your network.

Step 1 To create a dynamic interface (VLAN) for wired guest user access, enter this command:

config interface create *interface_name vlan_id*

Step 2 If a 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 To enable or disable the guest LAN VLAN, enter this command:

config interface guest-lan *interface_name* {**enable** | **disable**}

This VLAN is later associated with the ingress interface created in Step 5.

Step 4 To create a wired LAN for wired client traffic and associate it to an interface, enter this command:

config guest-lan create *guest_lan_id interface_name*

The guest LAN ID must be a value between 1 and 5 (inclusive).

Note To delete a wired guest LAN, enter this command: **config guest-lan delete** *guest_lan_id*

Step 5 To configure the wired guest VLAN's ingress interface, which provides a path between the wired guest client and the controller by way of the Layer 2 access switch, enter this command:

config guest-lan ingress-interface *guest_lan_id interface_name*

Step 6 To configure an egress interface to transmit wired guest traffic out of the controller, enter this command:

config guest-lan interface *guest_lan_id interface_name*

Note If the wired guest traffic is terminating on another controller, repeat Step 4 and Step 6 for the terminating (anchor) controller and Step 1 through Step 5 for the originating (foreign) controller. Additionally, configure the following command for both controllers:
config mobility group anchor add {**guest-lan** *guest_lan_id* | **wlan** *wlan_id*} *IP_address*

Step 7 To configure the security policy for the wired guest LAN, enter this command:

config guest-lan security {**web-auth enable** *guest_lan_id* | **web-passthrough enable** *guest_lan_id*}

Note Web authentication is the default setting.

Step 8 To enable or disable a wired guest LAN, enter this command:

config guest-lan {**enable** | **disable**} *guest_lan_id*

Step 9 If you want wired 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 guest LAN for which it should display:

- **config guest-lan custom-web login-page** *page_name guest_lan_id*—Defines a web login page.
- **config guest-lan custom-web loginfailure-page** *page_name guest_lan_id*—Defines a web login failure page.

  Note To use the controller's default login failure page, enter this command: **config guest-lan custom-web loginfailure-page none** *guest_lan_id*.

- **config guest-lan custom-web logout-page** *page_name guest_lan_id*—Defines a web logout page.

  Note To use the controller's default logout page, enter this command: **config guest-lan custom-web logout-page none** *guest_lan_id*.

Step 10 If you want wired guest users to be redirected to an external server before accessing the web login page, enter this command to specify the URL of the external server:

config guest-lan custom-web ext-webauth-url *ext_web_url guest_lan_id*

Step 11 If you want to define the order in which local (controller) or external (RADIUS, LDAP) web authentication servers are contacted, enter this command:

config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

The default order of server web authentication is local, RADIUS, LDAP.

Note All external servers must be pre-configured on the controller. You can configure them on the RADIUS Authentication Servers page or the LDAP Servers page.

Step 12 To define the web login page for wired guest users, enter this command:

config guest-lan custom-web webauth-type {**internal** | **customized** | **external**} *guest_lan_id*

where

- **internal** displays the default web login page for the controller. This is the default value.
- **customized** displays the custom web pages (login, login failure, or logout) that were configured in Step 9.
- **external** redirects users to the URL that was configured in Step 10.

Step 13 To use a guest-LAN specific custom web configuration rather than a global custom web configuration, enter this command:

config guest-lan custom-web global disable *guest_lan_id*

Note If you enter the **config guest-lan custom-web global enable** *guest_lan_id* command, the custom web authentication configuration at the global level is used.

Step 14 To save your changes, enter this command:

save config

Note Information on the configured web authentication appears in both the **show run-config** and **show running-config** commands.

Step 15 To display the customized web authentication settings for a specific guest LAN, enter 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
Index IP Address
----- ---------------
1       9.43.0.100
2       0.0.0.0
3       0.0.0.0
4       0.0.0.0
5       0.0.0.0
...
20      0.0.0.0

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
    Loginfailure page name....................... None
    Logout page name............................. None

WLAN ID: 3
WLAN Status.................................. Enabled
    Web Security Policy.......................... Web Based Authentication
    Global Status................................ Disabled
    WebAuth Type................................. Customized
    Login Page................................... login.html
    Loginfailure 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
Loginfailure page name....................... None
Logout page name............................. None
```

Step 16 To display a summary of the local interfaces, enter this command:

show interface summary

Information similar to the following appears:

```
Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
ap-manager                       1    untagged 1.100.163.25    Static  Yes    No

management                       1    untagged 1.100.163.24    Static  No     No

service-port                     N/A  N/A      172.19.35.31    Static  No     No

virtual                          N/A  N/A      1.1.1.1         Static  No     No

wired                            1    20       10.20.20.8      Dynamic No     No

wired-guest                      1  236     10.20.236.50   Dynamic No    Yes
```

Note The interface name of the wired guest LAN in this example is *wired-guest* and its VLAN ID is 236.

Step 17 To display detailed interface information, enter this command:

show interface detailed *interface_name*

Information similar to the following appears:

```
Interface Name................................... wired-guest
MAC Address...................................... 00:11:92:ff:e7:eb
IP Address....................................... 10.20.236.50
IP Netmask....................................... 255.255.255.0
IP Gateway....................................... 10.50.236.1
VLAN............................................. 236
Quarantine-vlan.................................. no
Active Physical Port............................. LAG (29)
Primary Physical Port............................ LAG (29)
Backup Physical Port............................. Unconfigured
Primary DHCP Server.............................. 10.50.99.1
Secondary DHCP Server............................ Unconfigured
DHCP Option 82................................... Disabled
ACL.............................................. Unconfigured
AP Manager....................................... No
Guest Interface............................... Yes
```

Step 18 To display the configuration of a specific wired guest LAN, enter 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 **show guest-lan summary** to view all wired guest LANs configured on the controller.

Step 19 To display the active wired guest LAN clients, enter 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 20 To display detailed information for a specific client, enter 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
...
```

CHAPTER 11

Configuring Radio Resource ManagementWireless Device Access

This chapter describes radio resource management (RRM) and explains how to configure it on the controllers. It contains these sections:

- Overview of Radio Resource Management, page 11-2
- Overview of RF Groups, page 11-5
- Configuring an RF Group, page 11-6
- Viewing RF Group Status, page 11-8
- Configuring RRM, page 11-9
- Overriding RRM, page 11-25
- Enabling Rogue Access Point Detection in RF Groups, page 11-34
- Configuring CCX Radio Management Features, page 11-36
- Configuring Pico Cell Mode, page 11-41

Overview of 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. In this way, administrators gain the perspective of every access point, thereby increasing network visibility.

Transmit Power Control

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the access points’ transmit power according to how the access points are seen by their third strongest neighbor.

The transmit power control algorithm only reduces an access point's power. However, the coverage hole algorithm, explained below, can increase access point power, thereby filling a coverage hole. For example, if a failed access point is detected, the coverage hole algorithm can automatically increase power on surrounding access points to fill the gap created by the loss in coverage.

Note See Step 7 on page 11-29 for an explanation of the transmit power levels.

Dynamic Channel Assignment

Two adjacent access points on the same channel can cause either signal contention or signal collision. In the case of a collision, data is simply 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 address this problem by dynamically allocating 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 band, such as 1 and 2, cannot both simultaneously use 11/54 Mbps. By effectively reassigning channels, the controller keeps adjacent channels separated, thereby avoiding this problem.

The controller examines a variety of real-time RF characteristics to efficiently handle channel assignments. These include:

- **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 non-overlapping 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 (and therefore utilization) reported.
- **Load**—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, 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, you can choose between DCA working at 20 or 40 MHz.

Note Radios using 40-MHz channels in the 2.4-GHz band are not supported by DCA.

Coverage Hole Detection and Correction

The RRM coverage hole detection algorithm is designed to 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 is not a remedy for poor upstream performance and might increase interference in the network.

Note While transmit power control and DCA can operate in multi-controller environments (based on RF domains), coverage hole detection is performed on a per-controller basis. In controller software release 5.2, you can disable coverage hole detection on a per-WLAN basis. See the "Disabling Coverage Hole Detection per WLAN" section on page 6-54 for more information.

RRM Benefits

RRM produces a network with optimal capacity, performance, and reliability while enabling you to avoid the cost of laborious historical data interpretation and individual lightweight access point reconfiguration. It also frees you from having to continually monitor the network for noise and interference problems, which can be transient and difficult to troubleshoot. Finally, 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 and 802.11b/g. That is, the RRM algorithms run separately for each radio type (802.11a and 802.11b/g). RRM uses both measurements and algorithms. RRM measurements can be adjusted using monitor intervals, but they cannot be disabled. RRM algorithms, on the other hand, 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.

Overview of RF Groups

An RF group, also known as an RF domain, is a cluster of controllers that coordinates its RRM calculations on a per 802.11-network basis. An RF group exists for each 802.11 network type. Clustering controllers into RF groups enables the RRM algorithms to scale beyond a single controller.

Lightweight access points periodically send out neighbor messages over the air. Access points using the the same RF group name are able to 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 group.

Note RF groups and mobility groups are similar in that they both define clusters of controllers, but they are different in terms of their use. These two concepts are often confused because the mobility group name and RF group name are configured to be the same in the Startup Wizard. Most of the time, all of the controllers in an RF group are also in the same mobility group and vice versa. However, an RF group facilitates scalable, system-wide dynamic RF management while a mobility group facilitates scalable, system-wide mobility and controller redundancy. Refer to Chapter 12 for more information on mobility groups.

Controller software release 4.2.99.0 or later supports 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 10 4404 controllers in an RF group (100 x 10 = 1000). The 2100-series-based controllers support a maximum of 25 access points, so you can have up to 20 of these controllers in an RF group.

Note In controller software release 4.2.61.0 or earlier, RRM supports no more than five 4400-series-based controllers in an RF group.

RF Group Leader

The members of an RF group elect an RF group leader to maintain a "master" power and channel scheme for the group. The RF group leader is dynamically chosen and cannot be selected by the user. In addition, the RF group leader can change at any time, depending on the RRM algorithm calculations.

The RF group leader analyzes real-time radio data collected by the system and calculates the master power and channel plan. The RRM algorithms employ dampening calculations to minimize system-wide dynamic changes. The end result is dynamically calculated optimal power and channel planning that is responsive to an always changing RF environment.

The RRM algorithms run at a specified updated interval, which is 600 seconds by default. Between update intervals, the RF group leader sends keep-alive messages to each of the RF group members and collects real-time RF data.

Note Several monitoring intervals are also available. See the "Configuring RRM" section on page 11-9 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 simply 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, the controllers should be configured 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.

Configuring an RF Group

This section provides instructions for configuring 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.

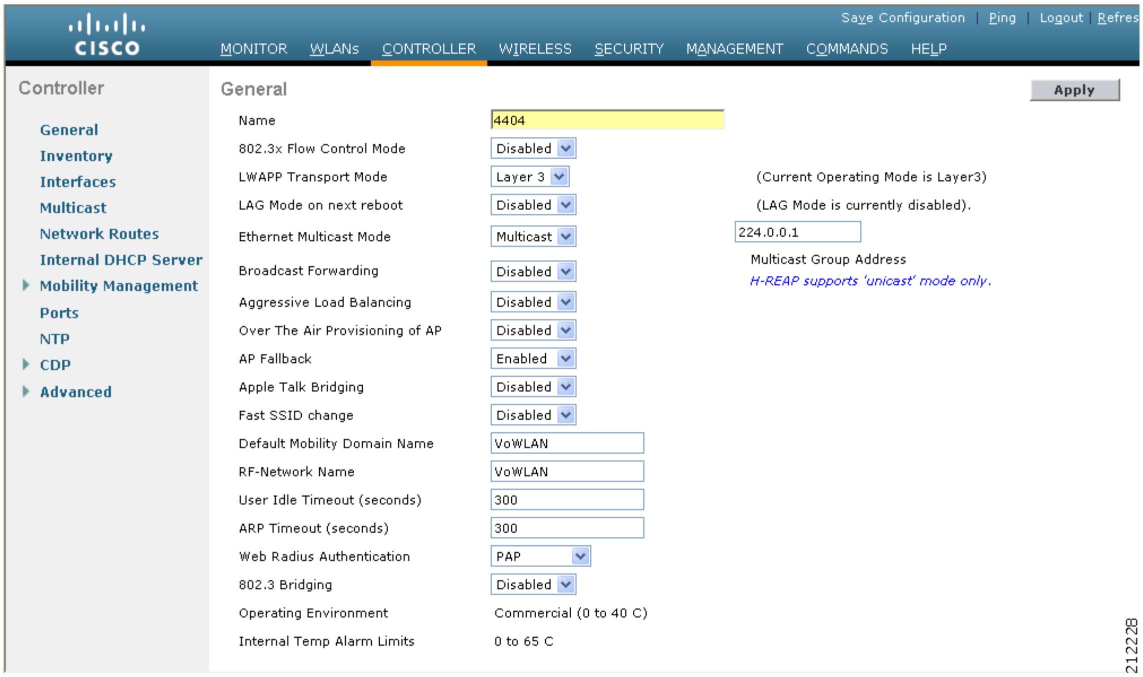
Note You can also configure RF groups using the Cisco Wireless Control System (WCS). Refer to the *Cisco Wireless Control System Configuration Guide* for instructions.

Using the GUI to Configure an RF Group

Follow these steps to create an RF group using the GUI.

Step 1 Click **Controller** > **General** to open the General page (see Figure 11-1).

Figure 11-1 General Page



General

Name	4404	
802.3x Flow Control Mode	Disabled	
LWAPP Transport Mode	Layer 3	(Current Operating Mode is Layer3)
LAG Mode on next reboot	Disabled	(LAG Mode is currently disabled).
Ethernet Multicast Mode	Multicast	224.0.0.1 Multicast Group Address H-REAP supports 'unicast' mode only.
Broadcast Forwarding	Disabled	
Aggressive Load Balancing	Disabled	
Over The Air Provisioning of AP	Disabled	
AP Fallback	Enabled	
Apple Talk Bridging	Disabled	
Fast SSID change	Disabled	
Default Mobility Domain Name	VoWLAN	
RF-Network Name	VoWLAN	
User Idle Timeout (seconds)	300	
ARP Timeout (seconds)	300	
Web Radius Authentication	PAP	
802.3 Bridging	Disabled	
Operating Environment	Commercial (0 to 40 C)	
Internal Temp Alarm Limits	0 to 65 C	

Step 2 Enter a name for the RF group in the RF-Network Name field. 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.

Using the CLI to Configure RF Groups

Follow these steps to configure an RF group using the CLI.

Step 1 Enter **config network rf-network-name** *name* to create an RF group.

Note Enter up to 19 ASCII characters for the group name.

Step 2 Enter **show network** to view the RF group.

Step 3 Enter **save config** to save your settings.

Step 4 Repeat this procedure for each controller that you want to include in the RF group.

Viewing RF Group Status

This section provides instructions for viewing the status of the RF group through either the GUI or the CLI.

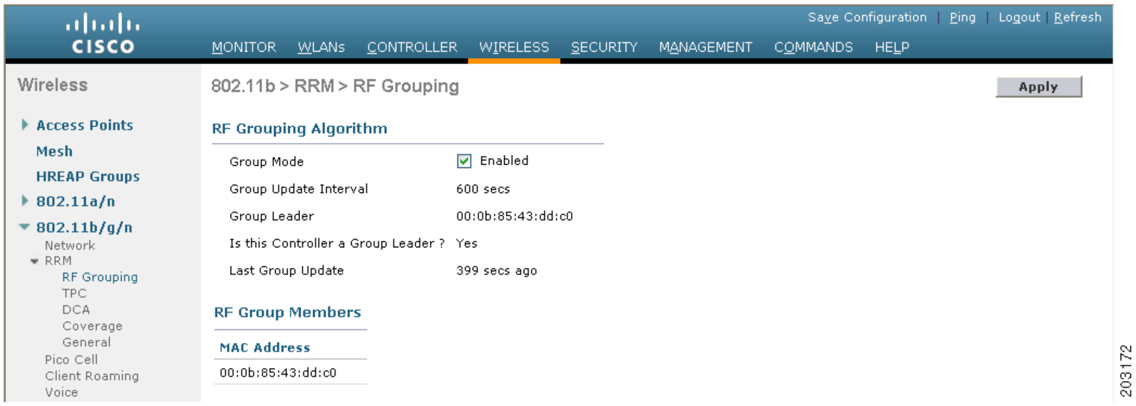
Note You can also view the status of RF groups using the Cisco Wireless Control System (WCS). Refer to the *Cisco Wireless Control System Configuration Guide* for instructions.

Using the GUI to View RF Group Status

Follow these steps to view the status of the RF group using the GUI.

Step 1 Click **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 (see Figure 11-2).

Figure 11-2 802.11a > RRM > RF Grouping Page



802.11b > RRM > RF Grouping

RF Grouping Algorithm

Group Mode	☑ Enabled
Group Update Interval	600 secs
Group Leader	00:0b:85:43:dd:c0
Is this Controller a Group Leader ?	Yes
Last Group Update	399 secs ago

RF Group Members

MAC Address
00:0b:85:43:dd:c0

This page shows the details of the RF group, specifically how often the group information is updated (600 seconds by default), the MAC address of the RF group leader, whether this particular controller is the group leader, the last time the group information was updated, and the MAC addresses of all group members.

Note Automatic RF grouping, which is set through the **Group Mode** check box, is enabled by default. See the "Using the GUI to Configure RF Group Mode" section on page 11-10 for more information on this parameter.

Step 2 If desired, repeat this procedure for the network type you did not select (802.11a or 802.11b/g).

Using the CLI to View RF Group Status

Follow these steps to view the status of the RF group using the CLI.

Step 1 Enter **show advanced 802.11a group** to see which controller is the RF group leader for the 802.11a RF network. Information similar to the following appears:

```
Radio RF Grouping
      802.11a Group Mode............................. AUTO
      802.11a Group Update Interval.................. 600 seconds
      802.11a Group Leader........................... 00:16:9d:ca:d9:60
        802.11a Group Member........................ 00:16:9d:ca:d9:60
      802.11a Last Run........................... 594 seconds ago
```

This text shows the details of the RF group, specifically whether automatic RF grouping is enabled for this controller, how often the group information is updated (600 seconds by default), the MAC address of the RF group leader, the MAC address of this particular controller, and the last time the group information was updated.

Note If the MAC addresses of the group leader and the group member are identical, this controller is currently the group leader.

Step 2 Enter **show advanced 802.11b group** to see which controller is the RF group leader for the 802.11b/g RF network.

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 GUI to Configure RRM

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. To configure these parameters, follow the instructions in the subsections below.

Using the GUI to Configure RF Group Mode

Using the controller GUI, follow these steps to configure RF group mode.

Step 1 Click **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 (see Figure 11-2).

Step 2 Check the **Group Mode** check box to enable this controller to participate in an RF group, or uncheck it to disable this feature. If you enable this feature, the controller automatically forms an RF group with other controllers, and the group dynamically elects a leader to optimize RMM parameter settings for the the group. If you disable it, the controller does not participate in automatic RF grouping; instead it optimizes the access points connected directly to it. The default value is checked.

Note Cisco recommends that controllers participate in automatic RF grouping. Note that you can override RRM settings without disabling automatic RF group participation. See the "Overriding RRM" section on page 11-25 for instructions.

Step 3 Click **Apply** to commit your changes.

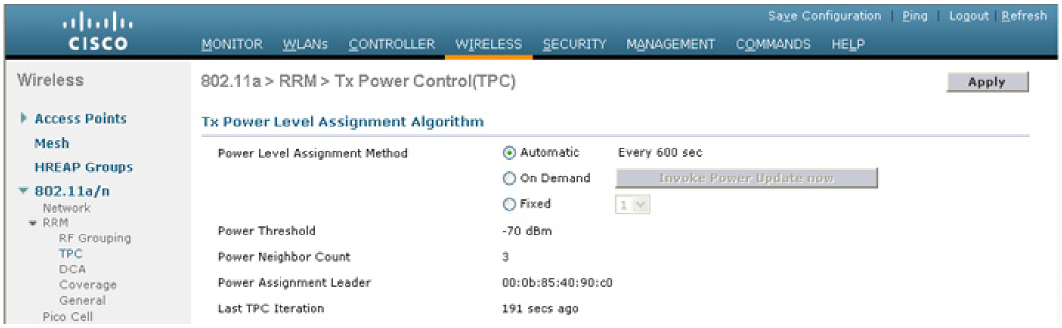
Step 4 Click **Save Configuration** to save your changes.

Using the GUI to Configure Transmit Power Control

Using the controller GUI, follow these steps to configure transmit power control settings.

Step 1 Click **Wireless** > **802.11a/n** or **802.11b/g/n** > **RRM** > **TPC** to open the 802.11a (or 802.11b/g) > RRM > Tx Power Control (TPC) page (see Figure 11-3).

Figure 11-3 802.11a > RRM > Tx Power Control (TPC) Page



802.11a > RRM > Tx Power Control(TPC)

Tx Power Level Assignment Algorithm

Power Level Assignment Method	● Automatic	Every 600 sec
	○ On Demand	
	○ Fixed	1
Power Threshold	-70 dBm	
Power Neighbor Count	3	
Power Assignment Leader	00:0b:85:40:90:c0	
Last TPC Iteration	191 secs ago	

Step 2 Choose one of the following options from the Power Level Assignment Method drop-down box 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 box.

  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 in which the access points are deployed. See Step 7 on page 11-29 for information on available transmit power levels.

Note For optimal performance, Cisco recommends that you use the Automatic setting. Refer to the "Disabling Dynamic Channel and Power Assignment Globally for a Controller" section on page 11-33 for instructions if you ever need to disable the controller's dynamic channel and power settings.

This page also shows the following non-configurable transmit power level parameter settings:

- **Power Threshold—**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 but can be changed through the controller CLI on rare occasions when access points are transmitting at higher (or lower) than desired power levels. See the "Using the CLI to Configure RRM" section on page 11-19 for the CLI command.
- **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 TPC Iteration**—The last time RRM evaluated the current transmit power level assignments.

Step 3 Click **Apply** to commit your changes.

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

Using the GUI to Configure Dynamic Channel Assignment

Using the controller GUI, follow these steps to specify the channels that the dynamic channel assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning. This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

Step 1 To disable the 802.11a or 802.11b/g network, follow these steps:

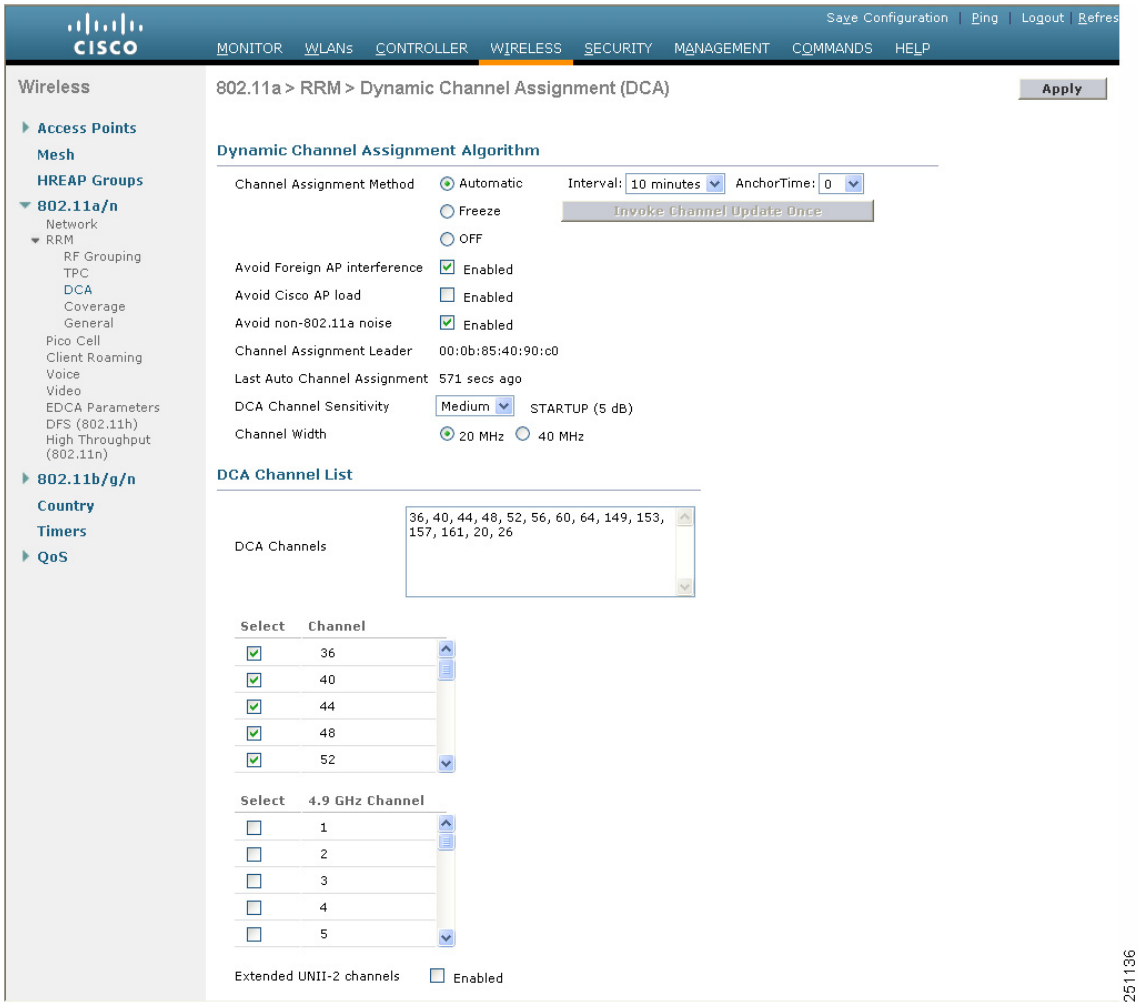
a. Click **Wireless** > **802.11a/n** or **802.11b/g/n** > **Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

Step 2 Click **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 (see Figure 11-4).

Figure 11-4 802.11a > RRM > Dynamic Channel Assignment (DCA) Page



802.11a > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

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

Avoid Foreign AP interference ☑ Enabled
Avoid Cisco AP load □ Enabled
Avoid non-802.11a noise ☑ Enabled
Channel Assignment Leader 00:0b:85:40:90:c0
Last Auto Channel Assignment 571 secs ago
DCA Channel Sensitivity Medium STARTUP (5 dB)
Channel Width ● 20 MHz ○ 40 MHz

DCA Channel List

DCA Channels 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 20, 26

Select	Channel
☑	36
☑	40
☑	44
☑	48
☑	52

Select	4.9 GHz Channel
□	1
□	2
□	3
□	4
□	5

Extended UNII-2 channels □ Enabled

Step 3 Choose one of the following options from the Channel Assignment Method drop-down box 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, Cisco recommends that you use the Automatic setting. Refer to the "Disabling Dynamic Channel and Power Assignment Globally for a Controller" section on page 11-33 for instructions if you ever need to disable the controller's dynamic channel and power settings.

Step 4 From the Interval drop-down box, 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 box, 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 Check 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 uncheck 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 Check 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 uncheck 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 unchecked.

Step 8 Check 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 uncheck it to disable this feature. For example, RRM may have access points avoid channels with significant interference from non-access point sources, such as microwave ovens. The default value is checked.

Step 9 From the DCA Channel Sensitivity drop-down box, 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 11-1.

Table 11-1 DCA Sensitivity Thresholds

Option	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

Step 10 For 802.11a/n networks only, choose one of the following Channel Width options to specify the channel bandwidth supported for all 802.11n 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 11 (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.

Note If you choose 40 MHz, you can also configure the primary and extension channels used by individual access points. Refer to the "Using the GUI to Statically Assign Channel and Transmit Power Settings" section on page 11-26 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 on the 802.11a/n Cisco APs > Configure page. If you ever then change the static RF channel assignment method to Global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

This page also shows the following non-configurable 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, check its check box in the Select column. To exclude a channel, uncheck its check box.

Range:
802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165, 190, 196
802.11b/g—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

Default:
802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161
802.11b/g—1, 6, 11

Note These extended UNII-2 channels in the 802.11a band do not appear in the channel list: 100, 104, 108, 112, 116, 132, 136, and 140. If you have Cisco Aironet 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, check the **Extended UNII-2 Channels** check box.

Step 12 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 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, check its check box in the Select column. To exclude a channel, uncheck 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 re-enable 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. Check the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

Step 15 Click **Save Configuration** to save your changes.

Note To see why the DCA algorithm changed channels, click **Monitor** and then **View All** under Most Recent Traps. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change.

Using the GUI to Configure Coverage Hole Detection

Using the controller GUI, follow these steps to enable coverage hole detection.

Note In controller software release 5.2, you can disable coverage hole detection on a per-WLAN basis. See the "Disabling Coverage Hole Detection per WLAN" section on page 6-54 for more information.

Step 1 To disable the 802.11a or 802.11b/g network, follow these steps:

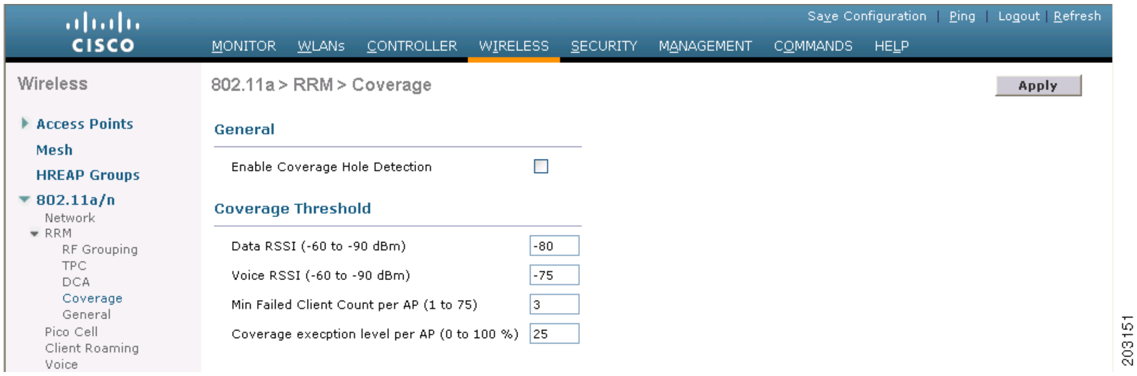
a. Click **Wireless** > **802.11a/n** or **802.11b/g/n** > **Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

Step 2 Click **Wireless** > **802.11a/n** or **802.11b/g/n** > **RRM** > **Coverage** to open the 802.11a (or 802.11b/g) > RRM > Coverage page (see Figure 11-5).

Figure 11-5 802.11a > RRM > Coverage Page



802.11a > RRM > Coverage

General

Enable Coverage Hole Detection	☐

Coverage Threshold

Data RSSI (-60 to -90 dBm)	-80
Voice RSSI (-60 to -90 dBm)	-75
Min Failed Client Count per AP (1 to 75)	3
Coverage execption level per AP (0 to 100 %)	25

Step 3 Check the **Enable Coverage Hole Detection** check box to enable coverage hole detection, or uncheck 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 checked.

Step 4 In the Data RSSI field, 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 –60 to –90 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 field, 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 –60 to –90 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 field, 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 field, 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; see page 11-22) 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 fields 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 To re-enable 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. Check the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

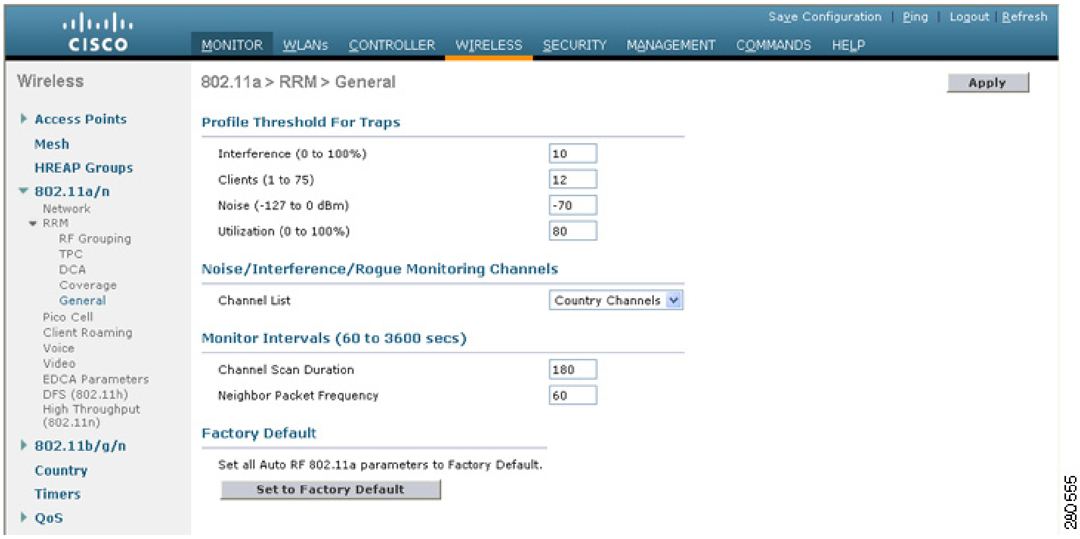
Step 10 Click **Save Configuration** to save your changes.

Using the GUI to Configure RRM Profile Thresholds, Monitoring Channels, and Monitor Intervals

Using the controller GUI, follow these steps to configure RRM profile thresholds, monitoring channels, and monitor intervals.

Step 1 Click **Wireless** > **802.11a/n** or **802.11b/g/n** > **RRM** > **General** to open the 802.11a (or 802.11b/g) > RRM > General page (see Figure 11-6).

Figure 11-6 802.11a > RRM > General Page



802.11a > RRM > General

Profile Threshold For Traps

Interference (0 to 100%)	10
Clients (1 to 75)	12
Noise (-127 to 0 dBm)	-70
Utilization (0 to 100%)	80

Noise/Interference/Rogue Monitoring Channels

Channel List	Country Channels

Monitor Intervals (60 to 3600 secs)

Channel Scan Duration	180
Neighbor Packet Frequency	60

Factory Default

Set all Auto RF 802.11a parameters to Factory Default.

Step 2 To configure profile thresholds used for alarming, follow these steps.

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 field, 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 field, 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 field, 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 field, 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 box, 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 "Using the GUI to Configure Dynamic Channel Assignment" section on page 11-12.

Step 4 To configure monitor intervals, follow these steps:

a. In the Channel Scan Duration field, 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 Channel Scan Duration interval. 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 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 Duration 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 radios.

b. In the Neighbor Packet Frequency field, 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 In controller software release 4.1.185.0 or later, 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.

Note Click **Set to Factory Default** if you ever want to return all of the controller's RRM parameters to their factory default values.

Using the CLI to Configure RRM

Using the controller CLI, follow these steps to configure RRM.

Step 1 Enter this command to disable the 802.11a or 802.11b/g network:

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

Step 2 Perform one of the following to configure transmit power control:

- To have RRM automatically set the transmit power for all 802.11a or 802.11b/g 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 or 802.11b/g radios one time, enter this command:

  config {**802.11a** | **802.11b**} **txPower global once**

- To manually change the default transmit power setting of –70 dBm, enter this command:

  config advanced {**802.11a** | **802.11b**} **tx-power-control-thresh** *threshold*

  where *threshold* is a value from –50 to –80 dBm. Increasing this value (between –50 and –65 dBm) 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 –75 or –80 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.

  Note See the Power Threshold description in "Using the GUI to Configure Transmit Power Control" section on page 11-10 for more information.

Step 3 Perform one of the following to configure dynamic channel assignment (DCA):

- To have RRM automatically configure all 802.11a or 802.11b/g 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 or 802.11b/g 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 4 Use these commands to configure additional DCA parameters:

- **config advanced** {**802.11a** | **802.11b**} **channel dca anchor-time** *value*—Specifies the time of day when the DCA algorithm is to start. *Valu*e is a number between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.
- **config advanced** {**802.11a** | **802.11b**} **channel dca interval** *value*—Specifies how often the DCA algorithm is allowed to run. *Valu*e 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).
- **config advanced** {**802.11a** | **802.11b**} **channel dca sensitivity** {**low** | **medium** | **high**}—Specifies how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channel.
  - **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 11-2.

Table 11-2 DCA Sensitivity Thresholds

Option	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

- **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 3 (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. Refer to the "Using the CLI to Statically Assign Channel and Transmit Power Settings" section on page 11-30 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 ever 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 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 5 Use these commands to configure coverage hole detection:

Note In controller software release 5.2, you can disable coverage hole detection on a per-WLAN basis. See the "Disabling Coverage Hole Detection per WLAN" section on page 6-54 for more information.

- **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 –60 to –90 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 6 Enter this command to enable the 802.11a or 802.11b/g network:

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 7 Enter this command to save your settings:

save config

Using the CLI to View RRM Settings

Use these commands to view 802.11a and 802.11b/g RRM settings:

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

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
```

- **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 or 802.11b/g receiver configuration and statistics.

```
802.11a Advanced Receiver Settings
 RxStart  : Signal Threshold..................... 15
 RxStart  : Signal Jump Threshold................ 5
 RxStart  : Preamble Power Threshold............. 2
 RxRestart: Signal Jump Status................... Enabled
 RxRestart: 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
 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 or 802.11b/g access points

```
AP Name                       Channel     TxPower Level
----------------------------- ----------- ----------------
AP1250                        (36, 40)        1
```

- **txpower**—Shows the transmit power assignment configuration and statistics.

```
Automatic Transmit Power Assignment
  Transmit Power Assignment Mode................. AUTO
  Transmit Power Update Interval................. 600 seconds
  Transmit Power Threshold....................... -65 dBm
  Transmit Power Neighbor Count.................. 3 APs
  Transmit Power Update Contribution............. SNI.
  Transmit Power Assignment Leader............... 00:0b:85:43:dd:c0
  Last Run....................................... 360 seconds ago
```

Using the CLI to Debug RRM Issues

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.

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. Follow the instructions in one of the following sections:

- Statically Assigning Channel and Transmit Power Settings to Access Point Radios, page 11-26
- Disabling Dynamic Channel and Power Assignment Globally for a Controller, page 11-33

Note 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.

Statically Assigning Channel and Transmit Power Settings to Access Point Radios

This section provides instructions for statically assigning channel and power settings using the GUI or CLI.

Note Cisco recommends 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 network.

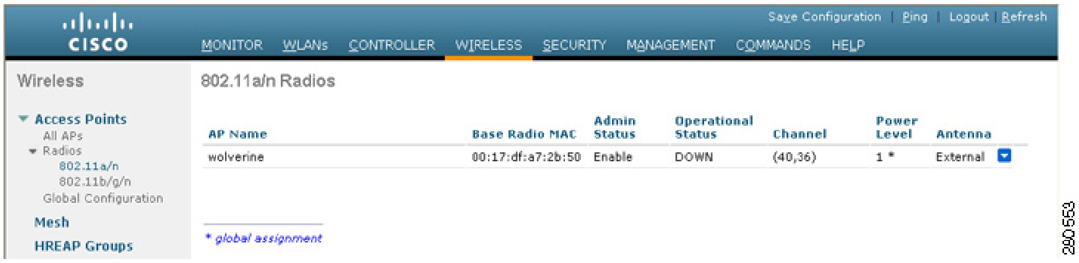
Note Cisco recommends that you do not assign all access points that are within close proximity to each other to the maximum power level.

Using the GUI to Statically Assign Channel and Transmit Power Settings

Follow these steps to statically assign channel and/or power settings on a per access point radio basis using the GUI.

Step 1 Click **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 (see Figure 11-7).

Figure 11-7 802.11a/n Radios Page



802.11a/n Radios

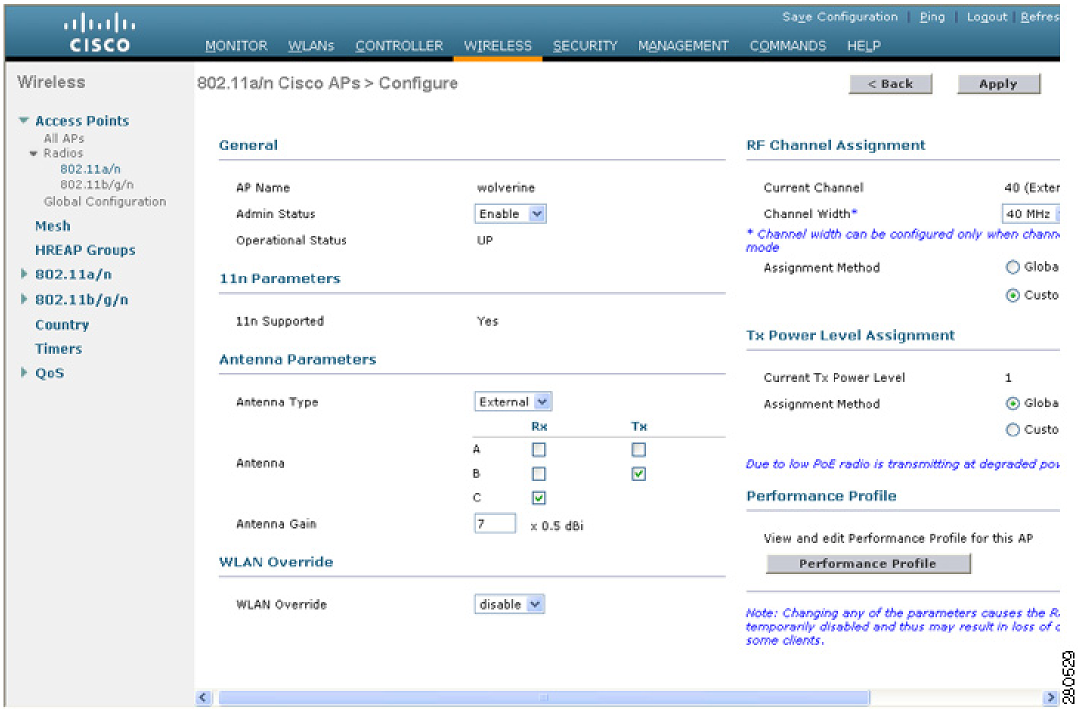
AP Name	Base Radio MAC	Admin Status	Operational Status	Channel	Power Level	Antenna
wolverine	00:17:df:a7:2b:50	Enable	DOWN	(40,36)	1 *	External

* global assignment

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 field 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 (see Figure 11-8).

Figure 11-8 802.11a/n Cisco APs > Configure Page



802.11a/n Cisco APs > Configure

General

AP Name wolverine

Admin Status Enable

Operational Status UP

11n Parameters

11n Supported Yes

Antenna Parameters

Antenna Type External

Antenna		Rx	Tx
	A	□	□
	B	□	☑
	C	☑	

Antenna Gain 7 x 0.5 dBi

WLAN Override

WLAN Override disable

RF Channel Assignment

Current Channel 40 (Exter

Channel Width* 40 MHz

* Channel width can be configured only when chann mode

Assignment Method ○ Globa ● Custo

Tx Power Level Assignment

Current Tx Power Level 1

Assignment Method ● Globa ○ Custo

Due to low PoE radio is transmitting at degraded pov

Performance Profile

View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the R temporarily disabled and thus may result in loss of c some clients.

Step 3 To be able to assign primary and extension channels to the access point radio, choose **Custom** for the Assignment Method under RF Channel Assignment.

Step 4 Choose one of the following options from the Channel Width drop-down box:

- **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. Conversely, if you choose a primary channel of 48, the controller would use channel 44 as the extension channel.

  Note Cisco recommends that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe co-channel interference can occur.

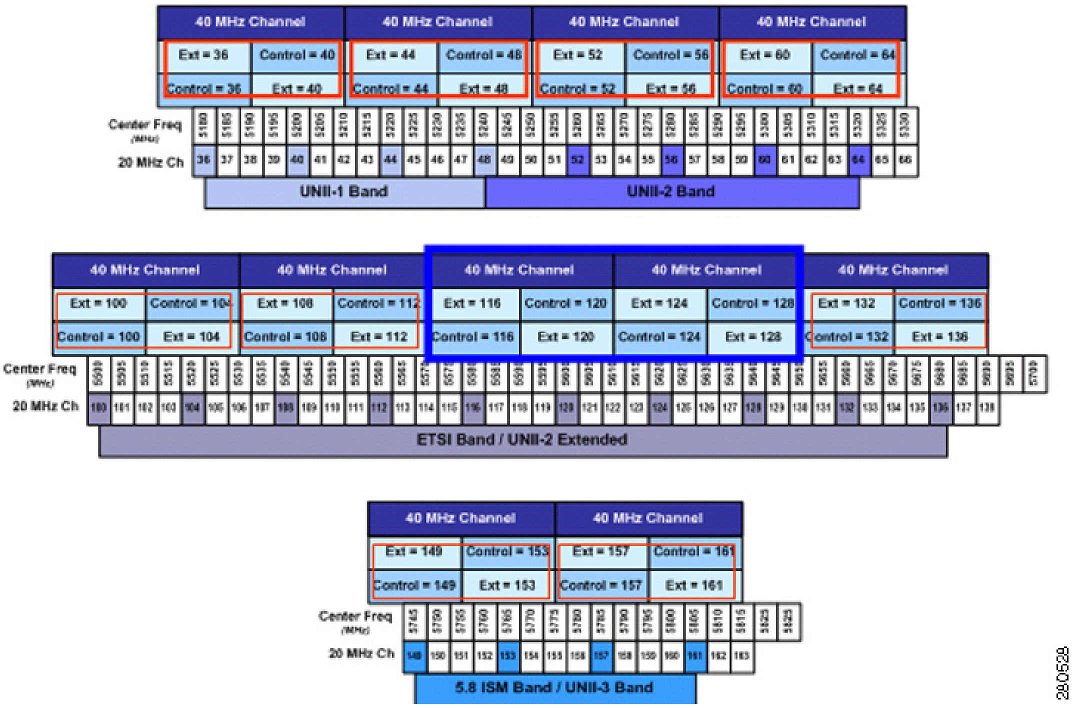
Note The Channel Width parameter can be configured for 802.11a/n radios only if the RF channel assignment method is in custom mode and for 802.11b/g/n radios only if both the RF channel assignment method and the Tx power level assignment method are in custom mode.

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 ever 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 11-9 illustrates 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 11-9 Channel Bonding in the 5-GHz Band



Step 5 Follow these steps to configure the antenna parameters for this radio:

a. From the Antenna Type drop-down box, choose **Internal** or **External** to specify the type of antennas used with the access point radio.

b. Check and uncheck the check boxes in the Antenna field 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 check the following check boxes: Tx: A and B and Rx: C.

c. In the Antenna Gain field, 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 (refer to the *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.

d. Choose one of the following options from the Diversity drop-down box:

- **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 To assign an RF channel to the access point radio, choose **Custom** for the Assignment Method under RF Channel Assignment and choose a channel from the drop-down box.

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 MHz for the channel width in Step 4.

Note The Current Channel field shows the current primary channel. If you chose 40 MHz for the channel width in Step 4, the extension channel appears in parentheses after the primary channel.

Note Changing the operating channel causes the access point radio to reset.

Step 7 To assign a transmit power level to the access point radio, choose **Custom** for the Assignment Method under Tx Power Level Assignment and choose a transmit power level from the drop-down box.

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 Refer to the hardware installation guide for your access point for the maximum transmit power levels supported per regulatory domain. Also, refer to 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. Refer to the "Configuring Power over Ethernet" section on page 7-70 for more information on PoE power levels.

Step 8 To enable this configuration for the access point, choose **Enable** from the Admin Status drop-down box.

Step 9 Click **Apply** to commit your changes.

Step 10 To have the controller send the access point radio admin state immediately to WCS, 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. Check the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save the changes to the access point radio.

Step 12 Repeat this procedure for each access point radio for which you want to assign a static channel and power level.

Using the CLI to Statically Assign Channel and Transmit Power Settings

Follow these steps to statically assign channel and/or power settings on a per access point radio basis using the CLI.

Step 1 To disable the radio of a particular access point on the 802.11a or 802.11b/g network, enter this command:

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

Step 2 To configure the channel width for a particular access point, enter 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. Conversely, 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 Cisco recommends that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe co-channel interference can occur.

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 11-9 on page 11-28 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 To enable or disable the use of specific antennas for a particular access point, enter 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 the following command:

config 802.11a 11nsupport antenna tx AP1 C enable

Step 4 To 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, enter 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 (refer to the *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 To specify the channel that a particular access point is to use, enter this command:

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

Example: To configure 802.11a channel 36 as the default channel on AP1, enter this command: **config 802.11a channel ap AP1 36**.

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 To specify the transmit power level that a particular access point is to use, enter this command:

config {**802.11a** | **802.11b**} **txPower ap** *Cisco_AP power_level*

Example: To set the transmit power for 802.11a AP1 to power level 2, enter this command: **config 802.11a txPower ap AP1 2**.

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 Refer to the hardware installation guide for your access point for the maximum transmit power levels supported per regulatory domain. Also, refer to the data sheet for your access point for the number of power levels supported.

Step 7 To save your settings, enter 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 To re-enable the access point radio, enter this command:

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

Step 10 To have the controller send the access point radio admin state immediately to WCS, enter this command:

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

Step 11 To save your settings, enter this command:

save config

Step 12 To see the configuration of a particular access point, enter this command:

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

Information similar to the following appears:

```
Cisco AP Identifier.............................. 7
Cisco AP Name.................................... AP1
...
Tx Power
Num Of Supported Power Levels ................... 8
      Tx Power Level 1 .......................... 20 dBm
      Tx Power Level 2 .......................... 17 dBm
      Tx Power Level 3 .......................... 14 dBm
      Tx Power Level 4 .......................... 11 dBm
      Tx Power Level 5 .......................... 8 dBm
      Tx Power Level 6 .......................... 5 dBm
      Tx Power Level 7 .......................... 2 dBm
      Tx Power Level 8 .......................... -1 dBm
      Tx Power Configuration .................... CUSTOMIZED
      Current Tx Power Level .................... 1
Phy OFDM parameters
      Configuration ............................. CUSTOMIZED
      Current Channel ........................... 36
      Extension Channel ......................... 40
      Channel Width.............................. 40 Mhz
      Allowed Channel List....................... 36,44,52,60,100,108,116,132,149,157
      TI Threshold .............................. -50
      Antenna Type............................... EXTERNAL_ANTENNA
      External Antenna Gain (in .5 dBi units).... 7
      Diversity.................................. DIVERSITY_ENABLED
802.11n Antennas
        Tx
         A....................................... ENABLED
         B....................................... ENABLED
        Rx
         A....................................... DISABLED
         B....................................... DISABLED
         C.................................... ENABLED
```

Disabling Dynamic Channel and Power Assignment Globally for a Controller

This section provides instructions for disabling dynamic channel and power assignment using the GUI or CLI.

Using the GUI to Disable Dynamic Channel and Power Assignment

Follow these steps to configure disable dynamic channel and power assignment using the GUI.

Step 1 Click **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 (see Figure 11-2).

Step 2 To disable dynamic channel assignment, choose **OFF** under RF Channel Assignment.

Step 3 To disable dynamic power assignment, choose **Fixed** under Tx Power Level Assignment and choose a default transmit power level from the drop-down box.

Note See Step 7 on page 11-29 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 If desired, repeat this procedure for the network type you did not select (802.11a or 802.11b/g).

Using the CLI to Disable Dynamic Channel and Power Assignment

Follow these steps to disable RRM for all 802.11a or 802.11b/g radios.

Step 1 Enter this command to disable the 802.11a or 802.11b/g network:

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

Step 2 Enter this command to disable RRM for all 802.11a or 802.11b/g radios and set all channels to the default value:

config {**802.11a** | **802.11b**} **channel global off**

Step 3 Enter this command to enable the 802.11a or 802.11b/g network:

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 4 Enter this command to save your settings:

save config

Enabling 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 check 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 check 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.

Using the GUI to Enable Rogue Access Point Detection in RF Groups

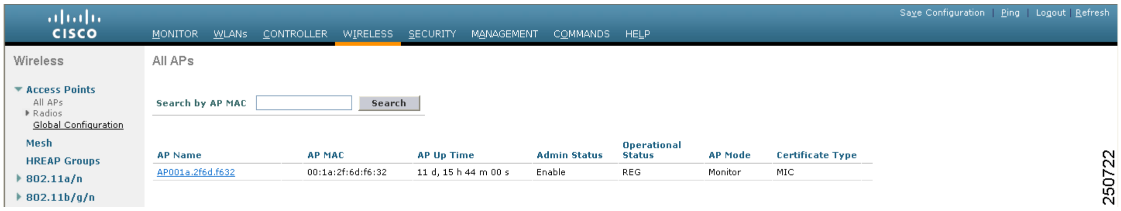
Using the controller GUI, follow these steps to enable rogue access point detection in RF groups.

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 Click **Wireless** to open the All APs page (see Figure 11-10).

Figure 11-10 All APs Page


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Save Configuration | Ping | Logout | Refresh
Wireless
Access Points
All APs
Radios
Global Configuration
Mesh
HREAP Groups
802.11a/n
802.11b/g/n
Search
250722

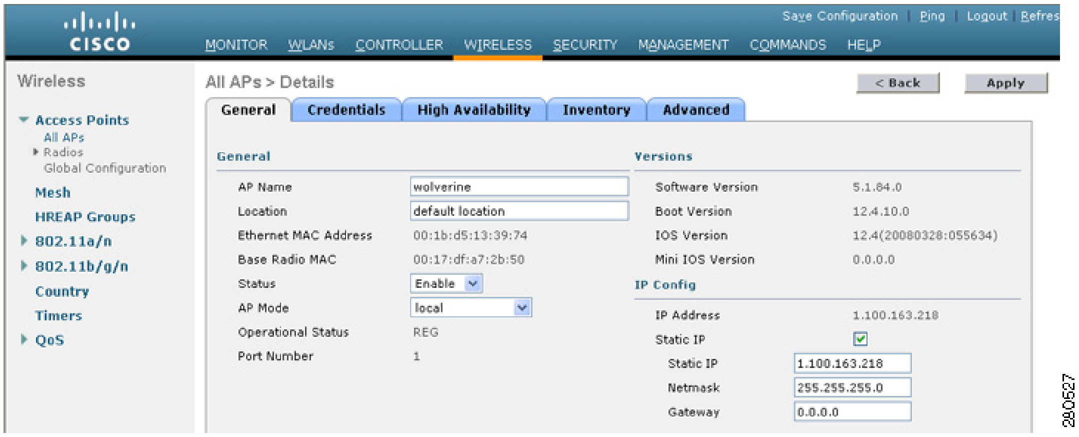
All APs

Search by AP MAC

AP Name	AP MAC	AP Up Time	Admin Status	Operational Status	AP Mode	Certificate Type
AP001a.2f6d.f632	00:1a:2f:6d:f6:32	11 d, 15 h 44 m 00 s	Enable	REG	Monitor	MIC

Step 3 Click the name of an access point to open the All APs > Details page (see Figure 11-11).

Figure 11-11 All APs > Details Page



All APs > Details

General

AP Name: wolverine
Location: default location
Ethernet MAC Address: 00:1b:d5:13:39:74
Base Radio MAC: 00:17:df:a7:2b:50
Status: Enable
AP Mode: local
Operational Status: REG
Port Number: 1

Versions

Software Version: 5.1.84.0
Boot Version: 12.4.10.0
IOS Version: 12.4(20080328:055634)
Mini IOS Version: 0.0.0.0

IP Config

IP Address: 1.100.163.218
Static IP: ☑
Static IP: 1.100.163.218
Netmask: 255.255.255.0
Gateway: 0.0.0.0

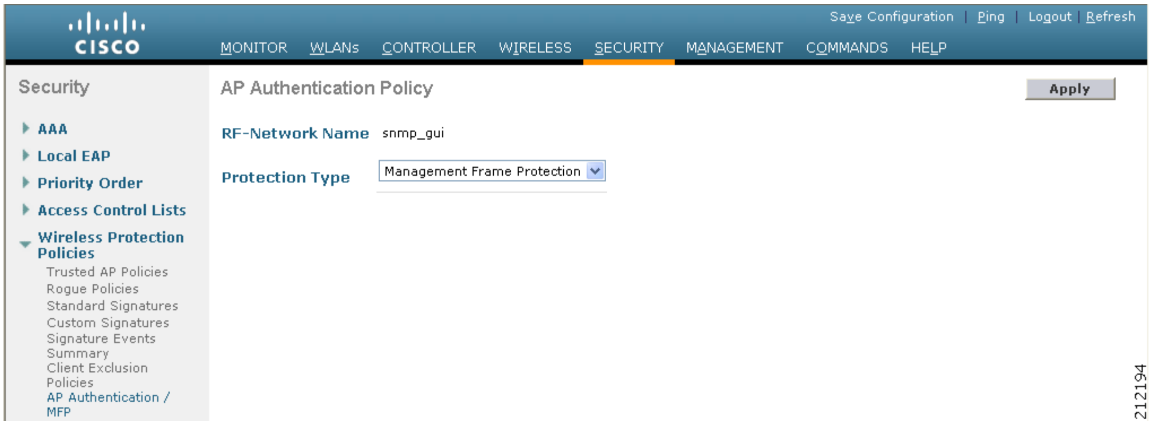
Step 4 Choose either **local** or **monitor** from the AP Mode drop-down box and click **Apply** to commit your changes.

Step 5 Click **Save Configuration** to save your changes.

Step 6 Repeat Step 2 through Step 5 for every access point connected to the controller.

Step 7 Click **Security** > **Wireless Protection Policies** > **AP Authentication/MFP** to open the AP Authentication Policy page (see Figure 11-12).

Figure 11-12 AP Authentication Policy Page



AP Authentication Policy

RF-Network Name snmp_gui

Protection Type Management Frame Protection

The name of the RF group to which this controller belongs appears at the top of the page.

Step 8 Choose **AP Authentication** from the Protection Type drop-down box to enable rogue access point detection.

Step 9 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.

Note The valid threshold range is from1 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 10 Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Step 12 Repeat this procedure on every controller in the RF group.

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.

Using the CLI to Enable Rogue Access Point Detection in RF Groups

Using the controller CLI, follow these steps to enable rogue access point detection in RF groups.

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 Enter **config ap mode local** *Cisco_AP* or **config ap mode monitor** *Cisco_AP* to configure this particular access point for local (normal) mode or monitor (listen-only) mode.

Step 3 Enter **save config** to save your settings.

Step 4 Repeat Step 2 and Step 3 for every access point connected to the controller.

Step 5 Enter **config wps ap-authentication** to enable rogue access point detection.

Step 6 Enter **config wps ap-authentication** *threshold* 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.

Note The valid threshold range is from1 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 Enter **save config** to save your settings.

Step 8 Repeat Step 5 through Step 7 on every controller in the RF group.

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.

Configuring 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 higher and are designed to enhance location accuracy and timeliness for participating CCX clients. See the "Configuring Cisco Client Extensions" section on page 6-39 for more information on CCX.

For the location features to operate properly, the access points must be configured for normal, monitor, or hybrid-REAP mode. However, for hybrid-REAP mode, the access point must be connected to the controller.

Note CCX is not supported on the AP1030.

Radio Measurement Requests

When this feature is enabled, lightweight access points issue broadcast radio measurement request messages to clients running CCXv2 or higher. 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, 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 on 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 twenty 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.

Controller software release 4.1 or later also improves the ability of the Location Appliance to accurately interpret the location of a device through a new 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 simply ignore the CCX measurement requests and therefore do not participate in the radio measurement activity.

Location Calibration

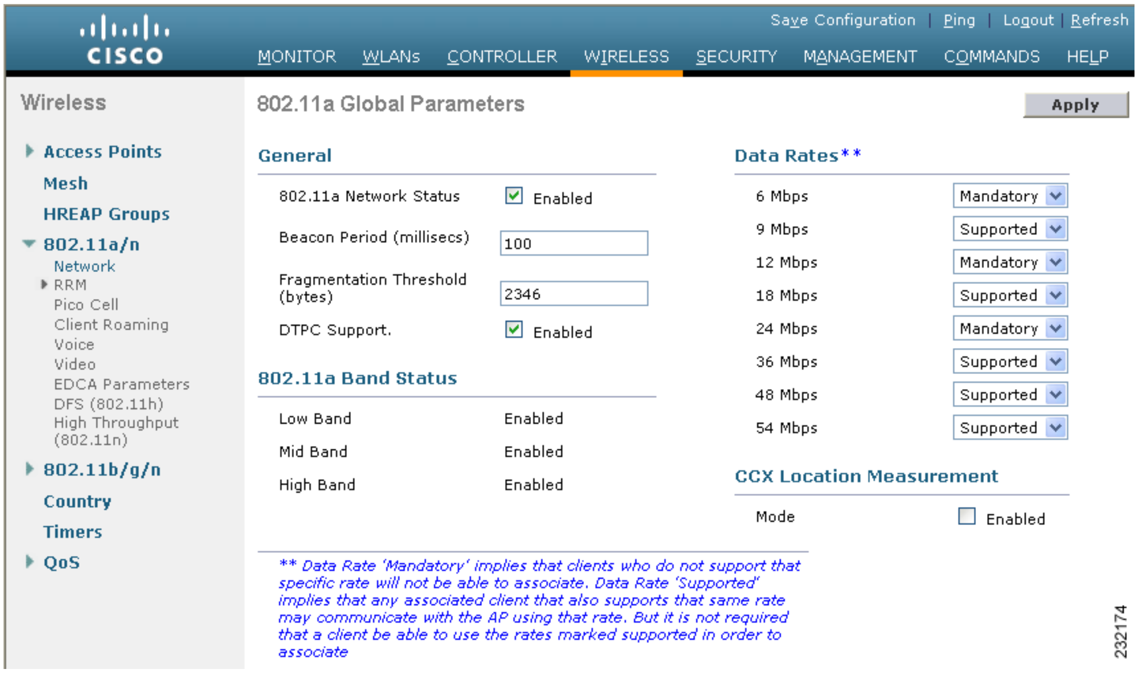
For CCX clients that need to be tracked more closely (for example, when a client calibration is performed), the controller can be configured to command the access point to send unicast measurement requests to these clients at a configured interval and whenever a CCX client roams to a new access point. 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.

Using the GUI to Configure CCX Radio Management

Follow these steps to configure CCX radio management using the controller GUI.

Step 1 Click **Wireless** > **802.11a/n** or **802.11b/g/n** > **Network**. The 802.11a (or 802.11b/g) Global Parameters page appears (see Figure 11-13).

Figure 11-13 802.11a Global Parameters Page



802.11a Global Parameters

General

802.11a Network Status	☑ Enabled
Beacon Period (millisecs)	100
Fragmentation Threshold (bytes)	2346
DTPC Support.	☑ Enabled

802.11a Band Status

Low Band	Enabled
Mid Band	Enabled
High Band	Enabled

Data Rates**

6 Mbps	Mandatory
9 Mbps	Supported
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Mandatory
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

CCX Location Measurement

Mode	□ Enabled

*** Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate*

Step 2 Under CCX Location Measurement, check 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 higher. The default value is disabled (or unchecked).

Step 3 If you checked the Mode check box in the previous step, enter a value in the Interval field to specify how often the access points are to issue the broadcast radio measurement requests.

Range: 60 to 32400 seconds

Default: 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 "Using the CLI to Configure CCX Radio Management" 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 or 802.11b/g).

Using the CLI to Configure CCX Radio Management

Follow these steps to enable CCX radio management using the controller CLI.

Step 1 To globally enable CCX radio management, enter 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 or 802.11b/g network to issue broadcast radio measurement requests to clients running CCXv2 or higher.

Step 2 To enable access point customization, enter 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 or 802.11b/g 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 or 802.11b/g network to issue broadcast radio measurement requests to clients running CCXv2 or higher.

Step 3 To enable or disable location calibration for a particular client, enter 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 To save your settings, enter this command:

save config

Using the CLI to Obtain CCX Radio Management Information

Use these commands to obtain information about CCX radio management on the controller.

1. To see the CCX broadcast location measurement request configuration for all access points connected to this controller in the 802.11a or 802.11b/g network, enter this command:

   show advanced {**802.11a** | **802.11b**} **ccx global**

2. To see the CCX broadcast location measurement request configuration for a particular access point in the 802.11a or 802.11b/g network, enter this command:

   show advanced {**802.11a** | **802.11b**} **ccx ap** *Cisco_AP*

3. 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
  Path Loss Request.............................. Disabled
  Interval....................................... 60
  Iteration................................... 5
```

4. To see the status of radio measurement requests for a particular client, enter this command:

   show client ccx rm *client_mac* **status**

   Information similar to the following appears:

```
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
```

5. 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.

6. To see the clients configured for location calibration, enter this command:

   show client location-calibration summary

7. To see the RSSI reported for both antennas on each access point that heard the client, enter this command:

   show client detail *client_mac*

Using the CLI to Debug CCX Radio Management Issues

Use these commands if you experience any CCX radio management problems.

1. To debug CCX broadcast measurement request activity, enter this command:

   debug airewave-director message {**enable** | **disable**}

2. To debug client location calibration activity, enter this command:

   debug ccxrm [**all** | **error** | **warning** | **message** | **packet** | **detail** {**enable** | **disable**}]

3. 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:

   debug iapp error {enable | disable}

4. To debug the output for forwarded probes and their included RSSI for both antennas, enter this command:

   debug dot11 load-balancing

Configuring Pico Cell Mode

In large multi-cell high-density wireless networks, it can be challenging to populate a site with a large number of access points to handle the desired cumulative bandwidth load while diminishing the contention between access points and maintaining quality of service. To optimize RF channel capacity and improve overall network performance, you can use the controller GUI or CLI to set high-density (or pico cell) mode parameters.

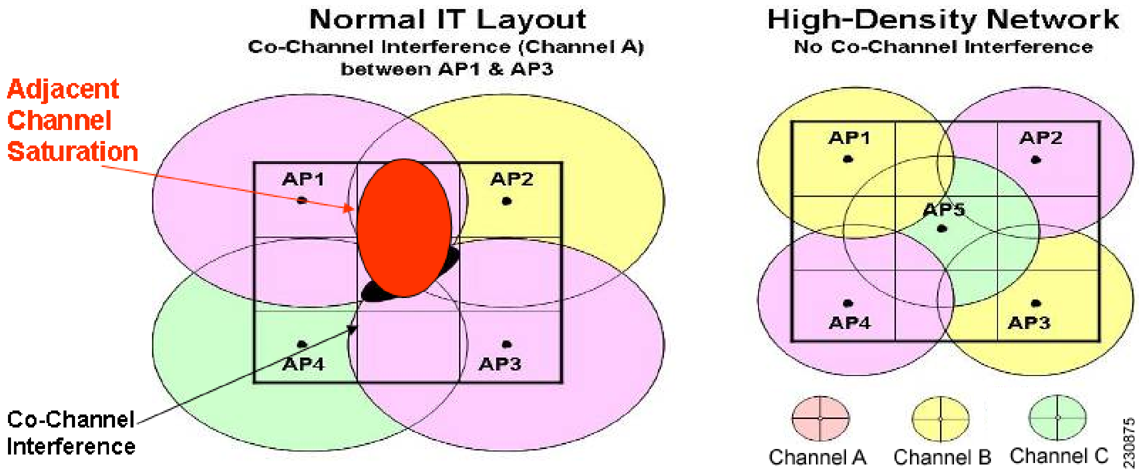
These parameters enable you to apply the same receiver sensitivity threshold, clear channel assessment (CCA) sensitivity threshold, and transmit power values across all access points registered to a given controller. When a client that supports high density associates to an access point with high density enabled, they exchange specific 802.11 information elements (IEs) that instruct the client to adhere to the access point's advertised receive sensitivity threshold, CCA sensitivity threshold, and transmit power values. These three parameters reduce the effective cell size by adjusting the received signal strength before an access point and client consider the channel accessible for the transfer of packets. When all access points and clients raise the signal standard in this way throughout a high-density area, access points can be deployed closer together without interfering with each other or being overwhelmed by environmental and distant-rogue signals.

The benefits of a high-density-enabled wireless network include the following:

- Most efficient use of the available spectrum
- Significant increase in aggregate client throughput or throughput per square feet
- Significant increase in wireless LAN capacity
- Linear capacity growth
- Higher interference tolerance by allowing WiFi to transmit over top of the interference

Figure 11-14 shows an example of a high-density network.

Figure 11-14   High-Density Network Example



Guidelines for Using Pico Cell Mode

Follow these guidelines for using pico cell mode:

- High-density networking is supported on Cisco lightweight access points and on notebooks using the Intel PRO/Wireless 3945ABG and Intel Wireless WiFi Link 4965AG clients.
- In order to use pico cell mode version 2, the WMM policy for the Intel clients must be set to Allowed.
- To support high-density, both the client s and access points must be configured for high density. Do not mix high-density and non-high-density devices in the same network.
- High-density access points must be joined to a dedicated controller.
- When you adjust the pico cell mode parameters, the following RRM values automatically change:
  - The default value of the Fixed option for the Power Level Assignment Method parameter [on the 802.11a (or 802.11b) > RRM > Tx Power Control (TPC) page] reflects the power setting that you specify for the pico cell Transmit Power parameter.
  - The default value of the Power Threshold parameter [on the 802.11a (or 802.11b) > RRM > Tx Power Control (TPC) page] reflects the value that you specify for the pico cell CCA Sensitivity Threshold parameter.

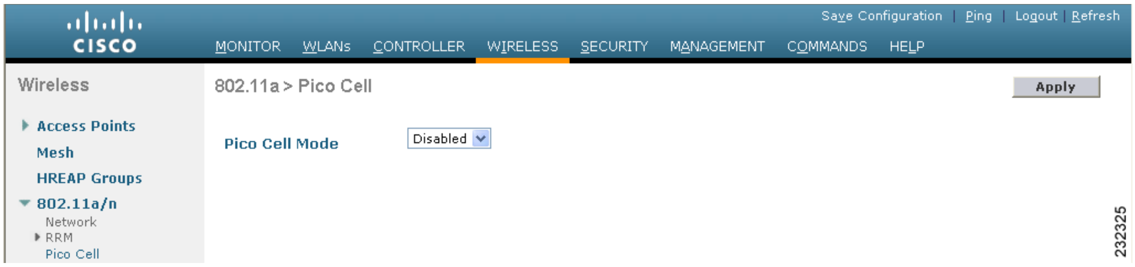
Using the GUI to Configure Pico Cell Mode

Follow these steps to configure pico cell mode using the controller GUI.

Step 1 Disable the 802.11a or 802.11b/g network before changing pico cell mode parameters. To do so, click **Wireless** > **802.11a/n** (or **802.11b/g/n**) > **Network** and uncheck the **802.11a Network Status** (or **802.11b/g Network Status**) check box.

Step 2 Click **Wireless** > **802.11a/n** (or **802.11b/g/n**) > **Pico Cell** to open the 802.11a (or 802.11b/g) > Pico Cell page (see Figure 11-15).

Figure 11-15 802.11a > Pico Cell Page



802.11a > Pico Cell

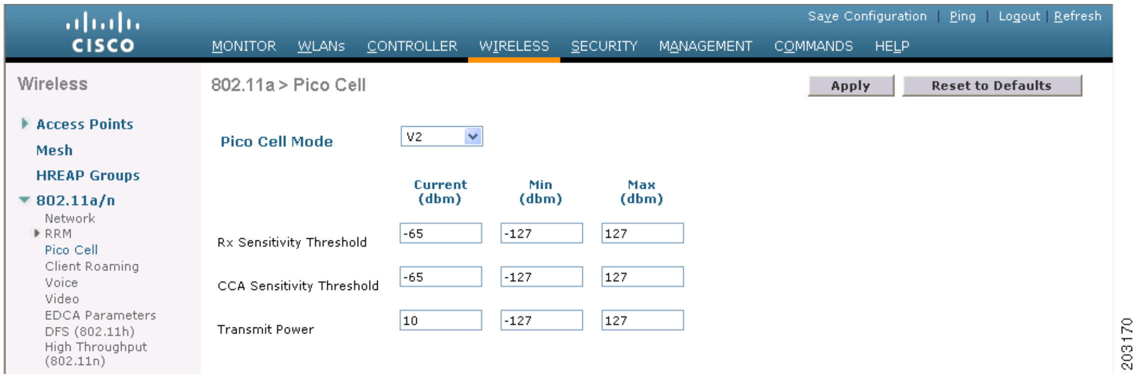
Pico Cell Mode: Disabled

Step 3 Choose one of these options from the Pico Cell Mode drop-down box:

- **Disable**—Disables pico cell mode. This is the default value.
- **V1**—Enables pico cell mode version 1. This option is designed for use with legacy Airespace products (those released prior to Cisco's acquisition of Airespace). Cisco recommends that you choose V2 if you want to enable pico cell mode.
- **V2**—Enables pico cell mode version 2. Choose this option if you want to adjust the pico cell mode parameters to optimize network performance in high-density areas, where all the clients support high density.

Step 4 If you chose V2 in Step 3, the 802.11a (or 802.11b/g) > Pico Cell page displays three configurable fields: Rx Sensitivity Threshold, CCA Sensitivity Threshold, and Transmit Power (see Figure 11-16).

Figure 11-16 802.11a > Pico Cell Page with Pico Cell Mode V2 Parameters



802.11a > Pico Cell

Pico Cell Mode: V2

	Current (dbm)	Min (dbm)	Max (dbm)
Rx Sensitivity Threshold	-65	-127	127
CCA Sensitivity Threshold	-65	-127	127
Transmit Power	10	-127	127

Use the information in Table 11-3 to adjust the values of these parameters as necessary.

Note The default values for these parameters should be appropriate for most applications. Therefore, Cisco recommends that you use the default values.

Table 11-3 Pico Cell Mode V2 Parameters

Parameter	Description
Rx Sensitivity Threshold	Specifies the current, minimum, and maximum values (in dBm) for the receiver sensitivity of the 802.11a or 802.11b/g radio. The current value sets the receiver sensitivity on the local radio. The min and max values are used only for inclusion in the Inter-Access Point Protocol (IAPP) high-density reports. **Default:** –65 dBm (Current), –127 dBm (Min), and 127 dBm (Max)
CCA Sensitivity Threshold	Specifies the clear channel assessment (CCA) sensitivity threshold on all radios in the high-density cell. The current value programs the 802.11a or 802.11b/g receiver. The min and max values are for advertisement in IAPP reports. **Default:** –65 dBm (Current), –127 dBm (Min), and 127 dBm (Max)
Transmit Power	Specifies the high-density transmit power used by both the access point and client 802.11a or 802.11b/g radios. **Default:** 10 dBm (Current), –127 dBm (Min), and 127 dBm (Max)

Note The min and max values in Figure 11-16 and Table 11-3 are used only to indicate the range to the client. They are not used on the access point.

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

Step 6 Re-enable the 802.11a or 802.11b/g network. To do so, click **Wireless** > **802.11a/n** (or **802.11b/g/n**) > **Network** and check the **802.11a Network Status** (or **802.11b/g Network Status**) check box.

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

Note If you change the values of the pico cell mode parameters and later want to reset them to their default values, click **Reset to Defaults** and then click **Apply**.

Using the CLI to Configure Pico Cell Mode

Note Refer to the "Using the GUI to Configure Pico Cell Mode" section on page 11-42 for descriptions and default values of the parameters used in the CLI commands.

Step 1 To disable the 802.11a or 802.11b/g network before changing pico cell mode parameters, enter this command:

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

Step 2 To enable pico cell mode, enter one of these commands:

- **config** {**802.11a** | **802.11b**} **picocell enable**—Enables pico cell mode version 1. This command is designed for use with a specific application. Cisco recommends that you use the **config** {**802.11a** | **802.11b**} **picocell-V2 enable** command if you want to enable pico cell mode.
- **config** {**802.11a** | **802.11b**} **picocell-V2 enable**—Enables pico cell mode version 2. Use this command if you want to adjust the pico cell mode parameters to optimize network performance in high-density areas.

Step 3 If you enabled pico cell mode version 2 in Step 2, follow these steps to configure the receive sensitivity threshold, CCA sensitivity threshold, and transmit power parameters:

a. To configure the receive sensitivity threshold, enter this command:

config advanced {**802.11a** | **802.11b**} **receiver pico-cell-V2 rx_sense_threshold** *min max current*

b. To configure the CCA sensitivity threshold, enter this command:

config advanced {**802.11a** | **802.11b**} **receiver pico-cell-V2 cca_sense_threshold** *min max current*

c. To configure the transmit power, enter this command:

config advanced {**802.11a** | **802.11b**} **receiver pico-cell-V2 sta_tx_pwr** *min max current*

Step 4 If you enabled pico cell mode version 2 in Step 2 and you want to transmit a unicast IAPP high-density frame request to a specific client, enter this command:

config advanced {**802.11a** | **802.11b**} **receiver pico-cell-V2 send_iapp_req** *client_mac*

Step 5 To re-enable the 802.11a or 802.11b/g network, enter this command:

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

Step 6 To save your settings, enter this command:

save config

Using the CLI to Debug Pico Cell Mode Issues

Use these commands if you experience any pico cell mode problems.

1. To see the current status of pico cell mode, enter this command:

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

   Information similar to the following appears:

```
802.11a Network.................................. Disabled
11nSupport....................................... Disabled
      802.11a Low Band........................... Enabled
      802.11a Mid Band........................... Enabled
      802.11a High Band.......................... Enabled
...
Pico-Cell Status................................. Disabled
Pico-Cell-V2 Status........................... Enabled
```

2. To see the receiver parameters that are set by the pico cell mode commands, enter this command:

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

   Information similar to the following appears:

```
802.11a Advanced Receiver Settings
 RxStart  : Signal Threshold..................... 30
 RxStart  : Signal Jump Threshold................ 5
 RxStart  : Preamble Power Threshold............. 30
 RxRestart: Signal Jump Status................... Enabled
 RxRestart: Signal Jump Threshold................ 10
 TxStomp  : Low RSSI Status...................... Disabled
 TxStomp  : Low RSSI Threshold................... 30
 TxStomp  : Wrong BSSID Status................... Disabled
 TxStomp  : 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................... 30
 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.... -127,127,-65
 CCA Threshold: Min,Max,Current Clear Channel.... -127,127,-65
Tx Pwr: Min,Max,Current Transmit Power for A..... -127,127,10
 --------------------------------------------....
```

3. To see the noise and interference information, coverage information, client signal strengths and signal-to-noise ratios, and nearby access points, enter this command:

   show ap auto-rf {**802.11a** | **802.11b**} *Cisco_AP*

   Information similar to the following appears:

```
Number Of Slots.................................. 2
AP Name.......................................... AP1242.47b2.31f6
MAC Address...................................... 00:16:47:b2:31:f6
  Radio Type..................................... RADIO_TYPE_80211a
  Noise Information
    Noise Profile................................ PASSED
  Interference Information
    Interference Profile......................... PASSED
  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
    RSSI  -76 dbm................................ 0 clients
    RSSI  -68 dbm................................ 0 clients
    RSSI  -60 dbm................................ 0 clients
    RSSI  -52 dbm................................ 0 clients
```

```
Client Signal To Noise Ratios
  SNR    0 dB................................. 0 clients
  SNR    5 dB................................. 0 clients
  SNR   10 dB................................. 0 clients
  SNR   15 dB................................. 0 clients
  SNR   20 dB................................. 0 clients
  SNR   25 dB................................. 0 clients
  SNR   30 dB................................. 0 clients
  SNR   35 dB................................. 0 clients
  SNR   40 dB................................. 0 clients
  SNR   45 dB................................. 0 clients
Nearby APs
Radar Information
RF Parameter Recommendations
  Power Level................................. 0
  RTS/CTS Threshold........................... 0
  Fragmentation Threshold..................... 0
  Antenna Pattern............................. 0
```

CHAPTER 12

Configuring Mobility GroupsWireless Device Access

This chapter describes mobility groups and explains how to configure them on the controllers. It contains these sections:

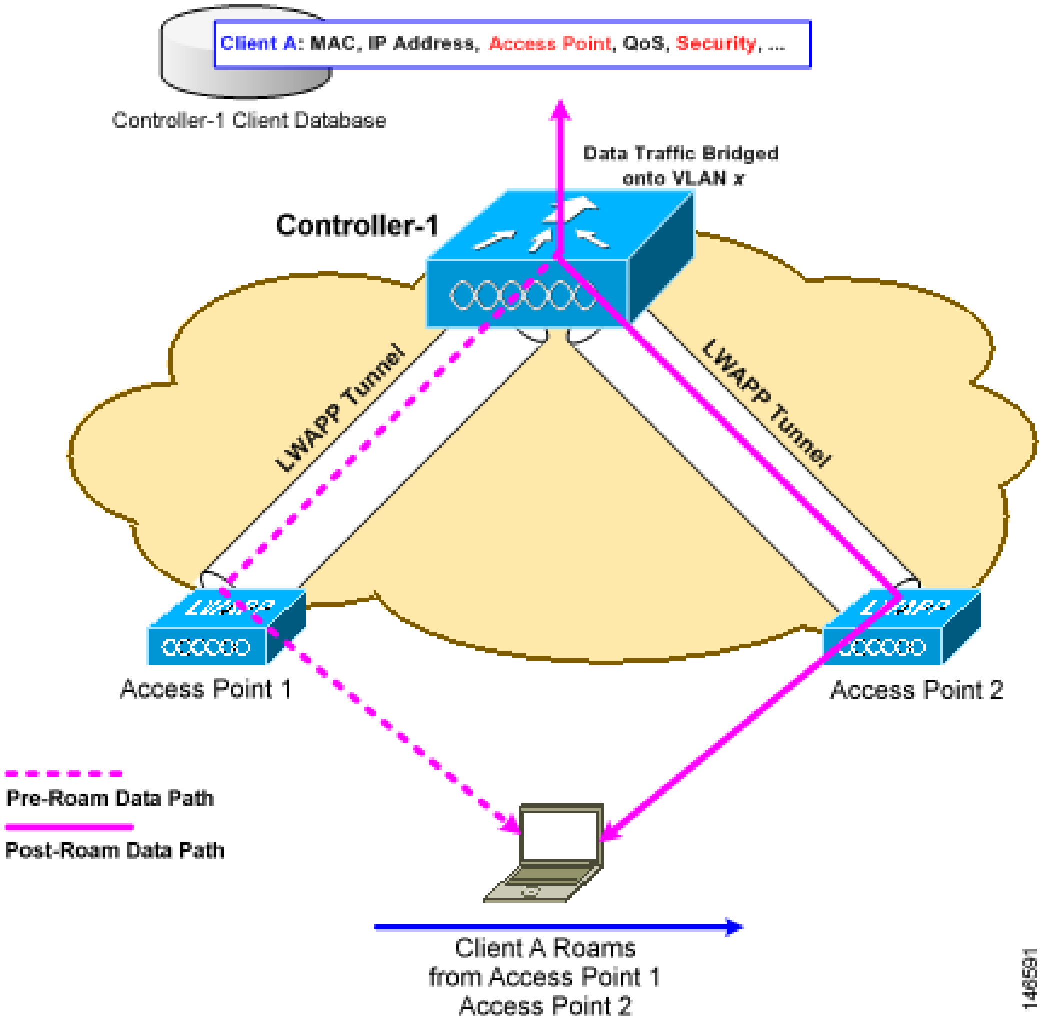
- Overview of Mobility, page 12-2
- Overview of Mobility Groups, page 12-5
- Configuring Mobility Groups, page 12-9
- Viewing Mobility Group Statistics, page 12-16
- Configuring Auto-Anchor Mobility, page 12-20
- WLAN Mobility Security Values, page 12-25
- Using Symmetric Mobility Tunneling, page 12-26
- Running Mobility Ping Tests, page 12-28

Overview of 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 12-1 illustrates a wireless client roaming from one access point to another when both access points are joined to the same controller.

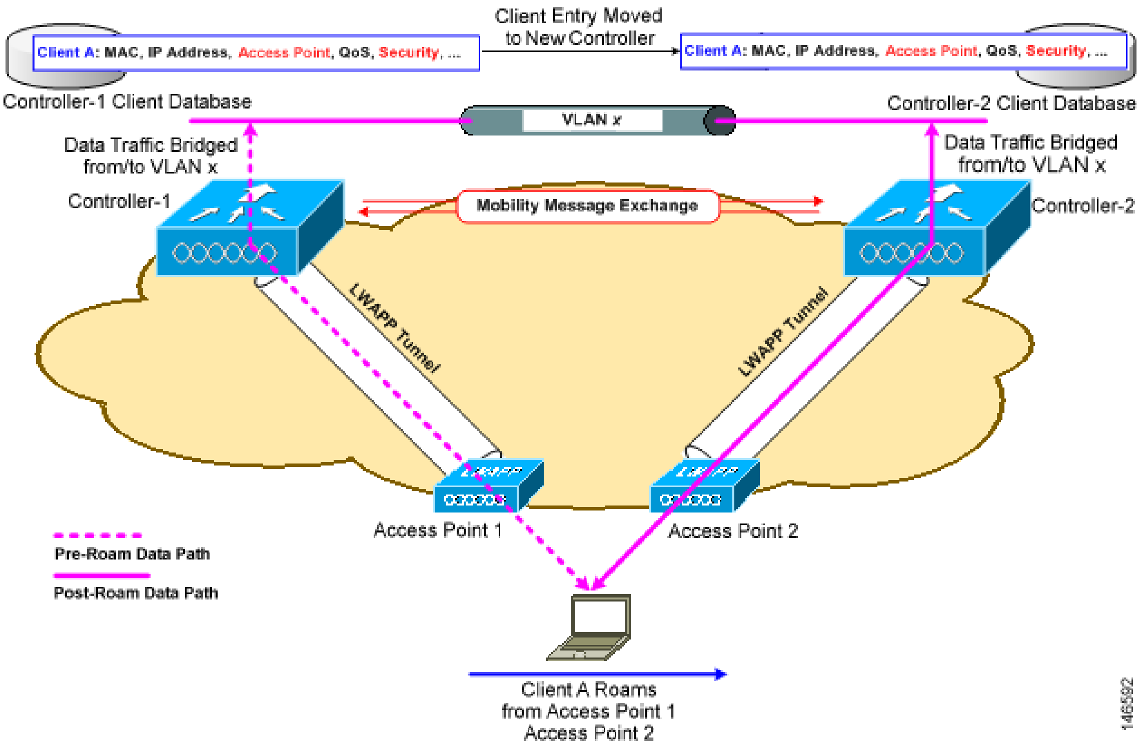
Figure 12-1 Intra-Controller Roaming


Client A: MAC, IP Address, Access Point, QoS, Security, ...
Controller-1 Client Database
Data Traffic Bridged onto VLAN x
Controller-1
LWAPP Tunnel
LWAPP Tunnel
LWAPP
LWAPP
Access Point 1
Access Point 2
Pre-Roam Data Path
Post-Roam Data Path
Client A Roams from Access Point 1 Access Point 2
146591

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 12-2 illustrates inter-controller roaming, which occurs when the controllers' wireless LAN interfaces are on the same IP subnet.

Figure 12-2 Inter-Controller Roaming

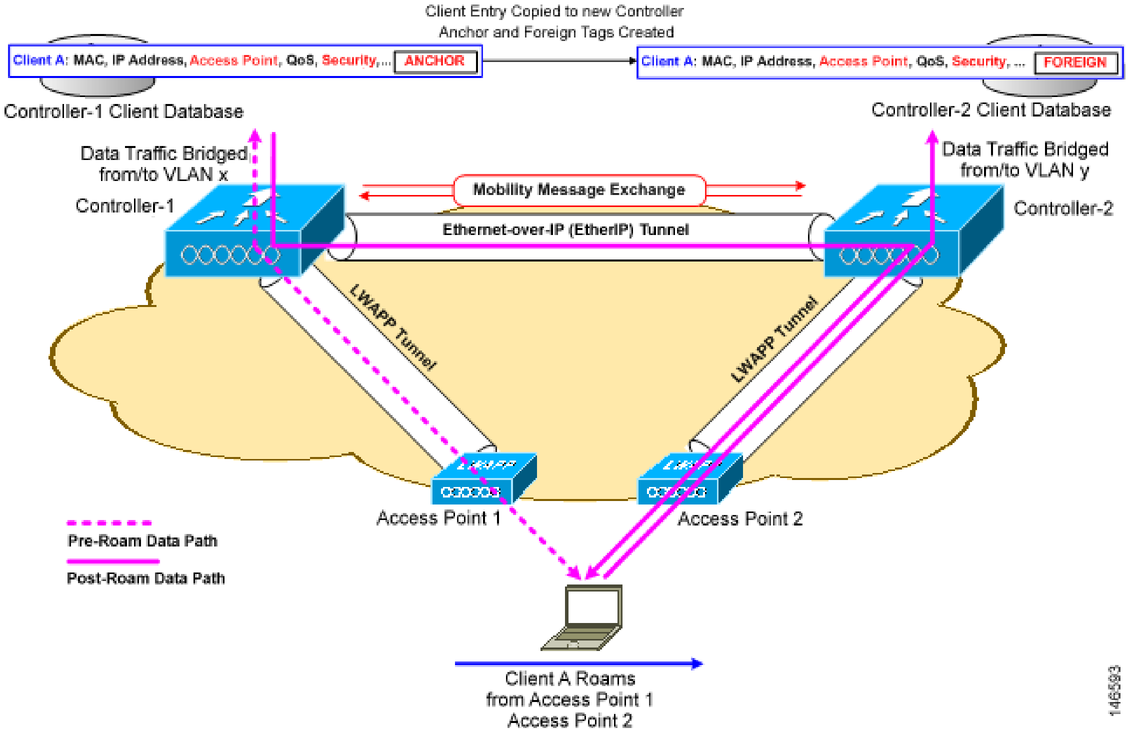


When the client associates to an access point joined to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database 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 12-3 illustrates inter-subnet roaming, which occurs when the controllers' wireless LAN interfaces are on different IP subnets.

Figure 12-3   Inter-Subnet Roaming


Client Entry Copied to new Controller
Anchor and Foreign Tags Created
Client A: MAC, IP Address, Access Point, QoS, Security,... ANCHOR
Client A: MAC, IP Address, Access Point, QoS, Security, ... FOREIGN
Controller-1 Client Database
Controller-2 Client Database
Data Traffic Bridged from/to VLAN x
Data Traffic Bridged from/to VLAN y
Controller-1
Controller-2
Mobility Message Exchange
Ethernet-over-IP (EtherIP) Tunnel
LWAPP Tunnel
LWAPP Tunnel
Access Point 1
Access Point 2
Pre-Roam Data Path
Post-Roam Data Path
Client A Roams from Access Point 1 Access Point 2
146593

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.

After an inter-subnet roam, data to and from the wireless client flows in an asymmetric traffic path. Traffic from the client to the network is forwarded directly into the network by the foreign controller. Traffic to the client arrives at the anchor controller, which forwards the traffic to the foreign controller in an EtherIP tunnel. The foreign controller then forwards the data to the client. If a wireless client roams to a new foreign controller, the client database entry is moved from the original foreign controller to the new foreign controller, but the original anchor controller is always maintained. If the client moves back to the original controller, it becomes local again.

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.

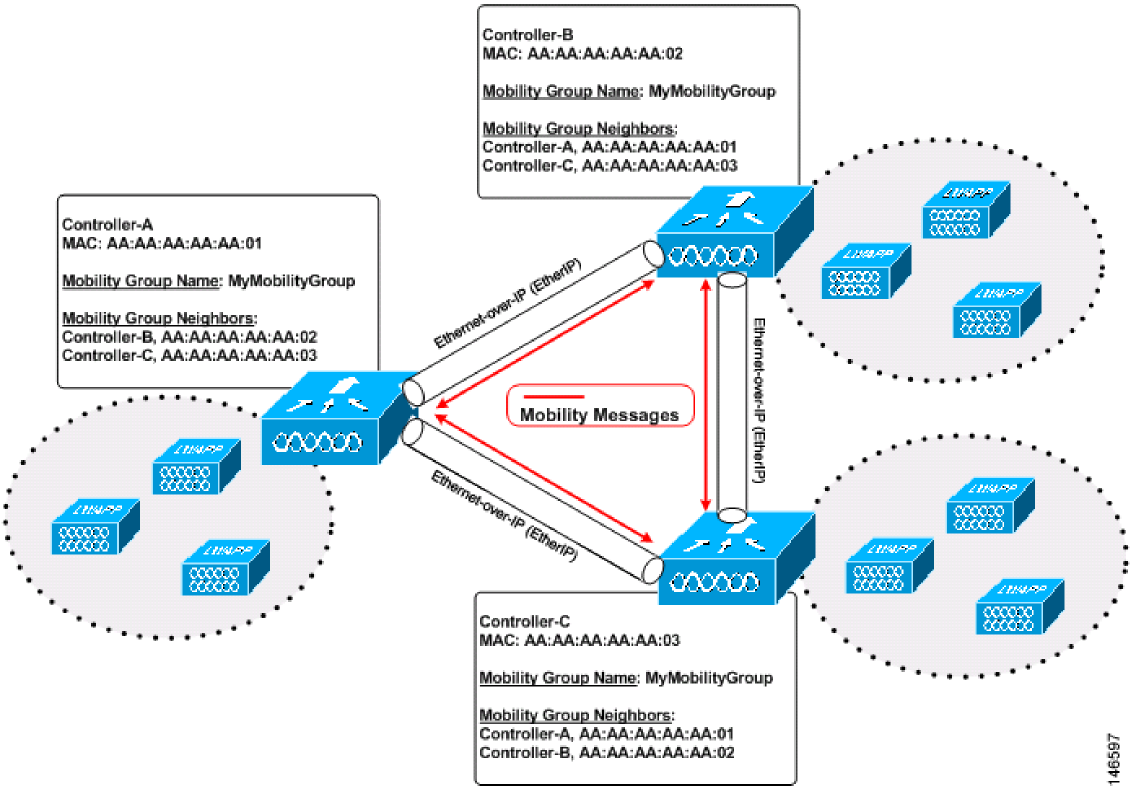
Note Currently, multicast traffic cannot be passed during inter-subnet roaming. With this in mind, you would not want to design an inter-subnet network for SpectraLink phones that need to send multicast traffic while using push to talk.

Overview of 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 12-4 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 12-4 A Single Mobility Group


Controller-B
MAC: AA:AA:AA:AA:AA:02
Mobility Group Name: MyMobilityGroup
Mobility Group Neighbors:
Controller-A, AA:AA:AA:AA:AA:01
Controller-C, AA:AA:AA:AA:AA:03
Controller-A
MAC: AA:AA:AA:AA:AA:01
Mobility Group Name: MyMobilityGroup
Mobility Group Neighbors:
Controller-B, AA:AA:AA:AA:AA:02
Controller-C, AA:AA:AA:AA:AA:03
Ethernet-over-IP (EtherIP)
Mobility Messages
Ethernet-over-IP (EtherIP)
Ethernet-over-IP (EtherIP)
LWAPP
Controller-C
MAC: AA:AA:AA:AA:AA:03
Mobility Group Name: MyMobilityGroup
Mobility Group Neighbors:
Controller-A, AA:AA:AA:AA:AA:01
Controller-B, AA:AA:AA:AA:AA:02
146597

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 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. All mobility message exchanges between controllers are carried out using UDP packets on port 16666.

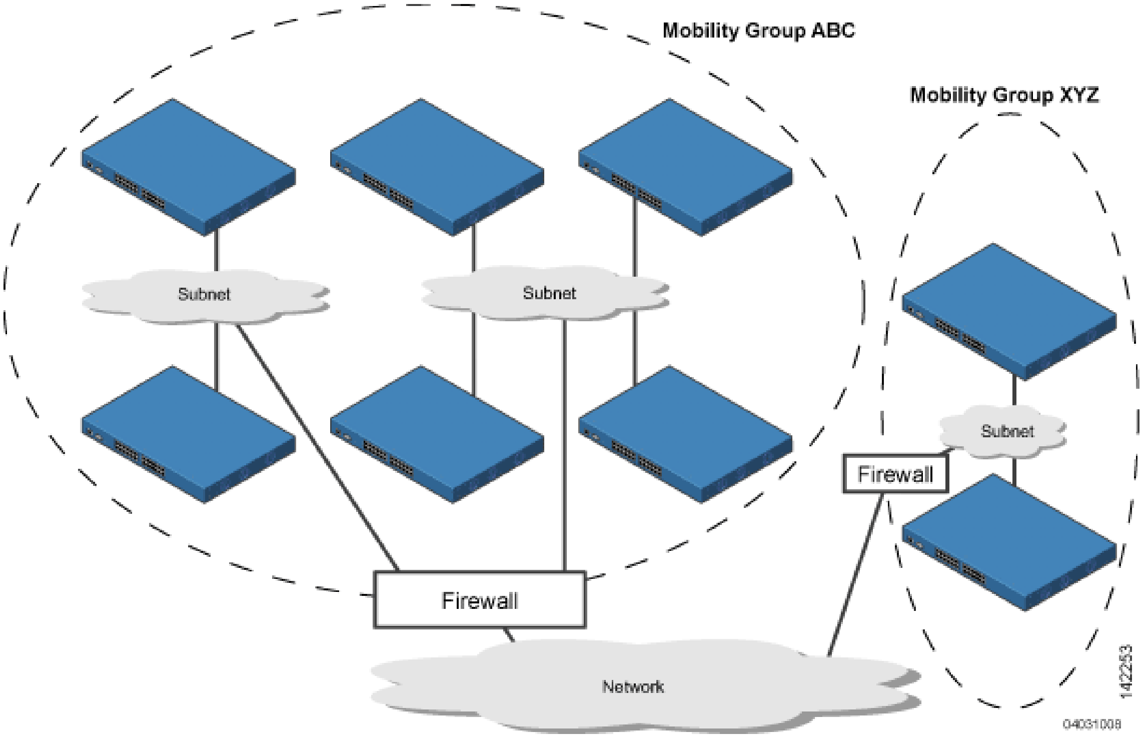
Controller software release 5.1 or later supports up to 24 controllers in a single mobility group. The number of access points supported in a mobility group is bound by the number of controllers and controller types in the group.

Examples:

1. A 4404-100 controller supports up to 100 access points. Therefore, a mobility group consisting 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 consisting 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 12-5 shows the results of creating distinct mobility group names for two groups of controllers.

Figure 12-5 Two Mobility Groups



The controllers in the ABC mobility group recognize and communicate with each other through their access points and through their shared subnets. The controllers in the ABC mobility group do not recognize or communicate with the XYZ controllers, which are in a different mobility group. Likewise, the controllers in the XYZ mobility group do not recognize or communicate with the controllers in the ABC mobility group. This feature ensures mobility group isolation across the network.

Controllers can communicate across mobility groups and clients may roam between access points in different mobility groups, provided that the controllers are included in each other's mobility lists. A mobility list is a list of controllers configured on a controller that specifies members in different mobility groups. 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:

```
Controller 1                  Controller 2                  Controller 3
Mobility group: A             Mobility group: A             Mobility group: C
Mobility list:                Mobility list:                Mobility list:
    Controller 1 (group A)        Controller 1 (group A)        Controller 1 (group A)
    Controller 2 (group A)        Controller 2 (group A)        Controller 3 (group C)
    Controller 3 (group C)
```

Controller software release 5.1 or later supports up to 72 controllers in a controller's mobility list and 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 intra-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 EtherIP tunneling is initiated for Layer 3 roaming.

Note Controller software release 5.0 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, 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, 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 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, 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, 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 containing all the mobility members. To derive the maximum benefit from multicast messaging, Cisco recommends 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 poses a problem when a NAT device is introduced in the network because it changes the source IP address in the IP header. Hence, in the guest WLAN feature, any mobility packet being routed through a NAT device is dropped because of the IP address mismatch.

In controller software release 4.2 or later, 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 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 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

Note 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 12-6 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 12-7 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.

Figure 12-6 Mobility Group Configuration with One NAT Device

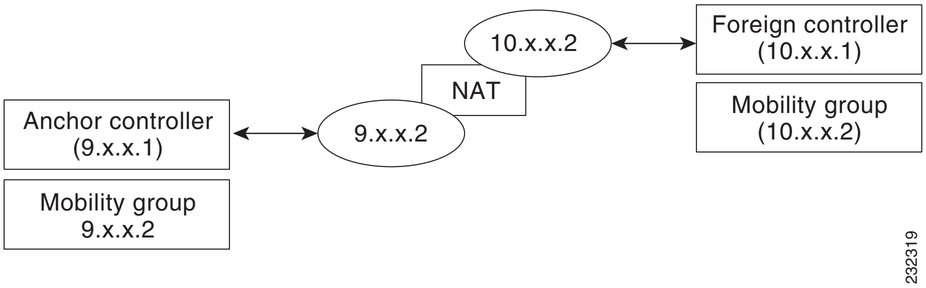
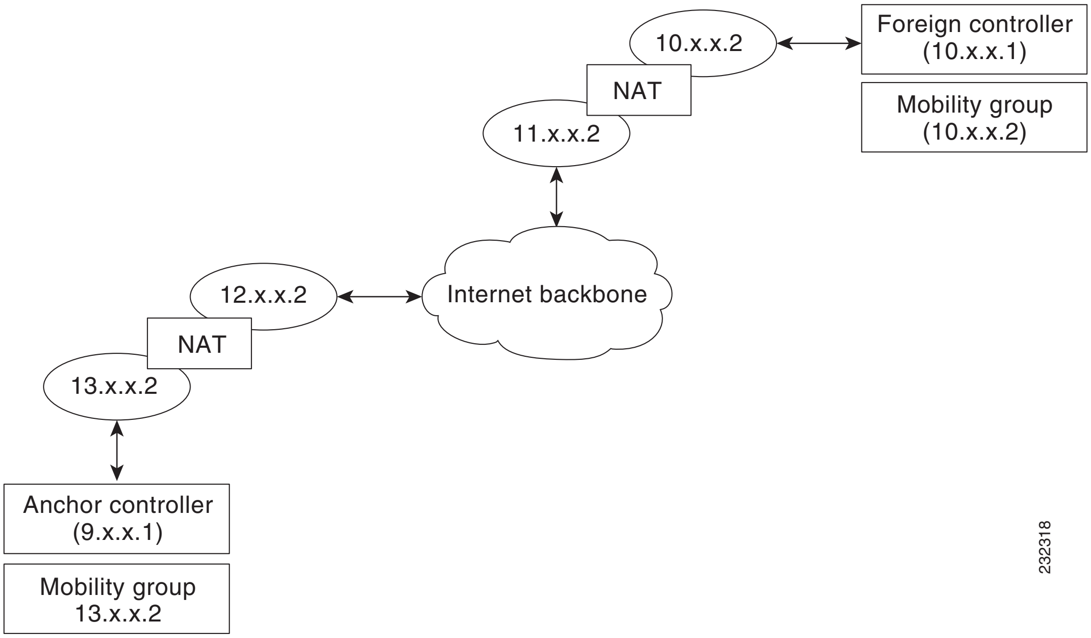


Figure 12-7 Mobility Group Configuration with Two NAT Devices



Configuring Mobility Groups

This section provides instructions for configuring controller mobility groups through either the GUI or the CLI.

Note You can also configure mobility groups using the Cisco Wireless Control System (WCS). Refer to the *Cisco Wireless Control System Configuration Guide* for instructions.

Prerequisites

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.

- All controllers must be configured with the same mobility group name.

  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 field 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.

- Controllers within the same mobility group that run different software releases (such as 4.2, 5.0, 5.1, and 5.2) can use guest tunneling, but they do not support normal client mobility.

  Note If you inadvertently configure a controller that is running software release 5.2 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.

- 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 3 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 hand-off 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, Cisco PIX, or Cisco ASA, you need to open ports 16666, 12222, and 12223; IP protocols 50 and 97; and UDP port 500.

  Note You cannot perform port address translation (PAT) on the firewall. You must configure one-to-one network address translation (NAT).

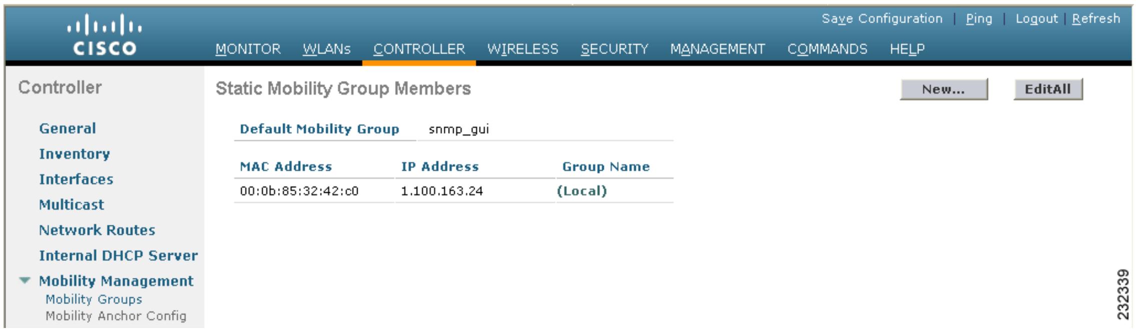
Using the GUI to Configure Mobility Groups

Follow these steps to configure mobility groups using the GUI.

Note See the "Using the CLI to Configure Mobility Groups" section on page 12-14 if you would prefer to configure mobility groups using the CLI.

Step 1 Click **Controller** > **Mobility Management** > **Mobility Groups** to open the Static Mobility Group Members page (see Figure 12-8).

Figure 12-8 Static Mobility Group Members Page



Static Mobility Group Members

Default Mobility Group snmp_gui

MAC Address	IP Address	Group Name
00:0b:85:32:42:c0	1.100.163.24	(Local)

This page shows the mobility group name in the Default Mobility Group field 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**.

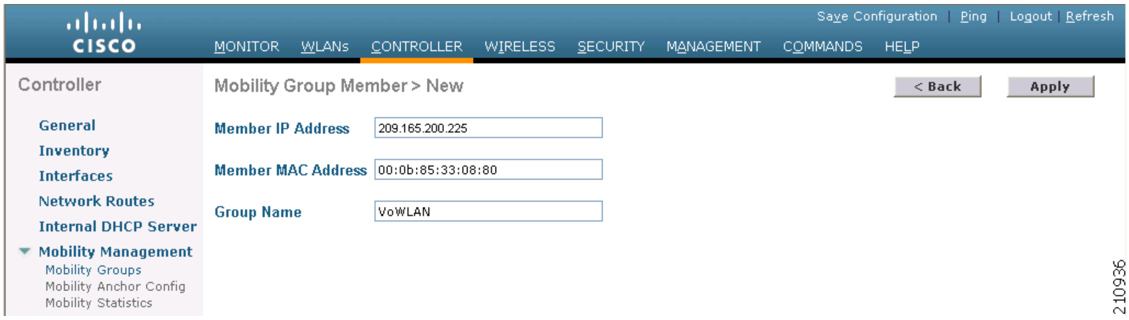
Step 2 Perform one of the following to add controllers to a mobility group:

- If you are adding only one controller or want to individually add multiple controllers, click **New** and go to Step 3.
- If you are adding multiple controllers and want to add them in bulk, click **EditAll** and go to Step 4.

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 The Mobility Group Member > New page appears (see Figure 12-9).

Figure 12-9 Mobility Group Member > New Page



Mobility Group Member > New

Member IP Address: 209.165.200.225

Member MAC Address: 00:0b:85:33:08:80

Group Name: VoWLAN

Follow these steps to add a controller to the mobility group:

a. In the Member IP Address field, 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 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 field, enter the MAC address of the controller to be added.

c. In the Group Name field, 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.

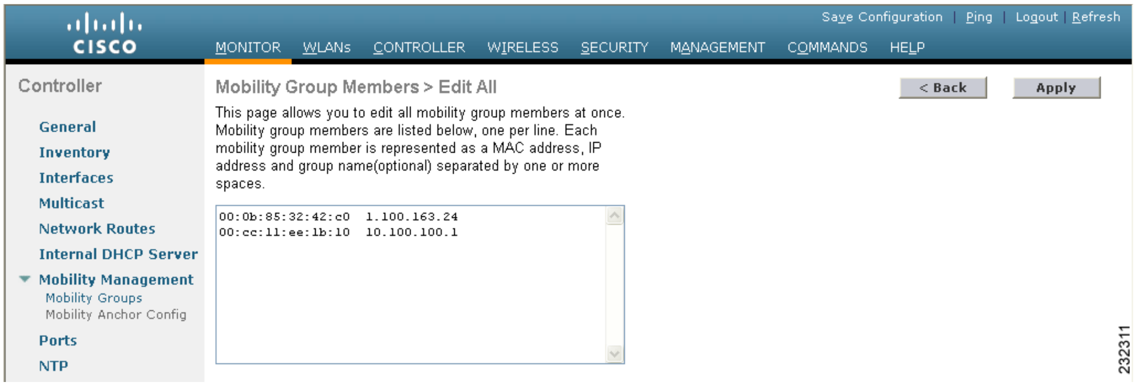
f. Repeat Step a through Step e to add all of the controllers in the mobility group.

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.

Step 4 The Mobility Group Members > Edit All page (see Figure 12-10) 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 12-10 Mobility Group Members > Edit All Page



Mobility Group Members > Edit All

This page allows you to edit all mobility group members at once. Mobility group members are listed below, one per line. Each mobility group member is represented as a MAC address, IP address and group name(optional) separated by one or more spaces.

```
00:0b:85:32:42:c0  1.100.163.24
00:cc:11:ee:1b:10  10.100.100.1
```

Follow these steps to add more controllers to the mobility group:

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** These values should be entered on one line and separated by 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.

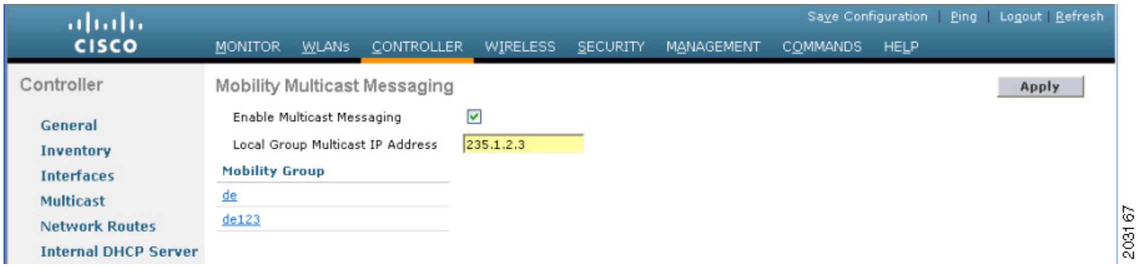
e. Click **Apply** to commit your changes. The new controllers are added to the list of mobility group members on the Static Mobility Group Members page.

f. Click **Save Configuration** to save your changes.

g. Paste the list into the edit 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 5 Click **Multicast Messaging** to open the Mobility Multicast Messaging page (see Figure 12-11).

Figure 12-11 Mobility Multicast Messaging Page



Mobility Multicast Messaging

Enable Multicast Messaging ☑

Local Group Multicast IP Address 235.1.2.3

Mobility Group
de
de123

The names of all the currently configured mobility groups appear in the middle of the page.

Step 6 On the Mobility Multicast Messaging page, check 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 unchecked, the controller uses unicast mode to send the Mobile Announce messages. The default value is unchecked.

Step 7 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 field. This address is used for multicast mobility messaging.

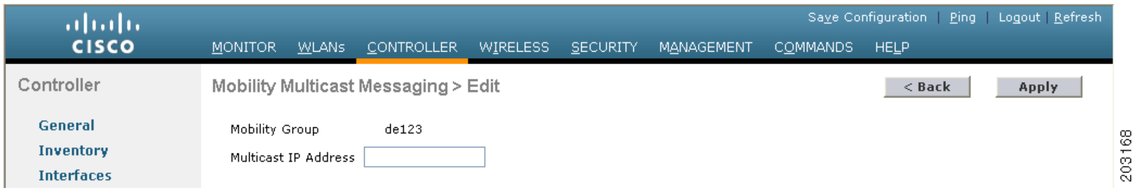
Note In order to use multicast messaging, you must configure the IP address for the local mobility group.

Step 8 Click **Apply** to commit your changes.

Step 9 If desired, you can also configure the multicast group IP address for non-local groups within the mobility list. To do so, click the name of a non-local mobility group to open the Mobility Multicast Messaging > Edit page (see Figure 12-12), and enter the multicast group IP address for the non-local mobility group in the Multicast IP Address field.

Note If you do not configure the multicast IP address for non-local groups, the controller uses unicast mode to send mobility messages to those members.

Figure 12-12 Mobility Multicast Messaging > Edit Page



Mobility Group de123

Multicast IP Address

Step 10 Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Using the CLI to Configure Mobility Groups

Follow these steps to configure mobility groups using the CLI.

Note The **config mobility secure-mode** {**enable** | **disable**} command is not supported in controller software release 5.2 even if it is present in the controller CLI.

Step 1 To check the current mobility settings, 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......................... 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
 MAC Address        IP Address       Group Name Multicast IP Status
 00:0b:85:32:42:c0 1.100.163.24     snmp_gui     0.0.0.0     Up
 00:cc:11:ee:1b:10 10.100.100.1    VoWLAN       0.0.0.0     Control and Data Path Down
 11:22:11:33:11:44 1.2.3.4         test         0.0.0.0     Control and Data Path Down
```

Step 2 To create a mobility group, enter 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 To add a group member, enter 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 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 **config mobility group member delete** *mac_address* if you want to delete a group member.

Step 4 To enable or disable multicast mobility mode, enter 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 If desired, you can also configure the multicast group IP address for non-local 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 non-local groups, the controller uses unicast mode to send mobility messages to those members.

Step 6 To verify the mobility configuration, enter this command:

show mobility summary

Step 7 To save your settings, enter 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 To enable or disable debugging of multicast usage for mobility messages, enter 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

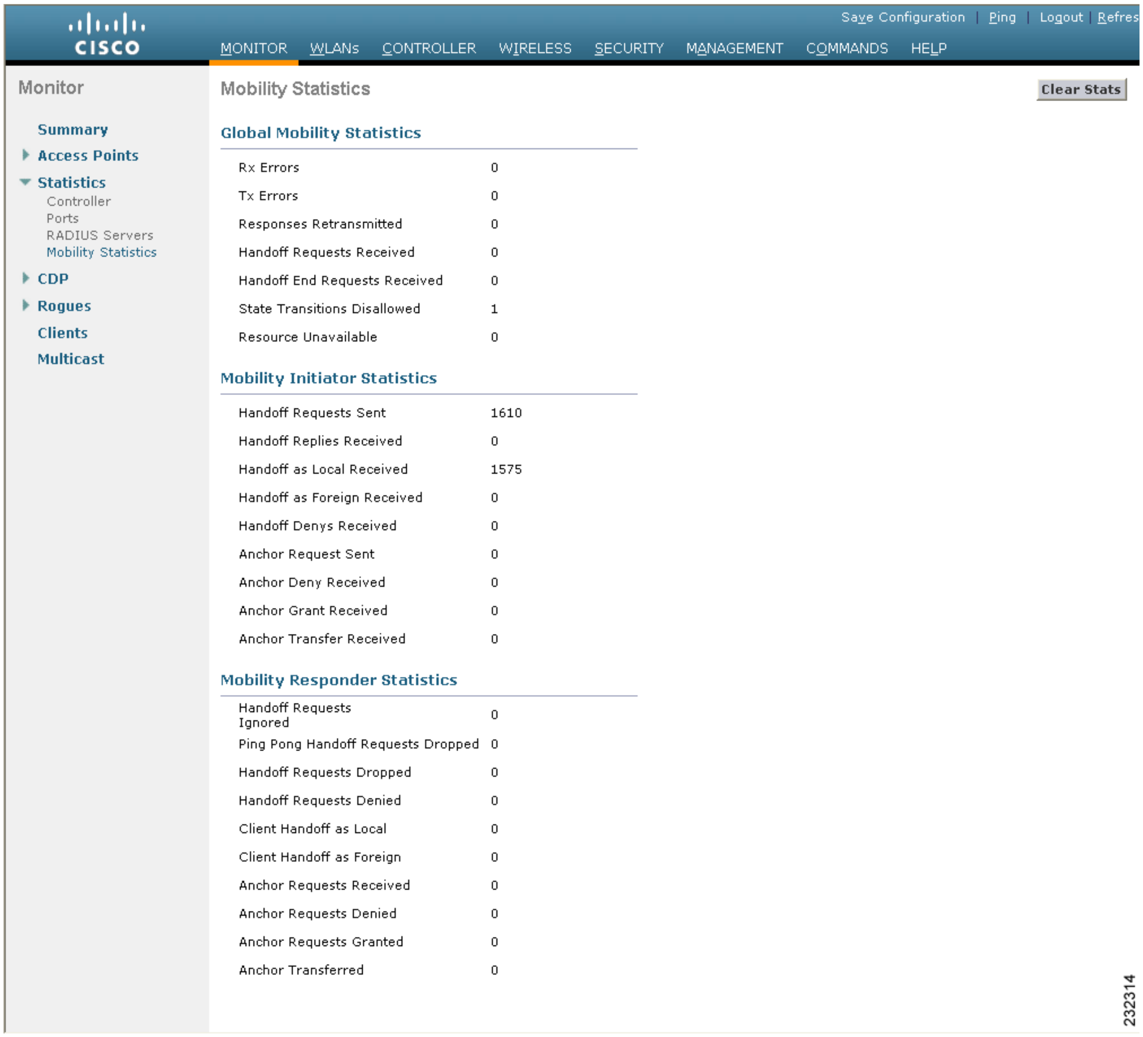
You can view mobility group statistics using the controller GUI or CLI.

Using the GUI to View Mobility Group Statistics

Using the controller GUI, follow these steps to view mobility group statistics.

Step 1 Click **Monitor** > **Statistics** > **Mobility Statistics** to open the Mobility Statistics page (see Figure 12-13).

Figure 12-13 Mobility Statistics Page



Mobility Statistics

Global Mobility Statistics

Rx Errors	0
Tx Errors	0
Responses Retransmitted	0
Handoff Requests Received	0
Handoff End Requests Received	0
State Transitions Disallowed	1
Resource Unavailable	0

Mobility Initiator Statistics

Handoff Requests Sent	1610
Handoff Replies Received	0
Handoff as Local Received	1575
Handoff as Foreign Received	0
Handoff Denys Received	0
Anchor Request Sent	0
Anchor Deny Received	0
Anchor Grant Received	0
Anchor Transfer Received	0

Mobility Responder Statistics

Handoff Requests Ignored	0
Ping Pong Handoff Requests Dropped	0
Handoff Requests Dropped	0
Handoff Requests Denied	0
Client Handoff as Local	0
Client Handoff as Foreign	0
Anchor Requests Received	0
Anchor Requests Denied	0
Anchor Requests Granted	0
Anchor Transferred	0

Step 2 Refer to Table 12-1 for a description of each statistic.

Table 12-1 Mobility Statistics

Parameter	Description
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	The mobility protocol uses UDP, and it 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 field shows a count of the response resends.

Table 12-1 Mobility Statistics (continued)

Parameter	Description
Handoff Requests Received	The total number of handoff requests received, ignored, or responded to.
Handoff End Requests Received	The 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.
State Transitions Disallowed	The policy enforcement module (PEM) has denied a client state transition, usually resulting in the handoff being aborted.
Resource Unavailable	A necessary resource, such as a buffer, was unavailable, resulting in the handoff being aborted.
Mobility Initiator Statistics	
Handoff Requests Sent	The number of clients that have associated to the controller and have been announced to the mobility group.
Handoff Replies Received	The number of handoff replies that have been received in response to the requests sent.
Handoff as Local Received	The number of handoffs in which the entire client session has been transferred.
Handoff as Foreign Received	The number of handoffs in which the client session was anchored elsewhere.
Handoff Denys Received	The number of handoffs that were denied.
Anchor Request Sent	The 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	The number of anchor requests that were denied by the current anchor.
Anchor Grant Received	The number of anchor requests that were approved by the current anchor.
Anchor Transfer Received	The number of anchor requests that closed the session on the current anchor and transferred the anchor back to the requestor.

Table 12-1 Mobility Statistics (continued)

Parameter	Description
Mobility Responder Statistics	
Handoff Requests Ignored	The number of handoff requests or client announcements that were ignored because the controller had no knowledge of that client.
Ping Pong Handoff Requests Dropped	The number of handoff requests that were denied because the handoff period was too short (3 seconds).
Handoff Requests Dropped	The 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	The number of handoff requests that were denied.
Client Handoff as Local	The number of handoff responses sent while the client is in the local role.
Client Handoff as Foreign	The number of handoff responses sent while the client is in the foreign role.
Anchor Requests Received	The number of anchor requests received.
Anchor Requests Denied	The number of anchor requests denied.
Anchor Requests Granted	The number of anchor requests granted.
Anchor Transferred	The 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 3 If you want to clear the current mobility statistics, click **Clear Stats**.

Using the CLI to View Mobility Group Statistics

Using the controller CLI, follow these steps to view mobility group statistics.

Step 1 To view mobility group statistics, enter this command:

show mobility statistics

Step 2 Refer to Table 12-1 for a description of each statistic.

Step 3 If you want to clear the current mobility statistics, enter this command:

clear stats mobility

Configuring 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, using 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, and the client is announced to the other controllers in the mobility list. 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.

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, 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 sent to each anchor controller. This functionality provides guest N+1 redundancy for guest tunneling and mobility failover for regular mobility.

Guest N+1 redundancy allows detection of failed anchors. Once a failed anchor controller is detected, all of the clients anchored to this controller are deauthenticated so that they can quickly become anchored to another controller. This same functionality is also extended to regular mobility clients through mobility failover. This feature enables mobility group members to detect failed members and reroute clients.

Note A 2100 series controller cannot be designated as an anchor for a WLAN. However, a WLAN created on a 2100 series controller can have a 4400 series controller as its anchor.

Note The IPSec and L2TP Layer 3 security policies are unavailable for WLANs configured with a mobility anchor.

Guidelines for Using Auto-Anchor Mobility

Keep these guidelines in mind when you configure auto-anchor mobility:

- Controllers must be added 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.
- The WLANs on both the foreign controller and the anchor controller must be configured 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

Using the GUI to Configure Auto-Anchor Mobility

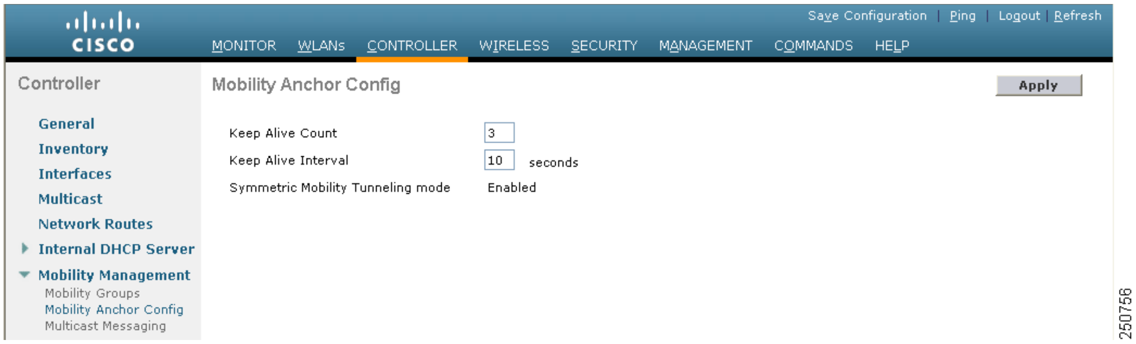
Follow these steps to create a new mobility anchor for a WLAN using the GUI.

Note See the "Using the CLI to Configure Auto-Anchor Mobility" section on page 12-23 if you would prefer to configure auto-anchor mobility using the CLI.

Step 1 Follow these steps to configure the controller to detect failed anchor controllers within a mobility group:

a. Click **Controller** > **Mobility Management** > **Mobility Anchor Config** to open the Mobility Anchor Config page (see Figure 12-14).

Figure 12-14   Mobility Anchor Config Page



Mobility Anchor Config

Keep Alive Count 3

Keep Alive Interval 10 seconds

Symmetric Mobility Tunneling mode Enabled

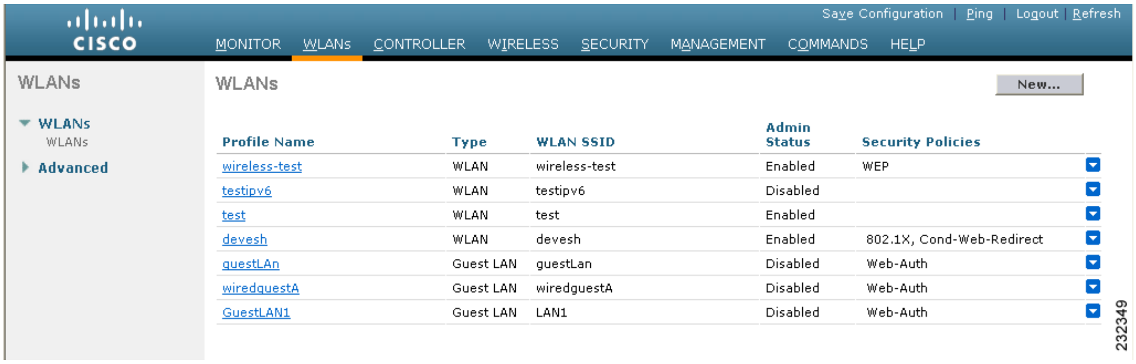
b. In the Keep Alive Count field, enter the number of times a ping request is sent to an anchor controller before the anchor is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.

c. In the Keep Alive Interval field, enter the amount of time (in seconds) between each ping request sent to an anchor controller. The valid range is 1 to 30 seconds, and the default value is 10 seconds.

d. Click **Apply** to commit your changes.

Step 2 Click **WLANs** to open the WLANs page (see Figure 12-15).

Figure 12-15   WLANs Page

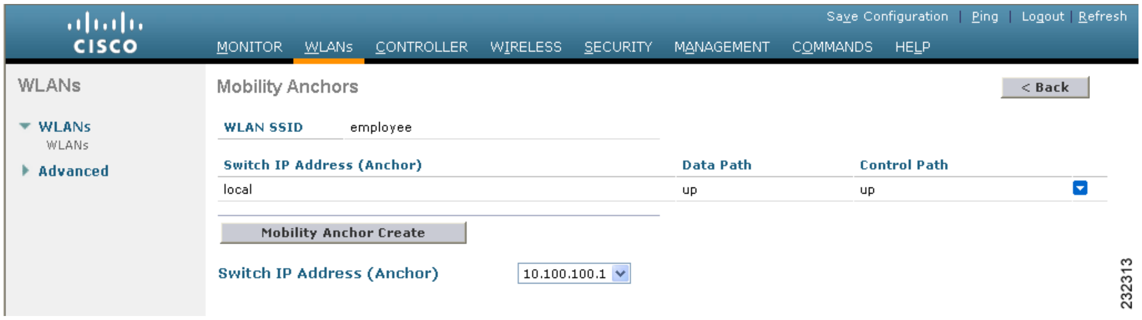

Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
New...
232349

WLANs

Profile Name	Type	WLAN SSID	Admin Status	Security Policies
wireless-test	WLAN	wireless-test	Enabled	WEP
testipv6	WLAN	testipv6	Disabled	
test	WLAN	test	Enabled	
devesh	WLAN	devesh	Enabled	802.1X, Cond-Web-Redirect
guestLAn	Guest LAN	guestLan	Disabled	Web-Auth
wiredguestA	Guest LAN	wiredguestA	Disabled	Web-Auth
GuestLAN1	Guest LAN	LAN1	Disabled	Web-Auth

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 (see Figure 12-16).

Figure 12-16   Mobility Anchors Page


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Mobility Anchor Create
232313

Mobility Anchors

WLAN SSID employee

Switch IP Address (Anchor)	Data Path	Control Path
local	up	up

Switch IP Address (Anchor) 10.100.100.1

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 control information over a well-known UDP port and exchange data traffic through an Ethernet-over-IP (EoIP) tunnel. Specifically, they send mpings, which test mobility control packet reachability over the management interface, over mobility UDP port 16666 and epings, which test the mobility data traffic over the management interface, over EoIP port 97. The Control Path field shows whether mpings have passed (up) or failed (down), and the Data Path field shows whether epings have passed (up) or failed (down). If the Data or Control Path field 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 box.

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.

Using the CLI to Configure Auto-Anchor Mobility

Use these commands to configure auto-anchor mobility using the CLI.

Note Refer to the "Using the GUI to Configure Auto-Anchor Mobility" section on page 12-21 for the valid ranges and default values of the parameters used in the CLI commands.

1. 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.
2. Enter **config {wlan | guest-lan} disable** {*wlan_id* | *guest_lan_id*} to disable the WLAN or wired guest LAN for which you are configuring mobility anchors.

3. To create a new mobility anchor for the WLAN or wired guest LAN, enter 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.

    Note Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor.

4. To delete a mobility anchor for the WLAN or wired guest LAN, enter 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.

5. To save your settings, enter this command:

    save config

6. To see a list and status of controllers configured as mobility anchors for a specific WLAN or wired guest LAN, enter 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 **show mobility anchor**.

    For example, information similar to the following appears for the **show mobility anchor** command:

```
Mobility Anchor Export List
WLAN ID     IP Address      Status
    1       10.50.234.2     UP
    1       10.50.234.6     UP
    2       10.50.234.2     UP
    2       10.50.234.3     CNTRL_DATA_PATH_DOWN

GLAN ID     IP Address      Status
    1       10.20.100.2     UP
    2       10.20.100.3     UP
```

The Status field shows one of these values:

- UP—The controller is reachable and able to pass data.
- CNTRL_PATH_DOWN—The mpings failed. The controller cannot be reached through the control path and is considered failed.
- DATA_PATH_DOWN—The epings failed. The controller cannot be reached and is considered failed.
- CNTRL_DATA_PATH_DOWN—Both the mpings and epings failed. The controller cannot be reached and is considered failed.

7. To see the status of all mobility group members, enter this command:

   show mobility summary

   Information similar to the following appears:

```
Mobility Keepalive interval...................... 10
Mobility Keepalive count......................... 3
Mobility Group members configured................ 3

Controllers configured in the mobility group
MAC Address        IP Address     Group Name     Status
00:0b:85:32:b1:80  10.10.1.1      local          Up
00:0b:85:33:a1:70  10.1.1.2       local          Data Path Down
00:0b:85:23:b2:30  10.20.1.2      local          Up
```

8. To troubleshoot mobility issues, enter these commands:

   - **debug mobility handoff** {**enable** | **disable**}—Debugs mobility handoff issues.
   - **debug mobility keep-alive** {**enable** | **disable**} **all**—Dumps the keepalive packets for all mobility anchors.
   - **debug mobility keep-alive** {**enable** | **disable**} *IP_address*—Dumps the keepalive packets for a specific mobility anchor.

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 12-2 lists the WLAN mobility security values and their corresponding security policy.

Table 12-2 WLAN Mobility Security Values

Security Hexadecimal Value	Security Policy
0x00000000	Security_None
0x00000001	Security_WEP
0x00000002	Security_802_1X
0x00000004	Security_IPSec*
0x00000008	Security_IPSec_Passthrough*
0x00000010	Security_Web
0x00000020	Security_PPTP*
0x00000040	Security_DHCP_Required

Table 12-2 WLAN Mobility Security Values (continued)

Security Hexadecimal Value	Security Policy
0x00000080	Security_WPA_NotUsed
0x00000100	Security_Cranite_Passthrough*
0x00000200	Security_Fortress_Passthrough*
0x00000400	Security_L2TP_IPSec*
0x00000800	Security_802_11i_NotUsed*
0x00001000	Security_Web_Passthrough

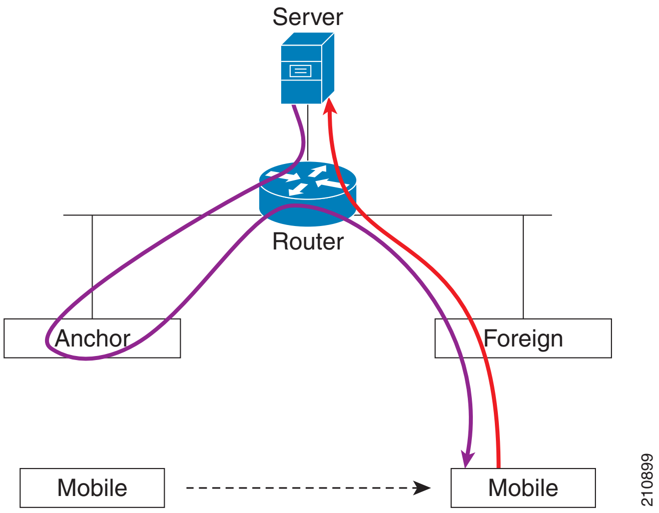
*Controllers running software release 5.2 do not support this security policy.

Using Symmetric Mobility Tunneling

Controller software releases 4.1 through 5.1 support both asymmetric and symmetric mobility tunneling. Controller software release 5.2 supports only symmetric mobility tunneling, which is now always enabled by default.

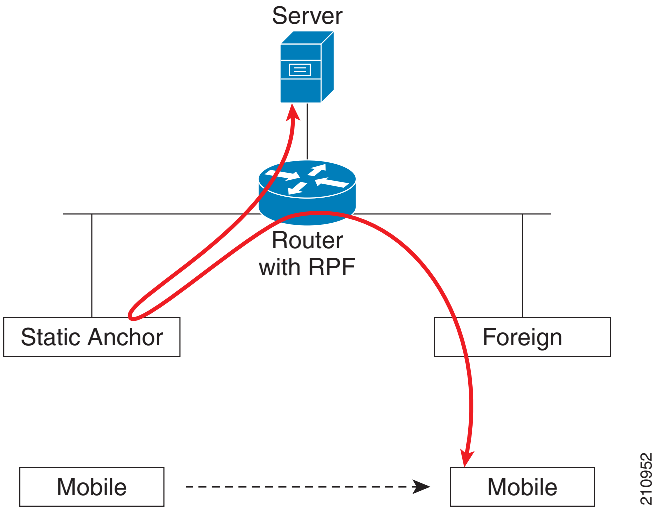
In asymmetric tunneling, client traffic to the wired network is routed directly through the foreign controller, as shown in Figure 12-17.

Figure 12-17 Asymmetric Tunneling or Uni-Directional Tunneling



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 12-18.

Figure 12-18 Symmetric Mobility Tunneling or Bi-Directional Tunneling



Symmetric mobility tunneling is also useful in the following situations:

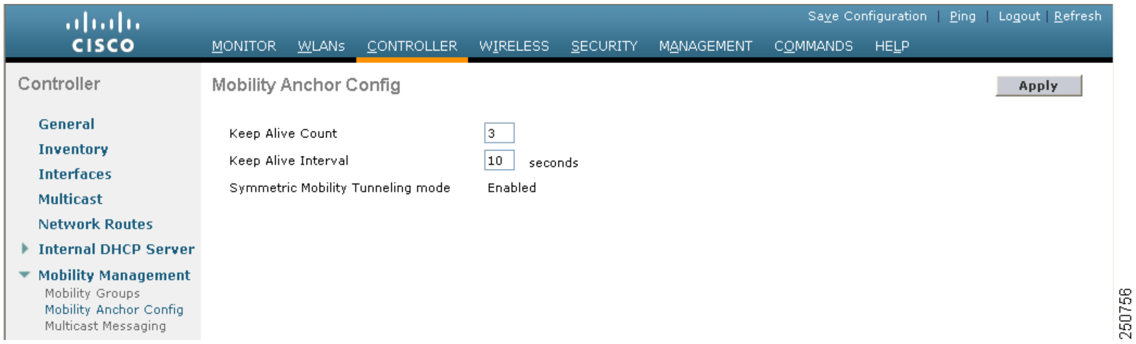
- If a firewall installation in the client packet path drops packets because the source IP address does not match the subnet on which the packets are received.
- If the access-point group VLAN on the anchor controller is different than the WLAN interface VLAN on the foreign controller. In this case, client traffic could be sent on an incorrect VLAN during mobility events.

Note Although a 2100 series controller cannot be designated as an anchor for a WLAN when you are using auto-anchor mobility, it can serve as an anchor in symmetric mobility tunneling to process and forward the upstream client data traffic tunneled from the foreign controller.

Both the controller GUI and CLI show that symmetric mobility tunneling is enabled on the controller:

- To use the controller GUI to verify that symmetric mobility tunneling is enabled, click **Controller** > **Mobility Management** > **Mobility Anchor Config** to open the Mobility Anchor Config page (see Figure 12-19). The Symmetric Mobility Tunneling Mode field shows Enabled.

Figure 12-19 Mobility Anchor Config Page



Mobility Anchor Config

Keep Alive Count 3

Keep Alive Interval 10 seconds

Symmetric Mobility Tunneling mode Enabled

- 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

Controllers configured in the Mobility Group
MAC Address         IP Address    Group Name      Status
00:0b:85:32:b0:80    10.28.8.30       User1        Up
00:0b:85:47:f6:00    10.28.16.10      User1        Up
00:16:9d:ca:d8:e0    10.28.32.10      User1        Up
00:18:73:34:a9:60    10.28.24.10      <local>      Up
00:18:73:36:55:00    10.28.8.10       User1        Up
00:1a:a1:c1:7c:e0    10.28.32.30      User1        Up
00:d0:2b:fc:90:20   10.28.32.61     User1         Control and Data Path Down
```

Running 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.

Controller software release 4.0 or later enables 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.

Use these commands to run mobility ping tests using the controller CLI.

1. To test the mobility UDP control packet communication between two controllers, enter this command:

   mping *mobility_peer_IP_address*

   The *mobility_peer_IP_address* parameter must be the IP address of a controller that belongs to the mobility list.

2. To test the mobility EoIP data packet communication between two controllers, enter this command:

   eping *mobility_peer_IP_address*

   The *mobility_peer_IP_address* parameter must be the IP address of a controller that belongs to the mobility list.

3. To troubleshoot your controller for mobility ping, enter these commands:

   config logging buffered debugging

   show logging

   To troubleshoot your controller for mobility ping over UDP, enter this command to display the mobility control packet:

   debug mobility handoff enable

   Note Cisco recommends using an ethereal trace capture when troubleshooting.

CHAPTER 13

Configuring Hybrid REAPWireless Device Access

This chapter describes hybrid REAP and explains how to configure this feature on controllers and access points. It contains these sections:

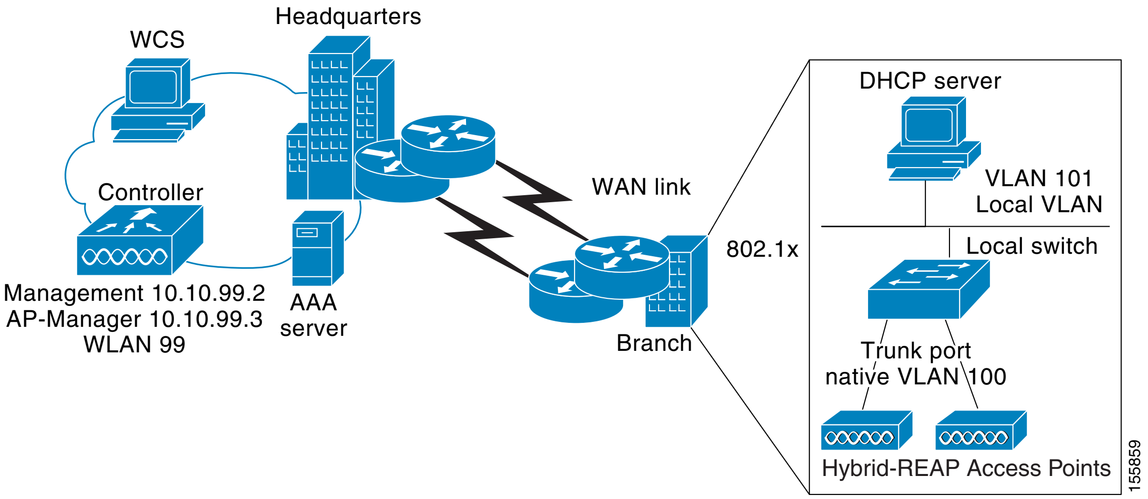
- Overview of Hybrid REAP, page 13-2
- Configuring Hybrid REAP, page 13-5
- Configuring Hybrid-REAP Groups, page 13-15

Overview of Hybrid REAP

Hybrid 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 hybrid-REAP 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.

Hybrid REAP is supported only on the 1130AG, 1140, 1240AG, 1250, and AP801 access points and on the 2100 and 4400 series controllers, the Catalyst 3750G Integrated Wireless LAN Controller Switch, the Cisco WiSM, and the Controller Network Module for Integrated Services Routers. Figure 13-1 illustrates a typical hybrid-REAP deployment.

Figure 13-1 Hybrid REAP Deployment



There is no deployment restriction on the number of hybrid-REAP 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.

Hybrid-REAP Authentication Process

When a hybrid-REAP 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 non-volatile memory for use in standalone mode.

A hybrid-REAP 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 [Layer 3 broadcast, over-the-air provisioning (OTAP), DNS, or DHCP option 43].

> **Note** OTAP does not work on the first boot out of the box. Refer to "The Controller Discovery Process" section on page 7-2 for more information.

- 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 or OTAP, Cisco recommends 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.

Note Refer to Chapter 7 or the controller deployment guide at this URL for more information on how access points find controllers:
http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html

When a hybrid-REAP access point can reach the controller (referred to as *connected mode*), the controller assists in client authentication. When a hybrid-REAP access point cannot access the controller, the access point enters standalone mode and authenticates clients by itself.

Note The LEDs on the access point change as the device enters different hybrid-REAP modes. Refer to the hardware installation guide for your access point for information on LED patterns.

When a client associates to a hybrid-REAP 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 hybrid-REAP access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the hybrid-REAP 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 hybrid-REAP access point handles client authentication and switches client data packets locally. This state is valid only in standalone mode.

  Note External webauth is not supported when using hybrid-REAP with local switching enabled on the WLAN.

- **authentication down, switching down**—In this state, the WLAN disassociates existing clients and stops sending beacon and probe responses. This state is valid only in standalone 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 hybrid-REAP 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, this is also true 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. 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 hybrid-REAP 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, in order to support 802.1X EAP authentication, hybrid-REAP access points in standalone mode need to have their own backup RADIUS server to authenticate clients. This backup RADIUS server may or may not be the one used by the controller. You can configure a backup RADIUS server for individual hybrid-REAP access points in standalone mode by using the controller CLI or for groups of hybrid-REAP 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 hybrid-REAP group.

When a hybrid-REAP 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 hybrid-REAP 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. Furthermore, 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 hybrid-REAP access point supports dynamic frequency selection in standalone 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 3-16 for information on creating quarantined VLANs and the “Configuring NAC Out-of-Band Integration” section on page 6-55 for information on configuring NAC out-of-band support.

The hybrid-REAP access point maintains client connectivity even after entering standalone mode. However, once the access point re-establishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and reallows client connectivity.

Hybrid REAP Guidelines

Keep these guidelines in mind when using hybrid REAP:

- A hybrid-REAP access point can be deployed 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.
- Hybrid REAP supports up to four fragmented packets or a minimum 500-byte maximum transmission unit (MTU) WAN link.
- Roundtrip 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.

- The controller can send multicast packets in the form of unicast or multicast packets to the access point. In hybrid-REAP mode, the access point can receive multicast packets only in unicast form.
- To use CCKM fast roaming with hybrid-REAP access points, you need to configure hybrid-REAP groups. See the "Configuring Hybrid-REAP Groups" section on page 13-15 for more information.
- Hybrid-REAP 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. Hybrid-REAP 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 hybrid-REAP 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, provided that these security types are accessible locally at the access point.
- Hybrid-REAP access points support multiple SSIDs. Refer to the "Using the CLI to Create WLANs" section on page 6-5 for more information.
- NAC out-of-band integration is supported only on WLANs configured for hybrid-REAP central switching. It is not supported for use on WLANs configured for hybrid-REAP local switching. Refer to the "Configuring NAC Out-of-Band Integration" section on page 6-55 for more information.
- The primary and secondary controllers for a hybrid-REAP access point must have the same configuration. Otherwise, the access point might lose its configuration, and certain features (such as WLAN override, AP group VLANs, static channel number, and so on) might not operate correctly. In addition, make sure to duplicate the SSID of the hybrid-REAP access point and its index number on both controllers.

Configuring Hybrid REAP

To configure hybrid REAP, you must follow the instructions in these sections in the order provided:

- Configuring the Switch at the Remote Site, page 13-5
- Configuring the Controller for Hybrid REAP, page 13-6
- Configuring an Access Point for Hybrid REAP, page 13-11
- Connecting Client Devices to the WLANs, page 13-15

Configuring the Switch at the Remote Site

Follow these steps to prepare the switch at the remote site.

Step 1 Attach the access point that will be enabled for hybrid REAP to a trunk or access port on the switch.

Note The sample configuration below shows the hybrid-REAP access point connected to a trunk port on the switch.

Step 2 Refer to the sample configuration below to configure the switch to support the hybrid-REAP access point.

In this sample configuration, the hybrid-REAP 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 in created in the local switch for both VLANs in the switch. The first DHCP pool (NATIVE) will be used by the hybrid-REAP access point, and the second DHCP pool (LOCAL-SWITCH) will be used by the clients when they associate to a WLAN that is locally switched. The bolded text in the sample configuration illustrates these settings.

Note The addresses in this sample configuration are for illustration purposes only. The addresses that you use must fit into your upstream network.

Sample local switch configuration:

```
ip dhcp pool NATIVE
   network 10.10.100.0 255.255.255.0
   default-router 10.10.100.1
!
ip dhcp pool LOCAL-SWITCH
   network 10.10.101.0 255.255.255.0
   default-router 10.10.101.1
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 10.10.98.2 255.255.255.0
 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 10.10.100.1 255.255.255.0
 ip helper-address 10.10.100.1
!
interface Vlan101
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

Configuring the Controller for Hybrid REAP

This section provides instructions for configuring the controller for hybrid REAP using either the GUI or the CLI.

Using the GUI to Configure the Controller for Hybrid REAP

The controller configuration for hybrid REAP consists of creating centrally switched and locally switched WLANs. Follow the steps in this section to use the GUI to configure the controller for these WLANs. This procedure uses these three WLANs as examples:

WLAN	Security	Switching	Interface Mapping (VLAN)
employee	WPA1+WPA2	Central	management (centrally switched VLAN)
employee-local	WPA1+WPA2 (PSK)	Local	101 (locally switched VLAN)
guest-central	Web authentication	Central	management (centrally switched VLAN)

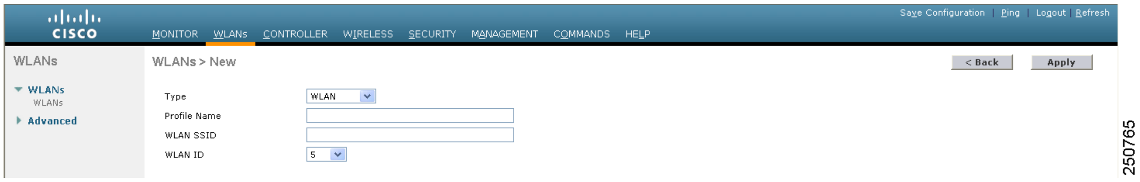
Note See the "Using the CLI to Configure the Controller for Hybrid REAP" section on page 13-11 if you would prefer to configure the controller for hybrid REAP using the CLI.

Step 1 Follow these steps to create a centrally switched WLAN. In our example, this is the first WLAN (employee).

a. Click **WLANs** to open the WLANs page.

b. Choose **Create New** from the drop-down box and click **Go** to open the WLANs > New page (see Figure 13-2).

Figure 13-2 WLANs > New Page



WLANs > New

Type: WLAN

Profile Name:

WLAN SSID:

WLAN ID: 5

c. From the Type drop-down box, choose **WLAN**.

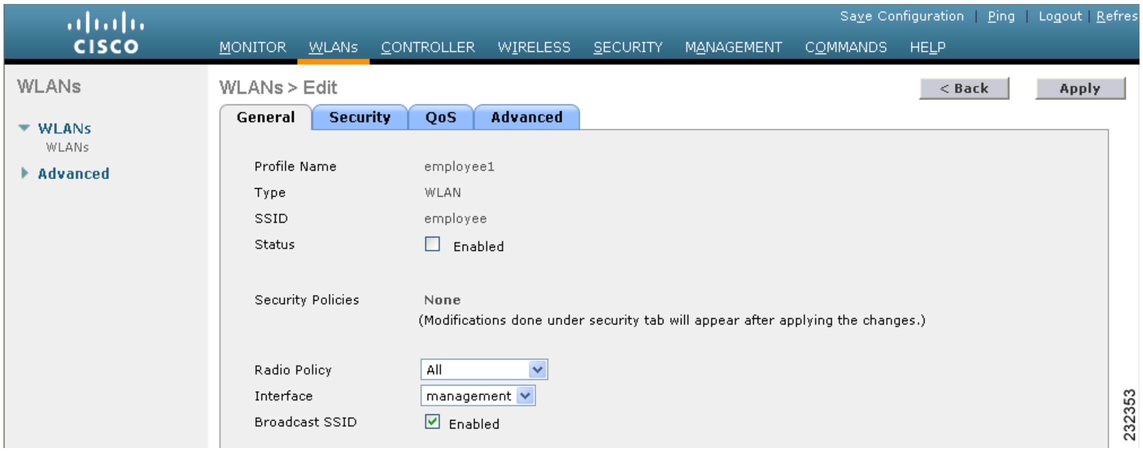
d. Enter a unique profile name for the WLAN in the Profile Name field.

e. Enter a name for the WLAN in the WLAN SSID field.

f. From the WLAN ID drop-down box, choose the ID number for this WLAN.

g. Click **Apply** to commit your changes. The WLANs > Edit page appears (see Figure 13-3).

Figure 13-3 WLANs > Edit Page


Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General
Security
QoS
Advanced
232353

Profile Name employee1
Type WLAN
SSID employee
Status □ Enabled
Security Policies None
(Modifications done under security tab will appear after applying the changes.)
Radio Policy All
Interface management
Broadcast SSID ☑ Enabled

h. Modify the configuration parameters for this WLAN using the various WLANs > Edit tabs. In our employee WLAN example, you would need to choose **WPA+WPA2** for Layer 2 Security from the Security > Layer 2 tabs and then set the WPA+WPA2 parameters.

> **Note** Be sure to enable this WLAN by checking the **Status** check box on the General tab.

> **Note** If NAC is enabled and you created a quarantined VLAN and want to use it for this WLAN, be sure to select it from the Interface drop-down box on the General tab.

i. Click **Apply** to commit your changes.

j. Click **Save Configuration** to save your changes.

Step 2 Follow these steps to create a locally switched WLAN. In our example, this is the second WLAN (employee-local).

a. Follow the substeps in Step 1 to create a new WLAN. In our example, this WLAN is named “employee-local.”

b. When the WLANs > Edit page appears, modify the configuration parameters for this WLAN. In our employee WLAN example, you would need to choose **WPA+WPA2** for Layer 2 Security from the Security > Layer 2 tabs and then set the WPA+WPA2 parameters.

> **Note** Be sure to enable this WLAN by checking the **Status** check box on the General tab. Also, be sure to enable local switching by checking the **H-REAP Local Switching** check box on the Advanced tab. When you enable local switching, any hybrid-REAP access point that advertises this WLAN is able to locally switch data packets (instead of tunneling them to the controller).

Note When you enable hybrid-REAP local switching, the **Learn Client IP Address** check box is enabled 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. Disable this option so that the controller maintains the client connection without waiting to learn the client IP address. The ability to disable this option is supported only with hybrid-REAP local switching; it is not supported with hybrid-REAP central switching.

Note For hybrid-REAP access points, the interface mapping at the controller for WLANs configured for H-REAP Local Switching is inherited at the access point as the default VLAN tagging. This can be easily changed per SSID, per hybrid-REAP access point. Non-hybrid-REAP access points tunnel all traffic back to the controller, and VLAN tagging is dictated by each WLAN's interface mapping.

c. Click **Apply** to commit your changes.

d. Click **Save Configuration** to save your changes.

Step 3 Follow these steps if you also want to create a centrally switched WLAN that is used for guest access. In our example, this is the third WLAN (guest-central). You might want to tunnel guest traffic to the controller so you can exercise your corporate data policies for unprotected guest traffic from a central site.

Note Chapter 10 provides additional information on creating guest user accounts.

a. Follow the substeps in Step 1 to create a new WLAN. In our example, this WLAN is named "guest-central."

b. When the WLANs > Edit page appears, modify the configuration parameters for this WLAN. In our employee WLAN example, you would need to choose **None** for both Layer 2 Security and Layer 3 Security on the Security > Layer 2 and Security > Layer 3 tabs and check the **Web Policy** check box and make sure **Authentication** is selected on the Layer 3 tab.

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. See Chapter 5 for more information on ACLs.

Note Make sure to enable this WLAN by checking the **Status** check box on the General tab.

c. Click **Apply** to commit your changes.

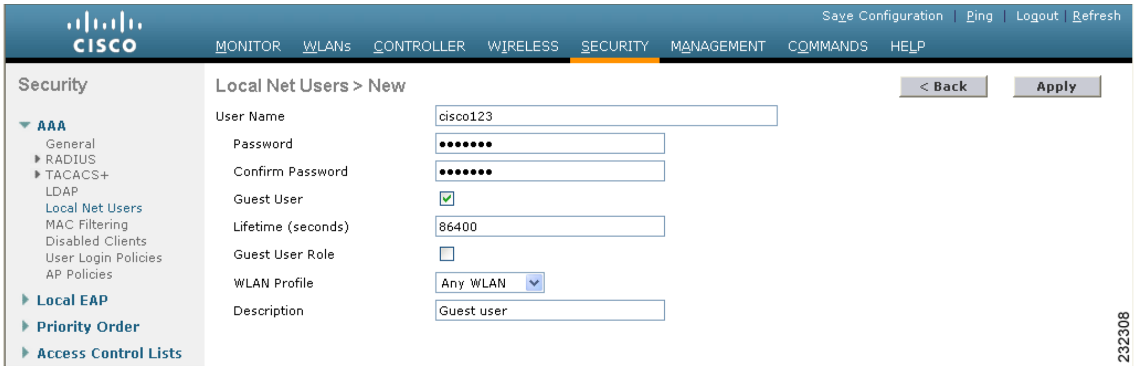
d. Click **Save Configuration** to save your changes.

e. If you want to customize the content and appearance of the login page that guest users will see the first time they access this WLAN, follow the instructions in Chapter 5.

f. To add a local user to this WLAN, click **Security > AAA > Local Net Users**.

g. When the Local Net Users page appears, click **New**. The Local Net Users > New page appears (see Figure 13-4).

Figure 13-4 Local Net Users > New Page



Local Net Users > New

User Name: cisco123

Password: •••••••

Confirm Password: •••••••

Guest User: ☑

Lifetime (seconds): 86400

Guest User Role: □

WLAN Profile: Any WLAN

Description: Guest user

h. In the User Name and Password fields, enter a username and password for the local user.

i. In the Confirm Password field, re-enter the password.

j. Check the **Guest User** check box to enable this local user account.

k. In the Lifetime field, enter the amount of time (in seconds) for this user account to remain active.

l. If you are adding a new user, you checked the Guest User check box, and you want to assign a QoS role to this guest user, check the **Guest User Role** check box. The default setting is unchecked.

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.

m. If you are adding a new user and you checked the Guest User Role check box, choose the QoS role that you want to assign to this guest user from the Role drop-down box. If you want to create a new QoS role, see the "Configuring Quality of Service Roles" section on page 4-48 for instructions.

n. From the WLAN Profile drop-down box, 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.

o. In the Description field, enter a descriptive title for the local user (such as "Guest user").

p. Click **Apply** to commit your changes.

q. Click **Save Configuration** to save your changes.

Step 4 Go to the "Configuring an Access Point for Hybrid REAP" section on page 13-11 to configure up to six access points for hybrid REAP.

Using the CLI to Configure the Controller for Hybrid REAP

Use these commands to configure the controller for hybrid REAP:

- **config wlan h-reap local-switching** *wlan_id* **enable**—Configures the WLAN for local switching.

  Note When you enable hybrid-REAP 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 this command to disable the client IP address learning feature so that the controller maintains the client connection without waiting to learn the client IP address: **config wlan h-reap learn-ipaddr** *wlan_id* **disable**. The ability to disable this feature is supported only with hybrid-REAP local switching; it is not supported with hybrid-REAP central switching. If you later want to re-enable this feature, enter this command: **config wlan h-reap learn-ipaddr** *wlan_id* **enable**.

- **config wlan h-reap local-switching** *wlan_id* **disable—**Configures the WLAN for central switching. This is the default value.

Note Go to the "Configuring an Access Point for Hybrid REAP" section on page 13-11 to configure up to six access points for hybrid REAP.

Use these commands to obtain hybrid-REAP 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 hreap aaa** {**event** | **error**} {**enable** | **disable**}—Enables or disables debugging of hybrid-REAP backup RADIUS server events or errors.
- **debug hreap cckm** {**enable** | **disable**}—Enables or disables debugging of hybrid-REAP CCKM.
- **debug hreap group** {**enable** | **disable**}—Enables or disables debugging of hybrid-REAP 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 Hybrid REAP

This section provides instructions for configuring an access point for hybrid REAP using either the controller GUI or CLI.

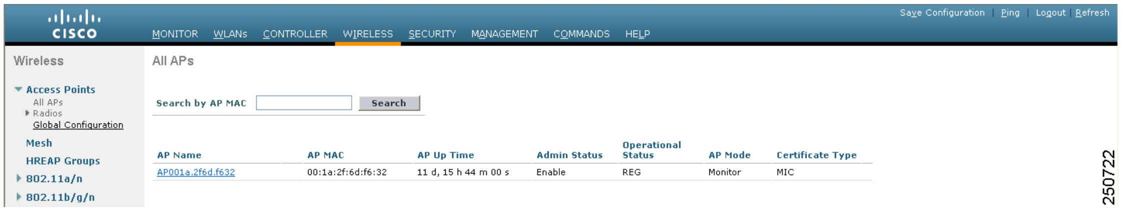
Using the GUI to Configure an Access Point for Hybrid REAP

Follow these steps to configure an access point for hybrid REAP using the controller GUI.

Step 1 Make sure that the access point has been physically added to your network.

Step 2 Click **Wireless** to open the All APs page (see Figure 13-5).

Figure 13-5 All APs Page


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Save Configuration | Ping | Logout | Refresh
Wireless
Access Points
All APs
Radios
Global Configuration
Mesh
HREAP Groups
802.11a/n
802.11b/g/n
Search
250722

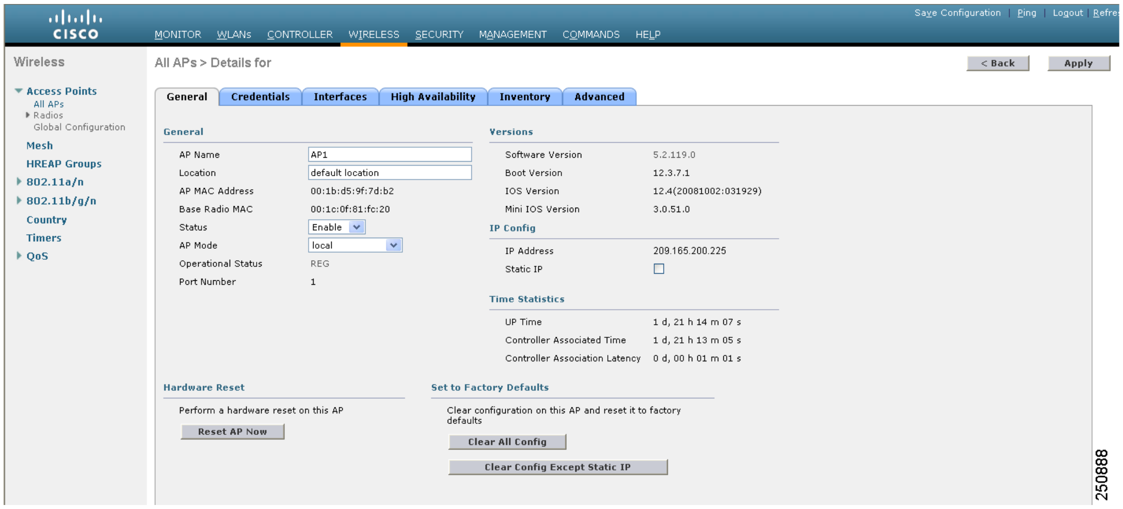
All APs

Search by AP MAC

AP Name	AP MAC	AP Up Time	Admin Status	Operational Status	AP Mode	Certificate Type
AP001a.2f6d.f632	00:1a:2f:6d:f6:32	11 d, 15 h 44 m 00 s	Enable	REG	Monitor	MIC

Step 3 Click the name of the desired access point. The All APs > Details (General) page appears (see Figure 13-6).

Figure 13-6 All APs > Details for (General) Page



All APs > Details for

General

AP Name AP1
Location default location
AP MAC Address 00:1b:d5:9f:7d:b2
Base Radio MAC 00:1c:0f:81:fc:20
Status Enable
AP Mode local
Operational Status REG
Port Number 1

Versions

Software Version 5.2.119.0
Boot Version 12.3.7.1
IOS Version 12.4(20081002:031929)
Mini IOS Version 3.0.51.0

IP Config

IP Address 209.165.200.225
Static IP ☐

Time Statistics

UP Time 1 d, 21 h 14 m 07 s
Controller Associated Time 1 d, 21 h 13 m 05 s
Controller Association Latency 0 d, 00 h 01 m 01 s

Hardware Reset

Perform a hardware reset on this AP

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

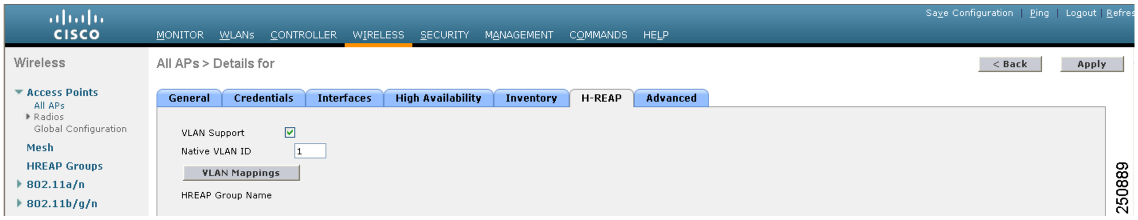
Step 4 Choose **H-REAP** from the AP Mode drop-down box to enable hybrid REAP for this access point.

Note The last parameter on the Inventory tab indicates whether this access point can be configured for hybrid REAP. Only the 1130AG, 1240AG, and 1250 access points support hybrid REAP.

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

Step 6 Click the **H-REAP** tab to open the All APs > Details for (H-REAP) page (see Figure 13-7).

Figure 13-7 All APs > Details for (H-REAP) Page



All APs > Details for

VLAN Support ☑
Native VLAN ID 1
HREAP Group Name

If the access point belongs to a hybrid-REAP group, the name of the group appears in the HREAP Group Name field.

Step 7 Check 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** field.

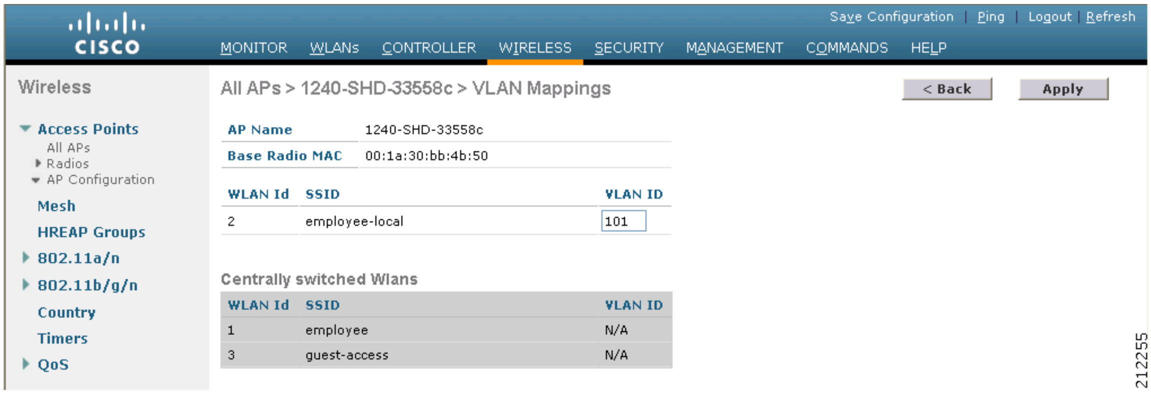
Note By default, a VLAN is not enabled on the hybrid-REAP access point. Once hybrid REAP is enabled, the access point inherits the VLAN ID associated to the WLAN. This configuration is saved in the access point and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per hybrid-REAP access point in a VLAN-enabled domain. Otherwise, the access point cannot send and receive packets to and from the controller.

Step 8 Click **Apply** to commit your changes. The access point temporarily loses its connection to the controller while its Ethernet port is reset.

Step 9 Click the name of the same access point and then click the **H-REAP** tab.

Step 10 Click **VLAN Mappings** to open the All APs > *Access Point Name* > VLAN Mappings page (see Figure 13-8).

Figure 13-8 All APs > Access Point Name > VLAN Mappings Page



All APs > 1240-SHD-33558c > VLAN Mappings

AP Name	1240-SHD-33558c
Base Radio MAC	00:1a:30:bb:4b:50

WLAN Id	SSID	VLAN ID
2	employee-local	101

Centrally switched Wlans

WLAN Id	SSID	VLAN ID
1	employee	N/A
3	guest-access	N/A

Step 11 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 field.

Step 12 Click **Apply** to commit your changes.

Step 13 Click **Save Configuration** to save your changes.

Step 14 Repeat this procedure for any additional access points that need to be configured for hybrid REAP at the remote site.

Using the CLI to Configure an Access Point for Hybrid REAP

Use these commands on the controller to configure an access point for hybrid REAP:

- **config ap mode h-reap** *Cisco_AP***—**Enables hybrid REAP for this access point.
- **config ap h-reap radius auth set** {**primary** | **secondary**} *ip_address auth_port secret Cisco_AP*—Configures a primary or secondary RADIUS server for a specific hybrid-REAP 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 hybrid-REAP access point, enter this command: **config ap h-reap radius auth delete** {**primary** | **secondary**} *Cisco_AP*

- **config ap h-reap vlan wlan** *wlan_id vlan-id Cisco_AP***—**Enables you to assign a VLAN ID to this hybrid-REAP access point. By default, the access point inherits the VLAN ID associated to the WLAN.
- **config ap h-reap vlan** {**enable** | **disable**} *Cisco_AP*—Enables or disables VLAN tagging for this hybrid-REAP access point. By default, VLAN tagging is not enabled. Once VLAN tagging is enabled on the hybrid-REAP access point, WLANs enabled for local switching inherit the VLAN assigned at the controller.
- **config ap h-reap vlan native** *vlan-id Cisco_AP*—Enables you to configure a native VLAN for this hybrid-REAP access point. By default, no VLAN is set as the native VLAN. One native VLAN must be configured per hybrid-REAP access point (when VLAN tagging is enabled). Make sure the switchport to which the access point is connected has a corresponding native VLAN configured as well. If the hybrid-REAP 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.

Use these commands on the hybrid-REAP access point to obtain status information:

- **show capwap reap status**—Shows the status of the hybrid-REAP 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 hybrid-REAP access point to obtain debug information:

- **debug capwap reap—**Shows general hybrid-REAP activities.
- **debug capwap reap mgmt**—Shows client authentication and association messages.
- **debug capwap reap load**—Shows payload activities, which is useful when the hybrid-REAP 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.

Connecting Client Devices to the WLANs

Follow the instructions for your client device to create profiles to connect to the WLANs you created in the "Configuring the Controller for Hybrid REAP" section on page 13-6.

In our example, you would create three profiles on the client:

1. To connect to the "employee" WLAN, you would create a client profile that uses WPA/WPA2 with PEAP-MSCHAPV2 authentication. Once the client becomes authenticated, it should get an IP address from the management VLAN of the controller.
2. To connect to the "local-employee" WLAN, you would create a client profile that uses WPA/WPA2 authentication. Once the client becomes authenticated, it should get an IP address from VLAN 101 on the local switch.
3. To connect to the "guest-central" WLAN, you would create a client profile that uses open authentication. Once the client becomes authenticated, it should get an IP address from VLAN 101 on the network local to the access point. Once 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 his or her username and password.

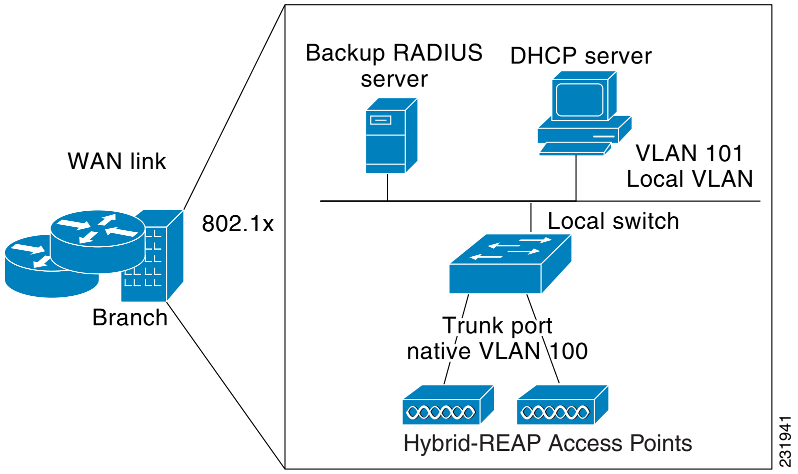
To see if a client's data traffic is being locally or centrally switched, click **Monitor** > **Clients** on the controller GUI, click the **Detail** link for the desired client, and look at the Data Switching parameter under AP Properties.

Configuring Hybrid-REAP Groups

In order to better organize and manage your hybrid-REAP access points, you can create hybrid-REAP groups and assign specific access points to them. Per controller, you can configure up to 20 hybrid-REAP groups with up to 25 access points per group.

All of the hybrid-REAP access points in a group share the same WLAN, backup RADIUS server, CCKM, and local authentication configuration information. This feature is helpful if you have multiple hybrid-REAP 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 hybrid-REAP group rather than having to configure the same server on each access point. Figure 13-9 illustrates a typical hybrid-REAP group deployment with a backup RADIUS server in the branch office.

Figure 13-9 Hybrid-REAP Group Deployment



Hybrid-REAP Groups and Backup RADIUS Servers

You can configure the controller to allow a hybrid-REAP 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 are used only when the hybrid-REAP access point is not connected to the controller.

Hybrid-REAP Groups and CCKM

Hybrid-REAP groups are required for CCKM fast roaming to work with hybrid-REAP 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 hybrid-REAP 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 hybrid-REAP group comprising a limited number of access points (for example, you create a group for four access points in a remote office), the clients roam only among those four access points, and the CCKM cache is distributed among those four access points only when the clients associate to one of them.

Note CCKM fast roaming among hybrid-REAP and non-hybrid-REAP access points is not supported. Refer to the "WPA1 and WPA2" section on page 6-22 for information on configuring CCKM.

Hybrid-REAP Groups and Local Authentication

You can configure the controller to allow a hybrid-REAP 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 hybrid-REAP 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 hybrid-REAP access point network and are not interested in maintaining a large user database nor adding another hardware device to replace the RADIUS server functionality available in the autonomous access point.

Note This feature can be used in conjunction with the hybrid-REAP backup RADIUS server feature. If a hybrid-REAP group is configured with both a backup RADIUS server and local authentication, the hybrid-REAP 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 hybrid-REAP access point itself (if the primary and secondary are not reachable).

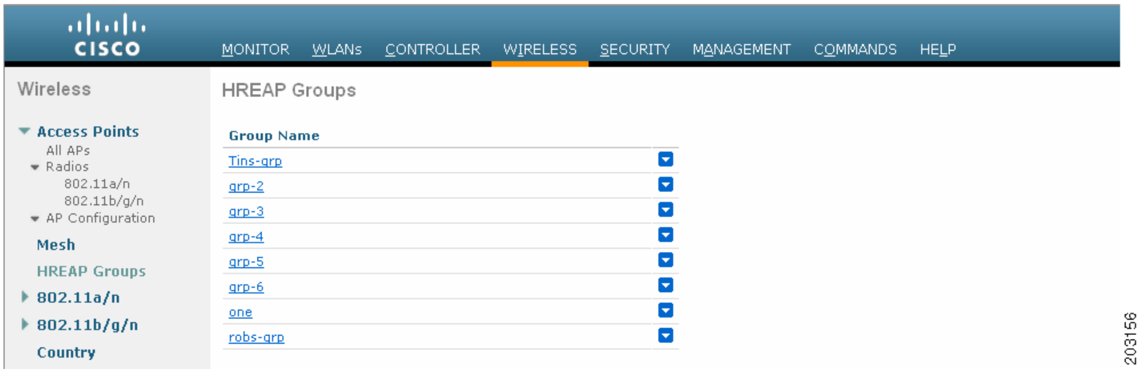
Follow the instructions in this section to configure hybrid-REAP groups using the controller GUI or CLI.

Using the GUI to Configure Hybrid-REAP Groups

Follow these steps to configure hybrid-REAP groups using the controller GUI.

Step 1 Click **Wireless** > **HREAP Groups** to open the HREAP Groups page (see Figure 13-10).

Figure 13-10 HREAP Groups Page



HREAP Groups

Group Name
Tins-grp
grp-2
grp-3
grp-4
grp-5
grp-6
one
robs-grp

This page lists any hybrid-REAP 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**.

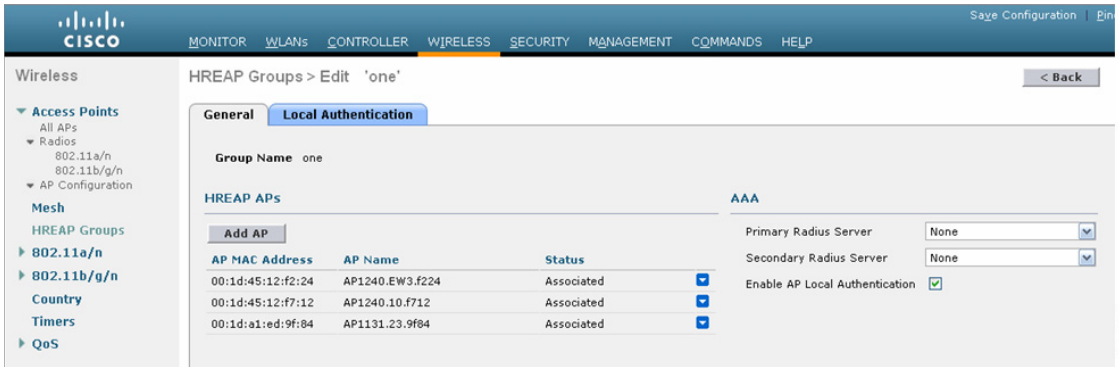
Step 2 To create a new hybrid-REAP group, click **New**.

Step 3 When the HREAP Groups > New page appears, enter the name of the new group in the Group Name field. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply** to commit your changes. The new group appears on the HREAP Groups page.

Step 5 To edit the properties of a group, click the name of the desired group. The HREAP Groups > Edit (General) page appears (see Figure 13-11).

Figure 13-11 HREAP Groups > Edit (General) Page



HREAP Groups > Edit 'one'

Group Name one

HREAP APs

AP MAC Address	AP Name	Status
00:1d:45:12:f2:24	AP1240.EW3.f224	Associated
00:1d:45:12:f7:12	AP1240.10.f712	Associated
00:1d:a1:ed:9f:84	AP1131.23.9f84	Associated

AAA

Primary Radius Server None

Secondary Radius Server None

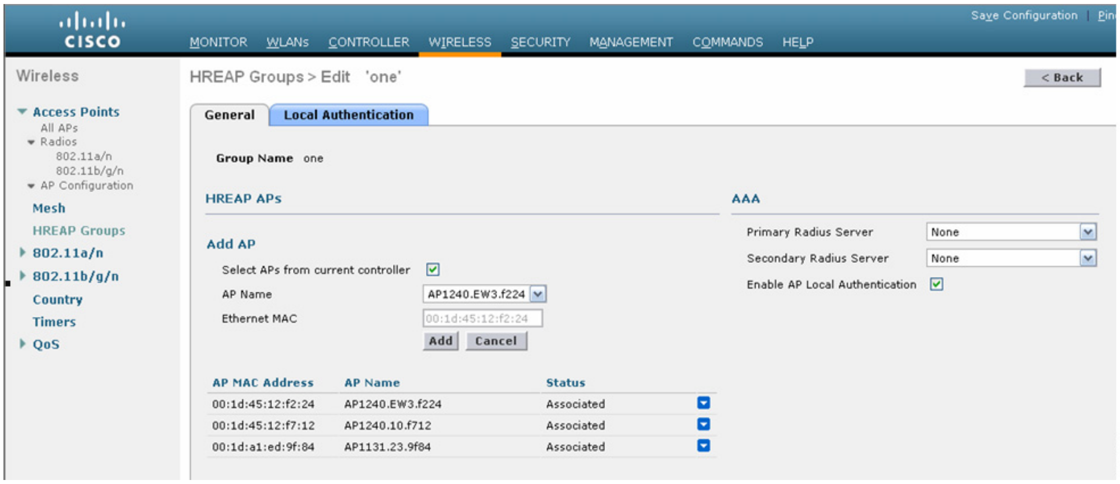
Enable AP Local Authentication ☑

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 field 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" (see Figure 13-12).

Figure 13-12 HREAP Groups > Edit (General) Page



HREAP Groups > Edit 'one'

Group Name one

HREAP APs

Add AP

Select APs from current controller ☑

AP Name AP1240.EW3.f224

Ethernet MAC 00:1d:45:12:f2:24

AP MAC Address	AP Name	Status
00:1d:45:12:f2:24	AP1240.EW3.f224	Associated
00:1d:45:12:f7:12	AP1240.10.f712	Associated
00:1d:a1:ed:9f:84	AP1131.23.9f84	Associated

AAA

Primary Radius Server None

Secondary Radius Server None

Enable AP Local Authentication ☑

Step 9 Perform one of the following:

- To choose an access point that is connected to this controller, check the **Select APs from Current Controller** check box and choose the name of the access point from the AP Name drop-down box.

  Note If you choose an access point on this controller, the MAC address of the access point is automatically entered in the Ethernet MAC field 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 unchecked and enter its MAC address in the Ethernet MAC field.

  Note If the hybrid-REAP 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 hybrid-REAP 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 hybrid-REAP group.

Step 13 If you want to enable local authentication for a hybrid-REAP group, follow these steps:

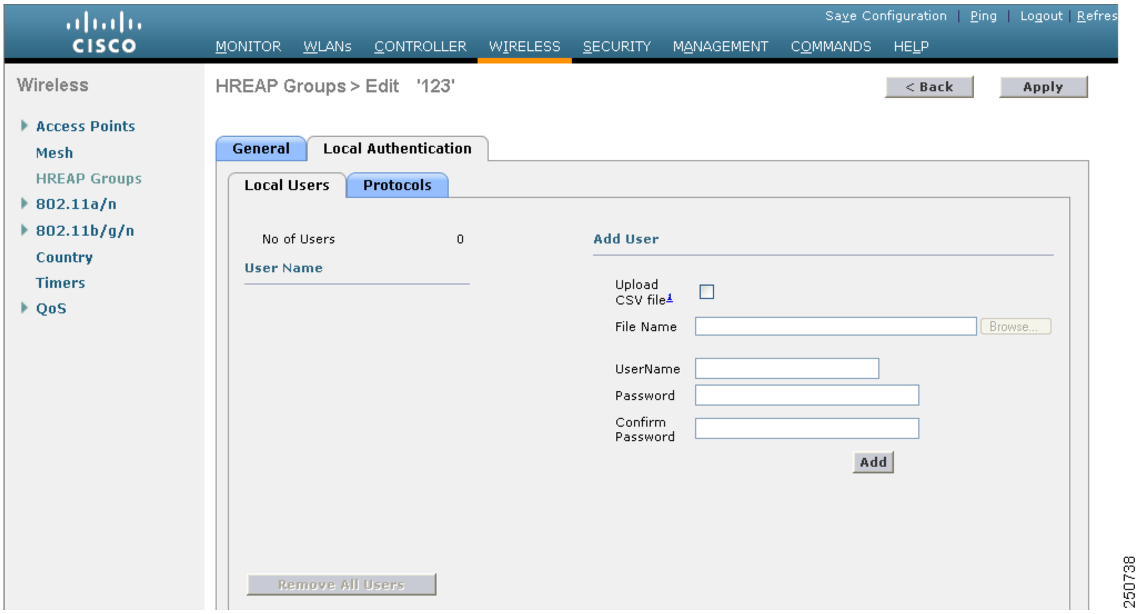
a. Make sure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to **None**.

b. Check the **Enable AP Local Authentication** check box to enable local authentication for this hybrid-REAP group. The default value is unchecked.

c. Click **Apply** to commit your changes.

d. Click the **Local Authentication** tab to open the HREAP Groups > Edit (Local Authentication > Local Users) page (see Figure 13-13).

Figure 13-13 HREAP Groups > 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:

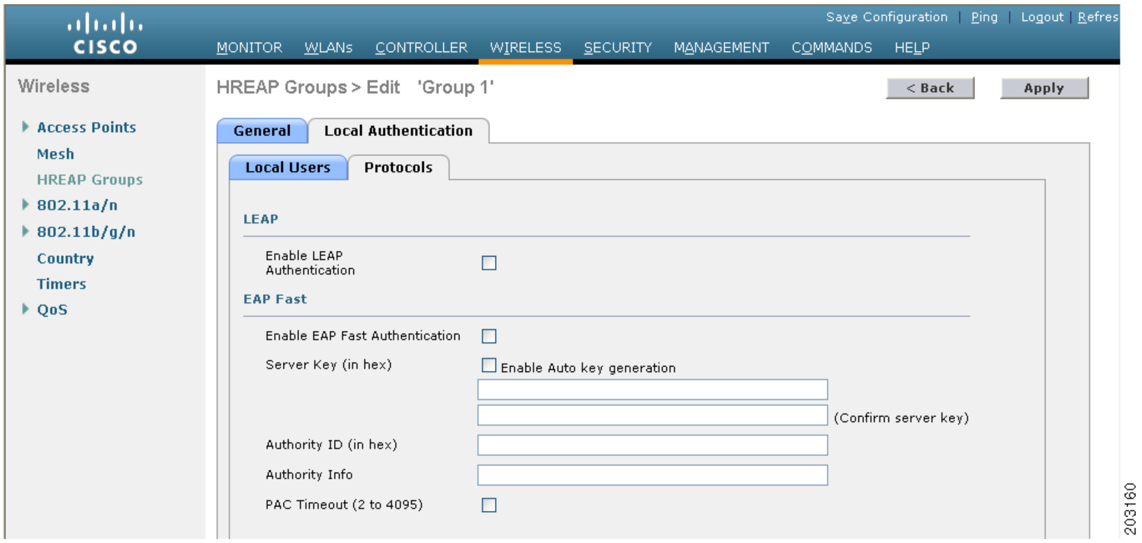
- Upload a comma-separated values (CSV) file by checking the **Upload CSV File** check box, clicking the **Browse** button to browse to an CSV file that contains usernames and passwords (each line of the file needs to be in the following format: username, password), and clicking **Add** to upload the 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 field and a password for the client in the Password and Confirm Password fields, 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 HREAP Groups > Edit (Local Authentication > Protocols) page (see Figure 13-14).

Figure 13-14 HREAP Groups > Edit (Local Authentication > Protocols) Page



HREAP Groups > Edit 'Group 1'

LEAP

Enable LEAP Authentication □

EAP Fast

Enable EAP Fast Authentication □

Server Key (in hex) □ Enable Auto key generation

(Confirm server key)

Authority ID (in hex)

Authority Info

PAC Timeout (2 to 4095) □

h. To allow a hybrid-REAP access point to authenticate clients using LEAP, check the **Enable LEAP Authentication** check box; then go to Step n.

i. To allow a hybrid-REAP access point to authenticate clients using EAP-FAST, check the **Enable EAP-FAST Authentication** check box; then go to the next step. The default value is unchecked.

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 fields. The key must be 32 hexadecimal characters.
- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, check the **Enable Auto Key Generation** check box.

k. In the Authority ID field, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

l. In the Authority Info field, 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, check the **PAC Timeout** check box and enter the number of seconds for the PAC to remain viable in the edit box. The default value is unchecked, 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 hybrid-REAP groups.

Note To see if an individual access point belongs to a hybrid-REAP group, you can click **Wireless** > **Access Points** > **All APs** > the name of the desired access point > the **H-REAP** tab. If the access point belongs to a hybrid-REAP group, the name of the group appears in the HREAP Group Name field.

Using the CLI to Configure Hybrid-REAP Groups

Follow these steps to configure hybrid-REAP groups using the controller CLI.

Step 1 To add or delete a hybrid-REAP group, enter this command:

config hreap group *group_name* {**add** | **delete**}

Step 2 To configure a primary or secondary RADIUS server for the hybrid-REAP group, enter this command:

config hreap group *group_name* **radius server** {**add** | **delete**} {**primary** | **secondary**} *server_index*

Step 3 To add an access point to the hybrid-REAP group, enter this command:

config hreap group *group_name* **ap** {**add** | **delete**} *ap_mac*

Step 4 To configure local authentication for a hybrid-REAP group, follow these steps:

a. Make sure that a primary and secondary RADIUS server are not configured for the hybrid-REAP group.

b. To enable or disable local authentication for this hybrid-REAP group, enter this command:

config hreap group *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:

config hreap group *group_name* **radius ap user add** *username* **password** *password*

Note You can add up to 100 clients.

d. To allow a hybrid-REAP access point to authenticate clients using LEAP or to disable this behavior, enter this command:

config hreap group *group_name* **radius ap leap** {**enable** | **disable**}

e. To allow a hybrid-REAP access point to authenticate clients using EAP-FAST or to disable this behavior, enter this command:

config hreap group *group_name* **radius ap eap-fast** {**enable** | **disable**}

f. Enter one of the following commands, depending on how you want PACs to be provisioned:

- **config hreap group** *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 hreap group** *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 hreap group *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 hreap group *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 hreap group *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 the default value, disables the PAC timeout.

Step 5 To save your changes, enter this command:

save config

Step 6 To see the current list of hybrid-REAP groups, enter this command:

show hreap group summary

Information similar to the following appears:

```
HREAP Group Summary: Count 2

Group Name     # Aps
Group 1        1
Group 2        1
```

Step 7 To see the details for a specific hybrid-REAP group, enter this command:

show hreap 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 User's in Group: 20

                   1cisco                   2cisco
                   3cisco                   4cisco
                    cisco                    test1
                   test10                   test11
                   test12                   test13
                   test14                   test15
                    test2                    test3
                    test4                    test5
                    test6                    test7
                   test8                 test9
```

APPENDIX **A**

Safety Considerations and Translated Safety Warnings

This appendix lists safety considerations and translations of the safety warnings that apply to the Cisco UWN Solution products. The following safety considerations and safety warnings appear in this appendix:

- Safety Considerations, page A-2
- Warning Definition, page A-2
- Class 1 Laser Product Warning, page A-5
- Ground Conductor Warning, page A-7
- Chassis Warning for Rack-Mounting and Servicing, page A-9
- Battery Handling Warning for 4400 Series Controllers, page A-18
- Equipment Installation Warning, page A-20
- More Than One Power Supply Warning for 4400 Series Controllers, page A-23

Safety Considerations

Keep these guidelines in mind when installing Cisco UWN Solution products:

- The Cisco lightweight access points with or without external antenna ports are only intended for installation in Environment A as defined in IEEE 802.3af. All interconnected equipment must be contained within the same building including the interconnected equipment's associated LAN connections.
- For lightweight access points provided with optional external antenna ports, make sure that all external antennas and their associated wiring are located entirely indoors. These lightweight access points and their optional external antennas are not suitable for outdoor use.
- Make sure that plenum-mounted lightweight access points are powered using Power over Ethernet (PoE) to comply with safety regulations.
- For all controllers, verify that the ambient temperature remains between 0 and 40° C (32 and 104° F), taking into account the elevated temperatures that occur when they are installed in a rack.
- When multiple controllers are mounted in an equipment rack, be sure that the power source is sufficiently rated to safely run all of the equipment in the rack.
- Verify the integrity of the ground before installing controllers in an equipment rack.
- Lightweight access points are suitable for use in environmental air space in accordance with Section 300.22.C of the National Electrical Code, and Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, C22.1.

Warning Definition

Warning **IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

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

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

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

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

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

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

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

SPARA DESSA ANVISNINGAR

FONTOS BIZTONSÁGI ELOÍRÁSOK

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

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

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

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

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

请保存这些安全性说明

警告 安全上の重要な注意事項

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

これらの注意事項を保管しておいてください。

Class 1 Laser Product Warning

Note The 1000BASE-SX and 1000BASE-LX SFP modules contain Class 1 Lasers (Laser Klasse 1) according to EN 60825-1+A1+A2.

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

Waarschuwing **Klasse-1 laser produkt.**

Varoitus **Luokan 1 lasertuote.**

Attention **Produit laser de classe 1.**

Warnung **Laserprodukt der Klasse 1.**

Avvertenza **Prodotto laser di Classe 1.**

Advarsel **Laserprodukt av klasse 1.**

Aviso **Produto laser de classe 1.**

¡Advertencia! **Producto láser Clase I.**

Varning! **Laserprodukt av klass 1.**

Class 1 besorolású lézeres termék.

Предупреждение Лазерное устройство класса 1.

警告 这是 1 类激光产品。

警告 クラス1レーザー製品です。

Aviso **Produto a laser de classe 1.**

Advarsel **Klasse 1 laserprodukt.**

تحذير **Class 1 Laser ١ منتج**

Upozorenje **Laserski proizvod klase 1**

Upozornění **Laserový výrobek třídy 1.**

Προειδοποίηση Προϊόν λέιζερ κατηγορίας 1.

אזהרה מוצר לייזר Class 1.

Opomena Ласерски производ од класа 1.

Ostrzeżenie **Produkt laserowy klasy 1.**

Upozornenie **Laserový výrobok triedy 1.**

Class 1 besorolású lézeres termék.

Предупреждение Лазерное устройство класса 1.

警告 这是 1 类激光产品。

警告 クラス1レーザー製品です。

주의 클래스 1 레이저 제품.

تحذير **منتج ١ Class 1 Laser**

Upozorenje **Laserski proizvod klase 1**

Upozornění **Laserový výrobek třídy 1.**

Προειδοποίηση Προϊόν λέιζερ κατηγορίας 1.

אזהרה מוצר לייזר Class 1.

Opomena Ласерски производ од класа 1.

Ostrzeżenie **Produkt laserowy klasy 1.**

Upozornenie **Laserový výrobok triedy 1.**

Ground Conductor Warning

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Waarschuwing **Deze apparatuur dient geaard te zijn. De aardingsleiding mag nooit buiten werking worden gesteld en de apparatuur mag nooit bediend worden zonder dat er een op de juiste wijze geïnstalleerde aardingsleiding aanwezig is. Neem contact op met de bevoegde instantie voor elektrische inspecties of met een elektricien als u er niet zeker van bent dat er voor passende aarding gezorgd is.**

Varoitus **Laitteiden on oltava maadoitettuja. Älä koskaan ohita maajohdinta tai käytä laitteita ilman oikein asennettua maajohdinta. Ota yhteys sähkötarkastusviranomaiseen tai sähköasentajaan, jos olet epävarma maadoituksen sopivuudesta.**

Attention **Cet équipement doit être mis à la masse. Ne jamais rendre inopérant le conducteur de masse ni utiliser l'équipement sans un conducteur de masse adéquatement installé. En cas de doute sur la mise à la masse appropriée disponible, s'adresser à l'organisme responsable de la sécurité électrique ou à un électricien.**

Warnung **Dieses Gerät muss geerdet sein. Auf keinen Fall den Erdungsleiter unwirksam machen oder das Gerät ohne einen sachgerecht installierten Erdungsleiter verwenden. Wenn Sie sich nicht sicher sind, ob eine sachgerechte Erdung vorhanden ist, wenden Sie sich an die zuständige Inspektionsbehörde oder einen Elektriker.**

Avvertenza **Questa apparecchiatura deve essere dotata di messa a terra. Non escludere mai il conduttore di protezione né usare l'apparecchiatura in assenza di un conduttore di protezione installato in modo corretto. Se non si è certi della disponibilità di un adeguato collegamento di messa a terra, richiedere un controllo elettrico presso le autorità competenti o rivolgersi a un elettricista.**

Advarsel **Dette utstyret må jordes. Omgå aldri jordingslederen og bruk aldri utstyret uten riktig montert jordingsleder. Ta kontakt med fagfolk innen elektrisk inspeksjon eller med en elektriker hvis du er usikker på om det finnes velegnet jordning.**

Aviso **Este equipamento deve ser aterrado. Nunca anule o fio terra nem opere o equipamento sem um aterramento adequadamente instalado. Em caso de dúvida com relação ao sistema de aterramento disponível, entre em contato com os serviços locais de inspeção elétrica ou um eletricista qualificado.**

¡Advertencia! **Este equipo debe estar conectado a tierra. No inhabilite el conductor de tierra ni haga funcionar el equipo si no hay un conductor de tierra instalado correctamente. Póngase en contacto con la autoridad correspondiente de inspección eléctrica o con un electricista si no está seguro de que haya una conexión a tierra adecuada.**

Varning! **Denna utrustning måste jordas. Koppla aldrig från jordledningen och använd aldrig utrustningen utan en på lämpligt sätt installerad jordledning. Om det föreligger osäkerhet huruvida lämplig jordning finns skall elektrisk besiktningsauktoritet eller elektriker kontaktas.**

A berendezés csak megfelelő védőföldeléssel működtethető. Ne iktassa ki a földelés csatlakozóját, és ne üzemeltesse a berendezést szabályosan felszerelt földelő vezeték nélkül! Ha nem biztos benne, hogy megfelelő földelés áll rendelkezésbe, forduljon a helyi elektromos hatóságokhoz vagy egy villanyszerelőhöz.

Предупреждение Данное устройство должно быть заземлено. Никогда не отключайте провод заземления и не пользуйтесь оборудованием при отсутствии правильно подключенного провода заземления. За сведениями об имеющихся возможностях заземления обратитесь к соответствующим контролирующим организациям по энергоснабжению или к инженеру-электрику.

警告 此设备必须接地。切勿使接地导体失效，或者在没有正确安装接地导体的情况下操作该设备。如果您不能肯定接地导体是否正常发挥作用，请咨询有关电路检测方面的权威人士或电工。

警告 この装置はアース接続する必要があります。アース導体を破損しないよう注意し、アース導体を正しく取り付けないまま装置を稼働させないでください。アース接続が適正であるかどうか分からない場合には、電気検査機関または電気技術者に相談してください。

A berendezés csak megfelelő védőföldeléssel működtethető. Ne iktassa ki a földelés csatlakozóját, és ne üzemeltesse a berendezést szabályosan felszerelt földelő vezeték nélkül! Ha nem biztos benne, hogy megfelelő földelés áll rendelkezésbe, forduljon a helyi elektromos hatóságokhoz vagy egy villanyszerelőhöz.

Предупреждение Данное устройство должно быть заземлено. Никогда не отключайте провод заземления и не пользуйтесь оборудованием при отсутствии правильно подключенного провода заземления. За сведениями об имеющихся возможностях заземления обратитесь к соответствующим контролирующим организациям по энергоснабжению или к инженеру-электрику.

警告 此设备必须接地。切勿使接地导体失效，或者在没有正确安装接地导体的情况下操作该设备。如果您不能肯定接地导体是否正常发挥作用，请咨询有关电路检测方面的权威人士或电工。

警告 この装置はアース接続する必要があります。アース導体を破損しないよう注意し、アース導体を正しく取り付けないまま装置を稼働させないでください。アース接続が適正であるかどうか分からない場合には、電気検査機関または電気技術者に相談してください。

Chassis Warning for Rack-Mounting and Servicing

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

- **This unit should be mounted at the bottom of the rack if it is the only unit in the rack.**
- **When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.**
- **If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.** Statement 1006

Waarschuwing **Om lichamelijk letsel te voorkomen wanneer u dit toestel in een rek monteert of het daar een servicebeurt geeft, moet u speciale voorzorgsmaatregelen nemen om ervoor te zorgen dat het toestel stabiel blijft. De onderstaande richtlijnen worden verstrekt om uw veiligheid te verzekeren:**

- **Dit toestel dient onderaan in het rek gemonteerd te worden als het toestel het enige in het rek is.**
- **Wanneer u dit toestel in een gedeeltelijk gevuld rek monteert, dient u het rek van onderen naar boven te laden met het zwaarste onderdeel onderaan in het rek.**
- **Als het rek voorzien is van stabiliseringshulpmiddelen, dient u de stabilisatoren te monteren voordat u het toestel in het rek monteert of het daar een servicebeurt geeft.**

Varoitus **Kun laite asetetaan telineeseen tai huolletaan sen ollessa telineessä, on noudatettava erityisiä varotoimia järjestelmän vakavuuden säilyttämiseksi, jotta vältytään loukkaantumiselta. Noudata seuraavia turvallisuusohjeita:**

- Jos telineessä ei ole muita laitteita, aseta laite telineen alaosaan.
- Jos laite asetetaan osaksi täytettyyn telineeseen, aloita kuormittaminen sen alaosasta kaikkein raskaimmalla esineellä ja siirry sitten sen yläosaan.
- Jos telinettä varten on vakaimet, asenna ne ennen laitteen asettamista telineeseen tai sen huoltamista siinä.

Attention **Pour éviter toute blessure corporelle pendant les opérations de montage ou de réparation de cette unité en casier, il convient de prendre des précautions spéciales afin de maintenir la stabilité du système. Les directives ci-dessous sont destinées à assurer la protection du personnelþ:**

- Si cette unité constitue la seule unité montée en casier, elle doit être placée dans le bas.
- Si cette unité est montée dans un casier partiellement rempli, charger le casier de bas en haut en plaçant l'élément le plus lourd dans le bas.
- Si le casier est équipé de dispositifs stabilisateurs, installer les stabilisateurs avant de monter ou de réparer l'unité en casier.

Warnung **Zur Vermeidung von Körperverletzung beim Anbringen oder Warten dieser Einheit in einem Gestell müssen Sie besondere Vorkehrungen treffen, um sicherzustellen, daß das System stabil bleibt. Die folgenden Richtlinien sollen zur Gewährleistung Ihrer Sicherheit dienen:**

- Wenn diese Einheit die einzige im Gestell ist, sollte sie unten im Gestell angebracht werden.
- Bei Anbringung dieser Einheit in einem zum Teil gefüllten Gestell ist das Gestell von unten nach oben zu laden, wobei das schwerste Bauteil unten im Gestell anzubringen ist.
- Wird das Gestell mit Stabilisierungszubehör geliefert, sind zuerst die Stabilisatoren zu installieren, bevor Sie die Einheit im Gestell anbringen oder sie warten.

Avvertenza **Per evitare infortuni fisici durante il montaggio o la manutenzione di questa unità in un supporto, occorre osservare speciali precauzioni per garantire che il sistema rimanga stabile. Le seguenti direttive vengono fornite per garantire la sicurezza personale:**

- Questa unità deve venire montata sul fondo del supporto, se si tratta dell'unica unità da montare nel supporto.
- Quando questa unità viene montata in un supporto parzialmente pieno, caricare il supporto dal basso all'alto, con il componente più pesante sistemato sul fondo del supporto.
- Se il supporto è dotato di dispositivi stabilizzanti, installare tali dispositivi prima di montare o di procedere alla manutenzione dell'unità nel supporto.

Advarsel **Unngå fysiske skader under montering eller reparasjonsarbeid på denne enheten når den befinner seg i et kabinett. Vær nøye med at systemet er stabilt. Følgende retningslinjer er gitt for å verne om sikkerheten:**

- Denne enheten bør monteres nederst i kabinettet hvis dette er den eneste enheten i kabinettet.
- Ved montering av denne enheten i et kabinett som er delvis fylt, skal kabinettet lastes fra bunnen og opp med den tyngste komponenten nederst i kabinettet.
- Hvis kabinettet er utstyrt med stabiliseringsutstyr, skal stabilisatorene installeres før montering eller utføring av reparasjonsarbeid på enheten i kabinettet.

Aviso **Para se prevenir contra danos corporais ao montar ou reparar esta unidade numa estante, deverá tomar precauções especiais para se certificar de que o sistema possui um suporte estável. As seguintes directrizes ajudá-lo-ão a efectuar o seu trabalho com segurança:**

- **Esta unidade deverá ser montada na parte inferior da estante, caso seja esta a única unidade a ser montada.**
- **Ao montar esta unidade numa estante parcialmente ocupada, coloque os itens mais pesados na parte inferior da estante, arrumando-os de baixo para cima.**
- **Se a estante possuir um dispositivo de estabilização, instale-o antes de montar ou reparar a unidade.**

¡Advertencia! **Para evitar lesiones durante el montaje de este equipo sobre un bastidor, o posteriormente durante su mantenimiento, se debe poner mucho cuidado en que el sistema quede bien estable. Para garantizar su seguridad, proceda según las siguientes instrucciones:**

- **Colocar el equipo en la parte inferior del bastidor, cuando sea la única unidad en el mismo.**
- **Cuando este equipo se vaya a instalar en un bastidor parcialmente ocupado, comenzar la instalación desde la parte inferior hacia la superior colocando el equipo más pesado en la parte inferior.**
- **Si el bastidor dispone de dispositivos estabilizadores, instalar éstos antes de montar o proceder al mantenimiento del equipo instalado en el bastidor.**

Varning! **För att undvika kroppsskada när du installerar eller utför underhållsarbete på denna enhet på en ställning måste du vidta särskilda försiktighetsåtgärder för att försäkra dig om att systemet står stadigt. Följande riktlinjer ges för att trygga din säkerhet:**

- **Om denna enhet är den enda enheten på ställningen skall den installeras längst ned på ställningen.**
- **Om denna enhet installeras på en delvis fylld ställning skall ställningen fyllas nedifrån och upp, med de tyngsta enheterna längst ned på ställningen.**
- **Om ställningen är försedd med stabiliseringsdon skall dessa monteras fast innan enheten installeras eller underhålls på ställningen.**

A készülék rackbe történő beszerelése és karbantartása során bekövetkező sérülések elkerülése végett speciális óvintézkedésekkel meg kell őrizni a rendszer stabilitását.
A személyes biztonsága érdekében tartsa be a következő szabályokat:

- **Ha a rackben csak ez az egy készülék található, a rack aljába kell beszerelni.**
- **Ha nincs teljesen tele az a rack, amelybe beszerelik a készüléket, alulról fölfelé haladva töltse fel a racket úgy, hogy a legnehezebb készülék kerüljön a rack aljába.**
- **Ha stabilizáló eszközök is tartoznak a rackhez, szerelje fel a stabilizátorokat, mielőtt beszerelné az egységet a rackbe, vagy karbantartást végezne rajta.**

Предупреждение Во избежание травм при монтаже и обслуживании устройства в стойке следует принять особые меры предосторожности, чтобы убедиться в устойчивости оборудования.
Для обеспечения безопасности работ необходимо соблюдать следующие правила.

- Если в стойке находится одно устройство, оно должно быть установлено в нижней части.
- При монтаже устройств в частично заполненную стойку устанавливайте оборудование снизу вверх, размещая наиболее тяжелые устройства в нижней части.
- Если стойка снабжена приспособлениями для стабилизации, их необходимо установить до начала монтажа или обслуживания оборудования.

警告 为避免在机架中安装或维修该部件时使身体受伤，您必须采取特殊的预防措施确保系统固定。以下是确保安全的原则：

- 如果此部件是机架中唯一的部件，应将其安装在机架的底部。
- 如果在部分装满的机架中安装此部件，请按从下往上的顺序安装各个部件，并且最重的组件应安装在机架的底部。
- 如果机架配有固定装置，请先装好固定装置，然后再在机架中安装或维修部件。

警告 この装置をラックに設置したり保守作業を行ったりするときは、人身事故を防ぐため、システムが安定しているかどうかを十分に確認する必要があります。次の注意事項に従ってください。

- ラックにこの装置を単独で設置する場合は、ラックの一番下に設置します。
- ラックに別の装置がすでに設置されている場合は、最も重量のある装置を一番下にして、重い順に下から上へ設置します。
- ラックに安定器具が付属している場合は、その安定器具を取り付けてから、装置をラックに設置するか、またはラック内の装置の保守作業を行ってください。

주의 이 장치를 랙에 장착하거나 서비스할 때 신체 부상을 방지하려면, 시스템이 안정된 상태를 유지하도록 특별히 주의해야 합니다. 사용자의 안전을 위해 다음 지침 사항을 준수하십시오.

- 이 장치가 랙에 장착되는 유일한 것일 경우, 랙의 맨 아래 부분에 장착되어야 합니다.
- 부분적으로 차 있는 랙에 이 장치를 장착할 경우, 가장 무거운 장치를 랙의 맨 아래 부분부터 차례로 장착하십시오.
- 안정기가 랙과 함께 제공되는 경우, 이 안정기를 설치한 후 이 장치를 랙에 장착하거나 서비스하십시오

Aviso **Para evitar lesões corporais ao montar ou dar manutenção a esta unidade em um rack, é necessário tomar todas as precauções para garantir a estabilidade do sistema. As seguintes orientações são fornecidas para garantir a sua segurança:**

- **Se esta for a única unidade, ela deverá ser montada na parte inferior do rack.**
- **Ao montar esta unidade em um rack parcialmente preenchido, carregue-o de baixo para cima com o componente mais pesado em sua parte inferior.**
- **Se o rack contiver dispositivos estabilizadores, instale-os antes de montar ou dar manutenção à unidade existente.**

Advarsel **For at forhindre legemesbeskadigelse ved montering eller service af denne enhed i et rack, skal du sikre at systemet står stabilt. Følgende retningslinjer er også for din sikkerheds skyld:**

- **Enheden skal monteres i bunden af dit rack, hvis det er den eneste enhed i racket.**
- **Ved montering af denne enhed i et delvist fyldt rack, skal enhederne installeres fra bunden og opad med den tungeste enhed nederst.**
- **Hvis racket leveres med stabiliseringsenheder, skal disse installeres for enheden monteres eller serviceres i racket.**

تحذير **لتجنب حدوث أي إصابات عند تركيب هذه الوحدة، يجب اتباع بعض الاحتياطات لضمان عمل النظام بشكل سليم.**
يتم ذكر الإرشادات التالية لضمان الأمان.
يجب تركيب هذه الوحدة في الجزء السفلي من الدولاب المتضمن قضبان إذا كانت هذه الوحدة هي الوحيدة في الدولاب الذي يحتوي على قضبان.
عند تركيب هذه الوحدة في دولاب شبه ممتلئ، قم برفع الدولاب من الجزء السفلي لأعلى بحيث يكون الجزء الأثقل وزناً أسفل الدولاب.
إذا كان الدولاب المتضمن قضباناً يحتوي على أجهزة حفظ التوازن، قم بتثبيت هذه الأجهزة قبل تركيب الوحدة في الدولاب.

Upozorenje

Kako ne bi došlo do tjelesnih ozljeda kod postavljanja ili servisiranja uređaja na polici, potrebno je poduzeti mjere predostrožnosti kako bi sustav uvijek bio stabilan. Sigurnost se može osigurati poštivanjem sljedećih smjernica:

- **Ovaj uređaj treba ugraditi na dno police, ukoliko je to jedini uređaj na polici.**
- **Kod ugradnje uređaja u policu na kojoj se već nalaze drugi uređaji, policu treba opremati počevši od dna, te tako da se na dno stave najteži dijelovi.**
- **Ukoliko su na polici ugrađeni stabilizatori, njih montirajte prije ugradnje ili servisiranja uređaja na polici.**

Upozornění

Abyste předešli poranění osob při montáži nebo opravě zařízení v montážním rámu, musíte dodržovat zvláštní preventivní opatření pro zajištění udržení stability systému. Pro zajištění bezpečnosti obsluhy jsou určeny následující zásady:

- **Pokud je toto zařízení jedinou jednotkou v montážním rámu, musí být namontováno na nejnižší místo rámu.**
- **Pokud je toto zařízení montováno do částečně obsazeného montážního rámu, obsazujte montážní rám ve směru zdola nahoru tak, aby byla nejtěžší součást nejníže.**
- **Pokud je montážní rám vybaven stabilizačními zařízeními, nainstalujte stabilizátory ještě před montáží nebo opravou zařízení v montážním rámu.**

Προειδοποίηση

Για να αποφύγετε τον τραυματισμό κατά την τοποθέτηση ή τη συντήρηση αυτής της συσκευής σε αρθρωτό σύστημα, πρέπει να λάβετε ειδικές προφυλάξεις για να διασφαλίσετε τη σταθερότητα του συστήματος. Οι παρακάτω οδηγίες παρέχονται για να εξασφαλίσουν την ασφάλειά σας:

- Αυτή η συσκευή πρέπει να τοποθετείται στο κάτω μέρος του αρθρωτού συστήματος αν είναι η μοναδική συσκευή σε αυτό.
- Όταν τοποθετείτε αυτήν τη συσκευή σε εν μέρει γεμάτο αρθρωτό σύστημα, τοποθετήστε συσκευές στο αρθρωτό σύστημα από κάτω προς τα επάνω, με τη βαρύτερη συσκευή στο κάτω μέρος του συστήματος.
- Εάν το αρθρωτό σύστημα διαθέτει διατάξεις σταθεροποίησης, τοποθετήστε τους σταθεροποιητές πριν τοποθετήσετε ή συντηρήσετε τη συσκευή στο αρθρωτό σύστημα.

אזהרה

כדי למנוע פציעה בעת הרכבת יחידה זו במעמד או טיפול בה, עליך לנקוט אמצעי זהירות מיוחדים כדי להבטיח את יציבות המערכת. הקווים המנחים הבאים ניתנים על מנת להבטיח את ביטחונך:

- אם יחידה זו היא יחידה בודדת במעמד, יש להרכיב את היחידה בחלקו התחתון של המעמד.
- בעת הרכבת יחידה זו במעמד המלא בחלקו, טען את המעמד החל בחלק התחתון וכלפי מעלה כאשר הרכיב הכבד ביותר נמצא בחלקו התחתון של המעמד.
- אם המעמד מסופק עם התקני ייצוב, התקן את המייצבים לפני הרכבה היחידה במעמד או טיפול בה.

Opomena

За да се не повредите кога го монтирате или го сервисирате уредот на полица, мора да бидете особено претпазливи за да ја обезбедите стабилноста на системот. Следите напатствија се дадени за да ја осигурaат Вашата безбедност:

- Уредот треба да се монтира најдолу на полицата ако е единствен уред на полицата.
- Кога го монтирате уредот на делумно пополнета полица, полнете ја полицата од дното кон врвот со најтешката компонента на дното на полицата.
- Ако полицата има стабилизаторски делови, наместете ги стабилизаторите пред да го монтирате или сервисирате уредот на полицата.

Ostrzeżenie **Aby zapobiec urazom podczas montażu lub serwisowania tego urządzenia w stojaku, należy zastosować szczególne środki ostrożności w celu zapewnienia stabilności układu. Poniżej przedstawiono wskazówki, których przestrzeganie zapewni bezpieczeństwo:**

- **Jeśli urządzenie to jest jedynym urządzeniem w stojaku, powinno być zamontowane na dole.**
- **W przypadku montażu urządzenia w częściowo zapełnionym stojaku należy instalować kolejne urządzenia od najniższego do najwyższego, przy czym element najcięższy powinien być zamontowany najniżej w stojaku.**
- **Jeśli stojak jest wyposażony w elementy stabilizujące, należy zamontować stabilizatory przed przystąpieniem do montażu lub serwisowania urządzeń w stojaku.**

Upozornenie **Aby ste predišli poraneniu osôb pri montáži alebo oprave zariadenia v montážnom ráme, musíte dodržiavať zvláštne preventívne opatrenia na zaistenie udržania stability systému. Na zaistenie bezpečnosti obsluhy sú určené nasledujúce zásady:**

- **Pokiaľ je toto zariadenie jedinou jednotkou v montážnom ráme, musí byť namontované na najnižšie miesto v ráme.**
- **Pokiaľ je toto zariadenie montované do čiastočne obsadeného montážneho rámu, obsadzujte montážny rám v smere zdola nahor tak, aby bola najťažšia súčasť najnižšie.**
- **Pokiaľ je montážny rám vybavený stabilizačnými zariadeniami, nainštalujte stabilizátory ešte pred montážou alebo opravou zariadenia v montážnom ráme.**

A készülék rackbe történő beszerelése és karbantartása során bekövetkező sérülések elkerülése végett speciális óvintézkedésekkel meg kell őrizni a rendszer stabilitását. A személyes biztonsága érdekében tartsa be a következő szabályokat:

- **Ha a rackben csak ez az egy készülék található, a rack aljába kell beszerelni.**
- **Ha nincs teljesen tele az a rack, amelybe beszerelik a készüléket, alulról fölfelé haladva töltse fel a racket úgy, hogy a legnehezebb készülék kerüljön a rack aljába.**
- **Ha stabilizáló eszközök is tartoznak a rackhez, szerelje fel a stabilizátorokat, mielőtt beszerelné az egységet a rackbe, vagy karbantartást végezne rajta.**

Предупреждение Во избежание травм при монтаже и обслуживании устройства в стойке следует принять особые меры предосторожности, чтобы убедиться в устойчивости оборудования. Для обеспечения безопасности работ необходимо соблюдать следующие правила.

- Если в стойке находится одно устройство, оно должно быть установлено в нижней части.
- При монтаже устройств в частично заполненную стойку устанавливайте оборудование снизу вверх, размещая наиболее тяжелые устройства в нижней части.
- Если стойка снабжена приспособлениями для стабилизации, их необходимо установить до начала монтажа или обслуживания оборудования.

警告 为避免在机架中安装或维修该部件时使身体受伤，您必须采取特殊的预防措施确保系统固定。以下是确保安全的原则：

- 如果此部件是机架中唯一的部件，应将其安装在机架的底部。
- 如果在部分装满的机架中安装此部件，请按从下往上的顺序安装各个部件，并且最重的组件应安装在机架的底部。
- 如果机架配有固定装置，请先装好固定装置，然后再在机架中安装或维修部件。

警告 この装置をラックに設置したり保守作業を行ったりするときは、人身事故を防ぐため、システムが安定しているかどうかを十分に確認する必要があります。次の注意事項に従ってください。

- ラックにこの装置を単独で設置する場合は、ラックの一番下に設置します。
- ラックに別の装置がすでに設置されている場合は、最も重量のある装置を一番下にして、重い順に下から上へ設置します。
- ラックに安定器具が付属している場合は、その安定器具を取り付けてから、装置をラックに設置するか、またはラック内の装置の保守作業を行ってください。

주의

이 장치를 랙에 장착하거나 서비스할 때 신체 부상을 방지하려면, 시스템이 안정된 상태를 유지하도록 특별히 주의해야 합니다. 사용자의 안전을 위해 다음 지침 사항을 준수하십시오.

- 이 장치가 랙에 장착되는 유일한 것일 경우, 랙의 맨 아래 부분에 장착되어야 합니다.
- 부분적으로 차 있는 랙에 이 장치를 장착할 경우, 가장 무거운 장치를 랙의 맨 아래 부분부터 차례로 장착하십시오.
- 안정기가 랙과 함께 제공되는 경우, 이 안정기를 설치한 후 이 장치를 랙에 장착하거나 서비스하십시오

تحذير

لتجنب حدوث أي إصابات عند تركيب هذه الوحدة، يجب اتباع بعض الاحتياطات لضمان عمل النظام بشكل سليم. يتم ذكر الإرشادات التالية لضمان الأمان.

يجب تركيب هذه الوحدة في الجزء السفلي من الدولاب المتضمن قضبان إذا كانت هذه الوحدة هي الوحدة الوحيدة في الدولاب الذي يحتوي على قضبان.

عند تركيب هذه الوحدة في دولاب شبه ممتلئ، قم برفع الدولاب من الجزء السفلي لأعلى بحيث يكون الجزء الأثقل وزناً أسفل الدولاب.

إذا كان الدولاب المتضمن قضباناً يحتوي على أجهزة حفظ التوازن، قم بتثبيت هذه الأجهزة قبل تركيب الوحدة في الدولاب.

Upozorenje

Kako ne bi došlo do tjelesnih ozljeda kod postavljanja ili servisiranja uređaja na polici, potrebno je poduzeti mjere predostrožnosti kako bi sustav uvijek bio stabilan. Sigurnost se može osigurati poštivanjem sljedećih smjernica:

- **Ovaj uređaj treba ugraditi na dno police, ukoliko je to jedini uređaj na polici.**
- **Kod ugradnje uređaja u policu na kojoj se već nalaze drugi uređaji, policu treba opremati počevši od dna, te tako da se na dno stave najteži dijelovi.**
- **Ukoliko su na polici ugrađeni stabilizatori, njih montirajte prije ugradnje ili servisiranja uređaja na polici.**

Upozornění

Abyste předešli poranění osob při montáži nebo opravě zařízení v montážním rámu, musíte dodržovat zvláštní preventivní opatření pro zajištění udržení stability systému. Pro zajištění bezpečnosti obsluhy jsou určeny následující zásady:

- **Pokud je toto zařízení jedinou jednotkou v montážním rámu, musí být namontováno na nejnižší místo rámu.**
- **Pokud je toto zařízení montováno do částečně obsazeného montážního rámu, obsazujte montážní rám ve směru zdola nahoru tak, aby byla nejtěžší součást nejníže.**
- **Pokud je montážní rám vybaven stabilizačními zařízeními, nainstalujte stabilizátory ještě před montáží nebo opravou zařízení v montážním rámu.**

Προειδοποίηση

Για να αποφύγετε τον τραυματισμό κατά την τοποθέτηση ή τη συντήρηση αυτής της συσκευής σε αρθρωτό σύστημα, πρέπει να λάβετε ειδικές προφυλάξεις για να διασφαλίσετε τη σταθερότητα του συστήματος. Οι παρακάτω οδηγίες παρέχονται για να εξασφαλίσουν την ασφάλειά σας:

- Αυτή η συσκευή πρέπει να τοποθετείται στο κάτω μέρος του αρθρωτού συστήματος αν είναι η μοναδική συσκευή σε αυτό.
- Όταν τοποθετείτε αυτήν τη συσκευή σε εν μέρει γεμάτο αρθρωτό σύστημα, τοποθετήστε συσκευές στο αρθρωτό σύστημα από κάτω προς τα επάνω, με τη βαρύτερη συσκευή στο κάτω μέρος του συστήματος.
- Εάν το αρθρωτό σύστημα διαθέτει διατάξεις σταθεροποίησης, τοποθετήστε τους σταθεροποιητές πριν τοποθετήσετε ή συντηρήσετε τη συσκευή στο αρθρωτό σύστημα.

אזהרה

כדי למנוע פציעה בעת הרכבת יחידה זו במעמד או טיפול בה, עליך לנקוט אמצעי זהירות מיוחדים כדי להבטיח את יציבות המערכת. הקווים המנחים הבאים ניתנים על מנת להבטיח את ביטחונך:

- אם יחידה זו היא יחידה בודדת במעמד, יש להרכיב את היחידה בחלקו התחתון של המעמד.
- בעת הרכבת יחידה זו במעמד המלא בחלקו, טען את המעמד החל בחלק התחתון וכלפי מעלה כאשר הרכיב הכבד ביותר נמצא בחלקו התחתון של המעמד.
- אם המעמד מסופק עם התקני ייצוב, התקן את המייצבים לפני הרכבה היחידה במעמד או טיפול בה.

Opomena

За да се не повредите кога го монтирате или го сервисирате уредот на полица, мора да бидете особено претпазливи за да ја обезбедите стабилноста на системот. Следите напатствија се дадени за да ја осигураат Вашата безбедност:

- Уредот треба да се монтира најдолу на полицата ако е единствен уред на полицата.
- Кога го монтирате уредот на делумно пополнета полица, полнете ја полицата од дното кон врвот со најтешката компонента на дното на полицата.
- Ако полицата има стабилизаторски делови, наместете ги стабилизаторите пред да го монтирате или сервисирате уредот на полицата.

Ostrzeżenie **Aby zapobiec urazom podczas montażu lub serwisowania tego urządzenia w stojaku, należy zastosować szczególne środki ostrożności w celu zapewnienia stabilności układu. Poniżej przedstawiono wskazówki, których przestrzeganie zapewni bezpieczeństwo:**

- **Jeśli urządzenie to jest jedynym urządzeniem w stojaku, powinno być zamontowane na dole.**
- **W przypadku montażu urządzenia w częściowo zapełnionym stojaku należy instalować kolejne urządzenia od najniższego do najwyższego, przy czym element najcięższy powinien być zamontowany najniżej w stojaku.**
- **Jeśli stojak jest wyposażony w elementy stabilizujące, należy zamontować stabilizatory przed przystąpieniem do montażu lub serwisowania urządzeń w stojaku.**

Upozornenie **Aby ste predišli poraneniu osôb pri montáži alebo oprave zariadenia v montážnom ráme, musíte dodržiavať zvláštne preventívne opatrenia na zaistenie udržania stability systému. Na zaistenie bezpečnosti obsluhy sú určené nasledujúce zásady:**

- **Pokiaľ je toto zariadenie jedinou jednotkou v montážnom ráme, musí byť namontované na najnižšie miesto v ráme.**
- **Pokiaľ je toto zariadenie montované do čiastočne obsadeného montážneho rámu, obsadzujte montážny rám v smere zdola nahor tak, aby bola najťažšia súčasť najnižšie.**
- **Pokiaľ je montážny rám vybavený stabilizačnými zariadeniami, nainštalujte stabilizátory ešte pred montážou alebo opravou zariadenia v montážnom ráme.**

Battery Handling Warning for 4400 Series Controllers

Warning **There is the danger of explosion if the Cisco 4400 Series Wireless LAN Controller battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.** Statement 1015

Waarschuwing **Er is ontploffingsgevaar als de batterij verkeerd vervangen wordt. Vervang de batterij slechts met hetzelfde of een equivalent type dat door de fabrikant aanbevolen is. Gebruikte batterijen dienen overeenkomstig fabrieksvoorschriften weggeworpen te worden.**

Varoitus **Räjähdyksen vaara, jos akku on vaihdettu väärään akkuun. Käytä vaihtamiseen ainoastaan saman- tai vastaavantyyppistä akkua, joka on valmistajan suosittelema. Hävitä käytetyt akut valmistajan ohjeiden mukaan.**

Attention **Danger d'explosion si la pile n'est pas remplacée correctement. Ne la remplacer que par une pile de type semblable ou équivalent, recommandée par le fabricant. Jeter les piles usagées conformément aux instructions du fabricant.**

Warnung **Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.**

Avvertenza **Pericolo di esplosione se la batteria non è installata correttamente. Sostituire solo con una di tipo uguale o equivalente, consigliata dal produttore. Eliminare le batterie usate secondo le istruzioni del produttore.**

Advarsel **Det kan være fare for eksplosjon hvis batteriet skiftes på feil måte. Skift kun med samme eller tilsvarende type som er anbefalt av produsenten. Kasser brukte batterier i henhold til produsentens instruksjoner.**

Aviso **Existe perigo de explosão se a bateria for substituída incorrectamente. Substitua a bateria por uma bateria igual ou de um tipo equivalente recomendado pelo fabricante. Destrua as baterias usadas conforme as instruções do fabricante.**

¡Advertencia! **Existe peligro de explosión si la batería se reemplaza de manera incorrecta. Reemplazar la batería exclusivamente con el mismo tipo o el equivalente recomendado por el fabricante. Desechar las baterías gastadas según las instrucciones del fabricante.**

Varning! **Explosionsfara vid felaktigt batteribyte. Ersätt endast batteriet med samma batterityp som rekommenderas av tillverkaren eller motsvarande. Följ tillverkarens anvisningar vid kassering av använda batterier.**

Robbanásveszélyt idézhet elő, ha helytelenül cserélik ki az akkumulátort. Csak a gyártó által javasolttal megegyező vagy azzal egyenértékű típusúra cserélje ki az akkumulátort! A használt akkumulátorok kidobásakor tartsa be a gyártó előírásait!

Предупреждение При неправильной замене батареи возможен взрыв. Для замены следует использовать батарею того же или аналогичного типа, рекомендованного изготовителем. Утилизацию батареи необходимо производить в соответствии с указаниями изготовителя.

警告 电池更换不当会有爆炸危险。请只用同类电池或制造商推荐的功能相当的电池更换原有电池。请按制造商的说明处理废旧电池。

警告 不適切なバッテリに交換すると、爆発の危険性があります。製造元が推奨するものと同じまたは同等のバッテリだけを使用してください。使用済みのバッテリは、製造元が指示する方法に従って処分してください。

Robbanásveszélyt idézhet elő, ha helytelenül cserélik ki az akkumulátort. Csak a gyártó által javasolttal megegyező vagy azzal egyenértékű típusúra cserélje ki az akkumulátort! A használt akkumulátorok kidobásakor tartsa be a gyártó előírásait!

Предупреждение При неправильной замене батареи возможен взрыв. Для замены следует использовать батарею того же или аналогичного типа, рекомендованного изготовителем. Утилизацию батареи необходимо производить в соответствии с указаниями изготовителя.

警告 电池更换不当会有爆炸危险。请只用同类电池或制造商推荐的功能相当的电池更换原有电池。请按制造商的说明处理废旧电池。

警告 不適切なバッテリに交換すると、爆発の危険性があります。製造元が推奨するものと同じまたは同等のバッテリだけを使用してください。使用済みのバッテリは、製造元が指示する方法に従って処分してください。

Equipment Installation Warning

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

Waarschuwing **Deze apparatuur mag alleen worden geïnstalleerd, vervangen of hersteld door bevoegd geschoold personeel.**

Varoitus **Tämän laitteen saa asentaa, vaihtaa tai huoltaa ainoastaan koulutettu ja laitteen tunteva henkilökunta.**

Attention **Il est vivement recommandé de confier l'installation, le remplacement et la maintenance de ces équipements à des personnels qualifiés et expérimentés.**

Warnung **Das Installieren, Ersetzen oder Bedienen dieser Ausrüstung sollte nur geschultem, qualifiziertem Personal gestattet werden.**

Avvertenza **Questo apparato può essere installato, sostituito o mantenuto unicamente da un personale competente.**

Advarsel **Bare opplært og kvalifisert personell skal foreta installasjoner, utskiftninger eller service på dette utstyret.**

Aviso **Apenas pessoal treinado e qualificado deve ser autorizado a instalar, substituir ou fazer a revisão deste equipamento.**

¡Advertencia! **Solamente el personal calificado debe instalar, reemplazar o utilizar este equipo.**

Varning! **Endast utbildad och kvalificerad personal bör få tillåtelse att installera, byta ut eller reparera denna utrustning.**

A berendezést csak szakképzett személyek helyezhetik üzembe, cserélhetik és tarthatják karban.

Предупреждение Установку, замену и обслуживание этого оборудования может осуществлять только специально обученный квалифицированный персонал.

警告 只有经过培训且具有资格的人员才能进行此设备的安装、更换和维修。

警告 この装置の設置、交換、保守は、訓練を受けた相応の資格のある人が行ってください。

주의 교육을 받고 자격을 갖춘 사람만 이 장비를 설치, 교체, 또는 서비스를 수행해야 합니다.

Aviso **Somente uma equipe treinada e qualificada tem permissão para instalar, substituir ou dar manutenção a este equipamento.**

Advarsel **Kun uddannede personer må installere, udskifte komponenter i eller servicere dette udstyr.**

تحذير يسمح للفنيين المتخصصين فقط بتركيب المعدة أو استبدالها أو إجراء الصيانة عليها.

Upozorenje **Uređaj smije ugrađivati, mijenjati i servisirati samo za to obučeno i osposobljeno servisno osoblje.**

Upozornění **Instalaci, výměnu nebo opravu tohoto zařízení smějí provádět pouze proškolené a kvalifikované osoby.**

Προειδοποίηση Η τοποθέτηση, η αντικατάσταση και η συντήρηση του εξοπλισμού επιτρέπεται να γίνονται μόνο από καταρτισμένο προσωπικό με τα κατάλληλα προσόντα.

אזהרה רק עובדים מיומנים ומוסמכים רשאים להתקין, להחליף, או לטפל בציד זה.

Opomena Местењето, заменувањето и сервисирањето на оваа опрема треба да му биде дозволено само на обучен и квалификуван персонал.

Ostrzeżenie **Do instalacji, wymiany i serwisowania tych urządzeń mogą być dopuszczone wyłącznie osoby wykwalifikowane i przeszkolone.**

Upozornenie **Inštaláciu, výmenu alebo opravu tohto zariadenia smú vykonávať iba vyškolené a kvalifikované osoby.**

A berendezést csak szakképzett személyek helyezhetik üzembe, cserélhetik és tarthatják karban.

Предупреждение Установку, замену и обслуживание этого оборудования может осуществлять только специально обученный квалифицированный персонал.

警告 只有经过培训且具有资格的人员才能进行此设备的安装、更换和维修。

警告 この装置の設置、交換、保守は、訓練を受けた相応の資格のある人が行ってください。

주의 교육을 받고 자격을 갖춘 사람만 이 장비를 설치, 교체, 또는 서비스를 수행해야 합니다.

تحذير **يسمح للفنيين المتخصصين فقط بتركيب المعدة أو استبدالها أو إجراء الصيانة عليها.**

Upozorenje **Uređaj smije ugrađivati, mijenjati i servisirati samo za to obučeno i osposobljeno servisno osoblje.**

Upozornění **Instalaci, výměnu nebo opravu tohoto zařízení smějí provádět pouze proškolené a kvalifikované osoby.**

Προειδοποίηση Η τοποθέτηση, η αντικατάσταση και η συντήρηση του εξοπλισμού επιτρέπεται να γίνονται μόνο από καταρτισμένο προσωπικό με τα κατάλληλα προσόντα.

אזהרה רק עובדים מיומנים ומוסמכים רשאים להתקין, להחליף, או
לטפל בציוד זה.

Opomena Местењето, заменувањето и сервисирањето на оваа опрема треба да му биде дозволено само на обучен и квалификуван персонал.

Ostrzeżenie **Do instalacji, wymiany i serwisowania tych urządzeń mogą być dopuszczone wyłącznie osoby wykwalifikowane i przeszkolone.**

Upozornenie **Inštaláciu, výmenu alebo opravu tohto zariadenia smú vykonávať iba vyškolené a kvalifikované osoby.**

More Than One Power Supply Warning for 4400 Series Controllers

Warning **The Cisco 4400 Series Wireless LAN Controller might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028

Waarschuwing **Deze eenheid kan meer dan één stroomtoevoeraansluiting bevatten. Alle aansluitingen dienen ontkoppeld te worden om de eenheid te ontkrachten.**

Varoitus **Tässä laitteessa voi olla useampia kuin yksi virtakytkentä. Kaikki liitännät on irrotettava, jotta jännite poistetaan laitteesta.**

Attention **Cette unité peut avoir plus d'une connexion d'alimentation. Pour supprimer toute tension et tout courant électrique de l'unité, toutes les connexions d'alimentation doivent être débranchées.**

Warnung **Dieses Gerät kann mehr als eine Stromzufuhr haben. Um sicherzustellen, dass der Einheit kein Strom zugeführt wird, müssen alle Verbindungen entfernt werden.**

Avvertenza **Questa unità può avere più di una connessione all'alimentazione elettrica. Tutte le connessioni devono essere staccate per togliere la corrente dall'unità.**

Advarsel **Denne enheten kan ha mer enn én strømtilførselskobling. Alle koblinger må fjernes fra enheten for å utkoble all strøm.**

Aviso **Esta unidade poderá ter mais de uma conexão de fonte de energia. Todas as conexões devem ser removidas para desligar a unidade.**

¡Advertencia! **Puede que esta unidad tenga más de una conexión para fuentes de alimentación. Para cortar por completo el suministro de energía, deben desconectarse todas las conexiones.**

Varning! **Denna enhet har eventuellt mer än en strömförsörjningsanslutning. Alla anslutningar måste tas bort för att göra enheten strömlös.**

Előfordulhat, hogy a készülék többszörösen van csatlakoztatva az áramforráshoz. A készülék áramtalanításához mindegyik csatlakozást meg kell szüntetni.

Предупреждение В данном устройстве может использоваться несколько подключений к электросети. Чтобы обесточить устройство, необходимо отключить все эти подключения.

警告 此部件连接的电源可能不止一个。必须将所有电源断开才能停止给该部件供电。

警告 この装置には、複数の電源が接続されている場合があります。装置の電源を完全にオフにするには、すべての電源を切断する必要があります。

주의 본 장치에는 2개 이상의 전원 공급 연결 단자가 있을 수 있습니다. 이 장치의 전원을 차단하려면 모든 연결 단자를 제거해야 합니다.

Aviso **Esta unidade pode ter mais de uma conexão de fonte de alimentação. Todas as conexões devem ser removidas para interromper a alimentação da unidade.**

Advarsel **Denne enhed har muligvis mere end en strømforsyningstilslutning. Alle tilslutninger skal fjernes for at aflade strømmen fra enheden.**

تحذير **قد تتضمن هذه الوحدة أكثر من اتصال بمورد الطاقة. يجب فصل كافة التوصيلات حتى يمكن إفراغ طاقة الوحدة.**

Upozorenje **Uređaj može imati više priključaka za izvore napajanja. Za potpuno isključivanje napajanja potrebno je iskopčati sve priključke.**

Upozornění **Toto zařízení může být připojeno k více než jednomu zdroji napájení. Aby se zařízení zcela odpojilo od proudu, musí být odpojeno od všech zdrojů napájení.**

Προειδοποίηση Αυτή η συσκευή ίσως να έχει περισσότερες συνδέσεις τροφοδοσίας.
Για να απενεργοποιηθεί η συσκευή, πρέπει να αφαιρεθούν όλες οι συνδέσεις.

אזהרה ייתכן שביחידה זו קיים יותר מחיבור אחד לספק כוח. יש להסיר את כל החיבורים כדי להפסיק את אספקת המתח ליחידה.

Opomena Уредот може да има повеќе од еден приклучок за напојување. Сите приклучоци мора да се извадат за да се прекине доводот на енергија во уредот.

Ostrzeżenie **To urządzenie może mieć podłączone więcej niż jedno źródło zasilania. Aby całkowicie odciąć dopływ energii do urządzenia, należy odłączyć wszystkie źródła zasilania.**

Upozornenie **Toto zariadenie môže byť pripojené k viac ako jednému zdroju napájania. Aby sa zariadenie odpojilo od prúdu, musí byť odpojené od všetkých zdrojov.**

Előfordulhat, hogy a készülék többszörösen van csatlakoztatva az áramforráshoz. A készülék áramtalanításához mindegyik csatlakozást meg kell szüntetni.

Предупреждение В данном устройстве может использоваться несколько подключений к электросети. Чтобы обесточить устройство, необходимо отключить все эти подключения.

警告 此部件连接的电源可能不止一个。必须将所有电源断开才能停止给该部件供电。

警告 この装置には、複数の電源が接続されている場合があります。装置の電源を完全にオフにするには、すべての電源を切断する必要があります。

주의 본 장치에는 2개 이상의 전원 공급 연결 단자가 있을 수 있습니다. 이 장치의 전원을 차단하려면 모든 연결 단자를 제거해야 합니다.

تحذير **قد تتضمن هذه الوحدة أكثر من اتصال بمورد الطاقة. يجب فصل كافة التوصيلات حتى يمكن إفراغ طاقة الوحدة.**

Upozorenje **Uređaj može imati više priključaka za izvore napajanja. Za potpuno isključivanje napajanja potrebno je iskopčati sve priključke.**

Upozornění **Toto zařízení může být připojeno k více než jednomu zdroji napájení. Aby se zařízení zcela odpojilo od proudu, musí být odpojeno od všech zdrojů napájení.**

Προειδοποίηση Αυτή η συσκευή ίσως να έχει περισσότερες συνδέσεις τροφοδοσίας.
Για να απενεργοποιηθεί η συσκευή, πρέπει να αφαιρεθούν όλες οι συνδέσεις.

אזהרה ייתכן שביחידה זו קיים יותר מחיבור אחד לספק כוח. יש להסיר את כל החיבורים כדי להפסיק את אספקת המתח ליחידה.

Opomena Уредот може да има повеќе од еден приклучок за напојување. Сите приклучоци мора да се извадат за да се прекине доводот на енергија во уредот.

Ostrzeżenie **To urządzenie może mieć podłączone więcej niż jedno źródło zasilania. Aby całkowicie odciąć dopływ energii do urządzenia, należy odłączyć wszystkie źródła zasilania.**

Upozornenie **Toto zariadenie môže byť pripojené k viac ako jednému zdroju napájania. Aby sa zariadenie odpojilo od prúdu, musí byť odpojené od všetkých zdrojov.**

APPENDIX B

Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for the products in the Cisco UWN Solution.

This appendix contains these sections:

- Regulatory Information for Lightweight Access Points, page B-2
- FCC Statement for Cisco 2100 Series Wireless LAN Controllers, page B-10
- FCC Statement for 4400 Series Wireless LAN Controllers, page B-10

Regulatory Information for Lightweight Access Points

This section contains regulatory information for lightweight access points. The information is in these sections:

- Manufacturers Federal Communication Commission Declaration of Conformity Statement, page B-2
- Department of Communications—Canada, page B-3
- European Community, Switzerland, Norway, Iceland, and Liechtenstein, page B-4
- Declaration of Conformity for RF Exposure, page B-5
- Guidelines for Operating Controllers and Access Points in Japan, page B-7
- Administrative Rules for Cisco Aironet Access Points in Taiwan, page B-8
- Declaration of Conformity Statements, page B-10

Manufacturers Federal Communication Commission Declaration of Conformity Statement

Tested To Comply
With FCC Standards

FOR HOME OR OFFICE USE

Model:

AIR-AP1010-A-K9, AIR-AP1020-A-K9, AIR-AP1030-A-K9

FCC Certification number:

LDK102057

Manufacturer:

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

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

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

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

- Reorient or relocate the receiving antenna.
- Increase separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician.

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

Caution Within the 5.15-to-5.25-GHz band (5-GHz radio channels 34 to 48) the U-NII devices are restricted to indoor operations to reduce any potential for harmful interference to co-channel Mobile Satellite System (MSS) operations.

Department of Communications—Canada

Model:

AIR-AP1010-A-K9, AIR-AP1020-A-K9, AIR-AP1030-A-K9

Certification number:

2461B-102057

Canadian Compliance Statement

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

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

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

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Cisco Aironet 2.4-GHz Access Points are certified to the requirements of RSS-210 for 2.4-GHz spread spectrum devices, and Cisco Aironet 54-Mbps, 5-GHz Access Points are certified to the requirements of RSS-210 for 5-GHz spread spectrum devices.The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Model:

AIR-AP1010-E-K9, AIR-AP1020-E-K9, AIR-AP1030-E-K9

Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC

English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Deutsch:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprecheneden Vorgaben der Richtlinie 1999/5/EU.
Dansk:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Directiv 1999/5/EF.
Español:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directive 1999/5/EC.
Έλληνας:	Αυτός ο εξοπλισμός συμμορφώνεται με τις ουσιώδεις απαιτήσεις και τις λοιπές διατάξεις της Οδηγίας 1999/5/EK.
Français:	Cet appareil est conforme aux exigencies essentialles et aux autres dispositions pertinantes de la Directive 1999/5/EC.
Íslenska:	Þessi búnaður samrýmist lögboðnum kröfum og öðrum ákvæðum tilskipunar 1999/5/ESB.
Italiano:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/EC.
Nederlands:	Deze apparatuur voldoet aan de belangrijkste eisen en andere voorzieningen van richtlijn 1999/5/EC.
Norsk:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-directiv 1999/5/EC.
Português:	Este equipamento satisfaz os requisitos essenciais e outras provisões da Directiva 1999/5/EC.
Suomalainen:	Tämä laite täyttää direktiivin 1999/5/EY oleelliset vaatimukset ja on siinä asetettujen muidenkin ehtojen mukainen.
Svenska:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

For 2.4-GHz radios, the following standards were applied:

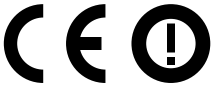
• Radio:	EN 300.328-1, EN 300.328-2
• EMC:	EN 301.489-1, EN 301.489-17
• Safety:	EN 60950

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

For 54-Mbps, 5-GHz access points, the following standards were applied:

- Radio: EN 301.893
- EMC: EN 301.489-1, EN 301.489-17
- Safety: EN 60950

The following CE mark is affixed to the access point with a 2.4-GHz radio and a 54-Mbps, 5-GHz radio:



Declaration of Conformity for RF Exposure

The radio has been found to be compliant to the requirements set forth in CFR 47 Sections 2.1091, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices as defined in Evaluating Compliance with FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields. The equipment should be installed more than 20 cm (7.9 in.) from your body or nearby persons.

The access point must be installed to maintain a minimum 20 cm (7.9 in.) co-located separation distance from other FCC approved indoor/outdoor antennas used with the access point. Any antennas or transmitters not approved by the FCC cannot be co-located with the access point. The access point's co-located 2.4-GHz and 5-GHz integrated antennas support a minimum separation distance of 8 cm (3.2 in.) and are compliant with the applicable FCC RF exposure limit when transmitting simultaneously.

Note Dual antennas used for diversity operation are not considered co-located.

Guidelines for Operating Controllers in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet 4400 and 2100 series controllers in Japan. These guidelines are provided in both Japanese and English.

VCCI Class A Warning for 4400 Series Controllers in Japan

Warning **This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.**

警告 VCCI 準拠クラスA機器（日本）

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI Class B Warning for 2100 Series Controllers in Japan

Warning **This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.**

警告 VCCI 準拠クラスB機器（日本）

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

Power Cable and AC Adapter Warning for Japan

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

警告

Guidelines for Operating Controllers and Access Points in Japan

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

Japanese Translation

English Translation

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

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.
2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.
3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

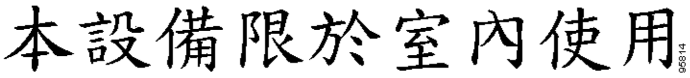
   Contact Number: 03-5549-6500

Administrative Rules for Cisco Aironet Access Points in Taiwan

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

Access Points with IEEE 802.11a Radios

Chinese Translation



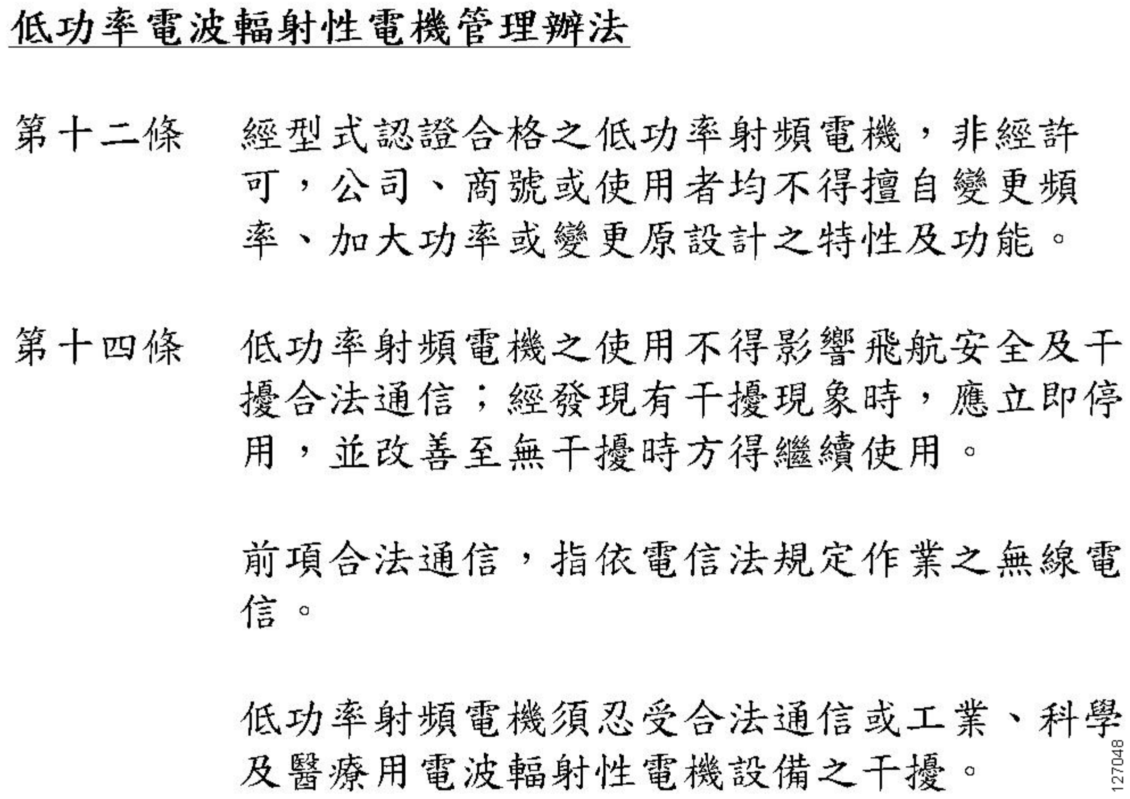
本設備限於室內使用

English Translation

This equipment is limited for indoor use.

All Access Points

Chinese Translation



低功率電波輻射性電機管理辦法

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

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

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

127048

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 12

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

Article 14

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

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

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

Declaration of Conformity Statements

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

http://www.ciscofax.com

FCC Statement for Cisco 2100 Series Wireless LAN Controllers

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help. [cfr reference 15.105]

FCC Statement for 4400 Series Wireless LAN Controllers

The Cisco 4400 Series Wireless LAN Controller equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

APPENDIX C

End User License and Warranty

This appendix describes the end user license and warranty that apply to the Cisco UWN Solution products:

- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco Wireless Services Modules

This appendix contains these sections:

- End User License Agreement, page C-2
- Limited Warranty, page C-4
- General Terms Applicable to the Limited Warranty Statement and End User License Agreement, page C-6
- Notices, page C-6

End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, “CUSTOMER”) TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

The following terms of this End User License Agreement (“Agreement”) govern Customer’s access and use of the Software, except to the extent (a) there is a separate signed agreement between Customer and Cisco governing Customer’s use of the Software or (b) the Software includes a separate “click-accept” license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the signed agreement, (2) the click-accept agreement, and (3) this End User License Agreement.

License. Conditioned upon compliance with the terms and conditions of this Agreement, Cisco Systems, Inc. or its subsidiary licensing the Software instead of Cisco Systems, Inc. (“Cisco”), grants to Customer a nonexclusive and nontransferable license to use for Customer’s internal business purposes the Software and the Documentation for which Customer has paid the required license fees. “Documentation” means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) specifically pertaining to the Software and made available by Cisco with the Software in any manner (including on CD-ROM, or on-line).

Customer’s license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or that number of agent(s), concurrent users, sessions, IP addresses, port(s), seat(s), server(s) or site(s), as set forth in the applicable Purchase Order which has been accepted by Cisco and for which Customer has paid to Cisco the required license fee.

Unless otherwise expressly provided in the Documentation, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer and used for Customer’s internal business purposes. NOTE: For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Cisco retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Cisco, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Accordingly, except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

(i) transfer, assign or sublicense its license rights to any other person or entity, or use the Software on unauthorized or secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;

(ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

(iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction;

(iv) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Cisco; or

(v) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Cisco. Customer shall implement reasonable security measures to protect such trade secrets; or

(vi) use the Software to develop any software application intended for resale which employs the Software.

To the extent required by law, and at Customer's written request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Cisco makes such information available. Customer is granted no implied licenses to any other intellectual property rights other than as specifically granted herein.

Software, Upgrades and Additional Copies. For purposes of this Agreement, “Software” shall include (and the terms and conditions of this Agreement shall apply to) computer programs, including firmware, as provided to Customer by Cisco or an authorized Cisco reseller, and any upgrades, updates, bug fixes or modified versions thereto (collectively, “Upgrades”) or backup copies of the Software licensed or provided to Customer by Cisco or an authorized Cisco reseller. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Cisco.

Open Source Content. Customer acknowledges that the Software contains open source or publicly available content under separate license and copyright requirements which are located either in an attachment to this license, the Software README file or the Documentation. Customer agrees to comply with such separate license and copyright requirements.

Third Party Beneficiaries. Certain Cisco or Cisco affiliate suppliers are intended third party beneficiaries of this Agreement. The terms and conditions herein are made expressly for the benefit of and are enforceable by Cisco’s suppliers; provided, however, that suppliers are not in any contractual relationship with Customer. Cisco’s suppliers include without limitation: (a) Hifn, Inc., a Delaware corporation with principal offices at 750 University Avenue, Los Gatos, California and (b) Wind River Systems, Inc., and its suppliers. Additional suppliers may be provided in subsequent updates of Documentation supplied to Customer.

Term and Termination. This Agreement and the license granted herein shall remain effective until terminated. Customer may terminate this Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer’s rights under this Agreement will terminate immediately without notice from Cisco if Customer fails to comply with any provision of this Agreement. Cisco and its suppliers are further entitled to obtain injunctive relief if Customer’s use of the Software is in violation of any license restrictions. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled “U.S. Government End User Purchasers” and “General Terms Applicable to the Limited Warranty Statement and End User License” shall survive termination of this Agreement.

Customer Records. Customer grants to Cisco and its independent accountants the right to examine Customer’s books, records and accounts during Customer’s normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit.

Export. Software and Documentation, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software and Documentation. Customer’s failure to comply with such restrictions shall constitute a material breach of the Agreement.

U.S. Government End User Purchasers. The Software and Documentation qualify as “commercial items,” as that term is defined at Federal Acquisition Regulation (“FAR”) (48 C.F.R.) 2.101, consisting of “commercial computer software” and “commercial computer software documentation” as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which this End User License Agreement may be incorporated, Customer may provide to Government end user or, if this Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in this End User License Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are “commercial computer software” and “commercial computer software documentation,” and constitutes acceptance of the rights and restrictions herein.

Limited Warranty

Hardware for Cisco 2100 Series Wireless LAN Controllers, Cisco 4400 Series Wireless LAN Controllers, and Cisco Wireless Services Modules. Cisco Systems, Inc., or the Cisco Systems, Inc. subsidiary selling the Product (“Cisco”) warrants that commencing from the date of shipment to Customer (and in case of resale by a Cisco reseller, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of ninety (90) days, the Hardware will be free from defects in material and workmanship under normal use. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. This limited warranty extends only to the original user of the Product. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers under this limited warranty will be, at Cisco's or its service center's option, shipment of a replacement within the warranty period and according to the replacement process described in the Warranty Card (if any), or if no Warranty Card, as described at http://www.cisco.com/en/US/products/prod_warranties_listing.html or a refund of the purchase price if the Hardware is returned to the party supplying it to Customer, freight and insurance prepaid. Cisco replacement parts used in Hardware replacement may be new or equivalent to new. Cisco's obligations hereunder are conditioned upon the return of affected Hardware in accordance with Cisco's or its service center's then-current Return Material Authorization (RMA) procedures.

Software. Cisco warrants that commencing from the date of shipment to Customer (but in case of resale by an authorized Cisco reseller, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the software warranty period (if any) set forth in the warranty card accompanying the Product (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to its published specifications. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided AS IS. This limited warranty extends only to the Customer who is the original licensee. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers and licensors under this limited warranty will be, at Cisco's option, repair, replacement, or refund of the Software if reported (or, upon request, returned) to Cisco or the party supplying the Software to Customer. In no event does Cisco warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; or (d) is licensed, for beta, evaluation, testing or demonstration purposes for which Cisco does not charge a purchase price or license fee.

Disclaimer of Warranty

EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

General Terms Applicable to the Limited Warranty Statement and End User License Agreement

Disclaimer of Liabilities. REGARDLESS WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Cisco's or its suppliers' or licensors’ liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim or if the Software is part of another Product, the price paid for such other Product. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Customer agrees that the limitations of liability and disclaimers set forth herein will apply regardless of whether Customer has accepted the Software or any other product or service delivered by Cisco. Customer acknowledges and agrees that Cisco has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

The Warranty and the End User License shall be governed by and construed in accordance with the laws of the State of California, without reference to or application of choice of law rules or principles. The United Nations Convention on the International Sale of Goods shall not apply. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement shall remain in full force and effect. Except as expressly provided herein, this Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any purchase order or elsewhere, all of which terms are excluded. This Agreement has been written in the English language, and the parties agree that the English version will govern. For warranty or license terms which may apply in particular countries and for translations of the above information please contact the Cisco Legal Department, 300 E. Tasman Drive, San Jose, California 95134.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

APPENDIX D

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, page D-2
- System Messages, page D-2
- Using the CLI to Troubleshoot Problems, page D-5
- Configuring System and Message Logging, page D-6
- Viewing Access Point Event Logs, page D-13
- Uploading Logs and Crash Files, page D-14
- Uploading Core Dumps from the Controller, page D-17
- Monitoring Memory Leaks, page D-17
- Troubleshooting CCXv5 Client Devices, page D-19
- Using the Debug Facility, page D-34
- Configuring Wireless Sniffing, page D-39
- Troubleshooting Access Points Using Telnet or SSH, page D-42
- Debugging the Access Point Monitor Service, page D-43

Interpreting LEDs

Interpreting Controller LEDs

Refer to the quick start guide for your specific controller for a description of the LED patterns. You can find the guides at this URL:

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

Interpreting Lightweight Access Point LEDs

Refer to the hardware installation guide for your specific access point for a description of the LED patterns. You can find the guides at this URL:

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

System Messages

Table D-1 lists some common system messages and their descriptions. For a complete list of system messages, refer to the *Cisco Wireless LAN Controller System Message Guide, Release 5.2*.

Table D-1 System Messages and Descriptions

Error Message	Description
apf_utils.c 680: Received a CIF field without the protected bit set from mobile xx:xx:xx:xx:xx:xx	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.
dtl_arp.c 480: Got an idle-timeout message from an unknown client xx:xx:xx:xx:xx:xx	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 normally 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.
STATION_DISASSOCIATE	Client may have intentionally terminated usage or may have experienced a service disruption.
STATION_DEAUTHENTICATE	Client may have intentionally terminated usage or it could indicate an authentication issue.
STATION_AUTHENTICATION_FAIL	Check disable, key mismatch or other configuration issues.

Table D-1 System Messages and Descriptions (continued)

Error Message	Description
STATION_ASSOCIATE_FAIL	Check load on the Cisco radio or signal quality issues.
LRAD_ASSOCIATED	The associated lightweight access point is now managed by this controller.
LRAD_DISASSOCIATED	The lightweight access point may have associated to a different controller or may have become completely unreachable.
LRAD_UP	The lightweight access point is operational, no action required.
LRAD_DOWN	The lightweight access point may have a problem or is administratively disabled.
LRADIF_UP	Cisco radio is UP.
LRADIF_DOWN	Cisco radio may have a problem or is administratively disabled.
LRADIF_LOAD_PROFILE_FAILED	Client density may have exceeded system capacity.
LRADIF_NOISE_PROFILE_FAILED	The non-802.11 noise has exceed configured threshold.
LRADIF_INTERFERENCE_PROFILE_FAILED	802.11 interference has exceeded threshold on channel -- check channel assignments.
LRADIF_COVERAGE_PROFILE_FAILED	Possible coverage hole detected. Check the lightweight access point history to see if it is a common problem and add lightweight access points if necessary.
LRADIF_LOAD_PROFILE_PASSED	Load is now within threshold limits.
LRADIF_NOISE_PROFILE_PASSED	Detected noise is now less than threshold.
LRADIF_INTERFERENCE_PROFILE_PASSED	Detected interference is now less than threshold.
LRADIF_COVERAGE_PROFILE_PASSED	Number of clients receiving poor signal are within threshold.
LRADIF_CURRENT_TXPOWER_CHANGED	Informational message.
LRADIF_CURRENT_CHANNEL_CHANGED	Informational message.
LRADIF_RTS_THRESHOLD_CHANGED	Informational message.
LRADIF_ED_THRESHOLD_CHANGED	Informational message.
LRADIF_FRAGMENTATION_THRESHOLD_ CHANGED	Informational message.
RRM_DOT11_A_GROUPING_DONE	Informational message.
RRM_DOT11_B_GROUPING_DONE	Informational message.
ROGUE_AP_DETECTED	May be a security issue.Use maps and trends to investigate.

Table D-1 System Messages and Descriptions (continued)

Error Message	Description
ROGUE_AP_REMOVED	Detected rogue access point has timed out. The unit might have shut down or moved out of the coverage area.
AP_MAX_ROGUE_COUNT_EXCEEDED	The current number of active rogue access points has exceeded system threshold.
LINK_UP	Positive confirmation message.
LINK_DOWN	Port may have a problem or is administratively disabled.
LINK_FAILURE	Port may have a problem or is administratively disabled.
AUTHENTICATION_FAILURE	Attempted security breech. Investigate.
STP_NEWROOT	Informational message.
STP_TOPOLOGY_CHANGE	Informational message.
IPSEC_ESP_AUTH_FAILURE	Check WLAN IPSec configuration.
IPSEC_ESP_REPLAY_FAILURE	Check for attempt to spoof IP Address.
IPSEC_ESP_POLICY_FAILURE	Check for IPSec configuration mismatch between WLAN and client.
IPSEC_ESP_INVALID_SPI	Informational message.
IPSEC_OTHER_POLICY_FAILURE	Check for IPSec configuration mismatch between WLAN and client.
IPSEC_IKE_NEG_FAILURE	Check for IPSec IKE configuration mismatch between WLAN and client.
IPSEC_SUITE_NEG_FAILURE	Check for IPSec IKE configuration mismatch between WLAN and client.
IPSEC_INVALID_COOKIE	Informational message.
RADIOS_EXCEEDED	Maximum number of supported Cisco radios exceeded. Check for controller failure in the same Layer 2 network or add another controller.
SENSED_TEMPERATURE_HIGH	Check fan, air conditioning and/or other cooling arrangements.
SENSED_TEMPERATURE_LOW	Check room temperature and/or other reasons for low temperature.
TEMPERATURE_SENSOR_FAILURE	Replace temperature sensor ASAP.
TEMPERATURE_SENSOR_CLEAR	Temperature sensor is operational.
POE_CONTROLLER_FAILURE	Check ports — possible serious failure detected.
MAX_ROGUE_COUNT_EXCEEDED	The current number of active rogue access points has exceeded system threshold.
SWITCH_UP	Controller is responding to SNMP polls.
SWITCH_DOWN	Controller is not responding to SNMP polls, check controller and SNMP settings.

Table D-1 System Messages and Descriptions (continued)

Error Message	Description
RADIUS_SERVERS_FAILED	Check network connectivity between RADIUS and the controller.
CONFIG_SAVED	Running configuration has been saved to flash - will be active after reboot.
MULTIPLE_USERS	Another user with the same username has logged in.
FAN_FAILURE	Monitor controller temperature to avoid overheating.
POWER_SUPPLY_CHANGE	Check for power-supply malfunction.
COLD_START	The controller may have been rebooted.
WARM_START	The controller may have been rebooted.

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:

```
Name                Priority      CPU Use       Reaper
 reaperWatcher      ( 3/124)      0 %          (  0/  0)%   I
 osapiReaper          (10/121)    0 %          (  0/  0)%   I
 TempStatus          (255/  1)    0 %          (  0/  0)%   I
 emWeb               (255/  1)    0 %          (  0/  0)%   T 300
 cliWebTask          (255/  1)    0 %          (  0/  0)%   I
 UtilTask            (255/  1)    0 %          (  0/  0)%   T 300
```

   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:

```
Name               Priority     BytesInUse  BlocksInUse  Reaper
 reaperWatcher      ( 3/124)     0           0           (  0/  0)%  I
 osapiReaper         (10/121)    0           0           (  0/  0)%  I
 TempStatus         (255/  1)    308         1           (  0/  0)%  I
 emWeb              (255/  1)    294440      4910        (  0/  0)% T 300
 cliWebTask         (255/  1)    738         2           (  0/  0)%  I
 UtilTask           (255/  1)    308         1           (  0/  0)% T 300
```

   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 an array of 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 **config passwd-cleartext enable**. 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

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.

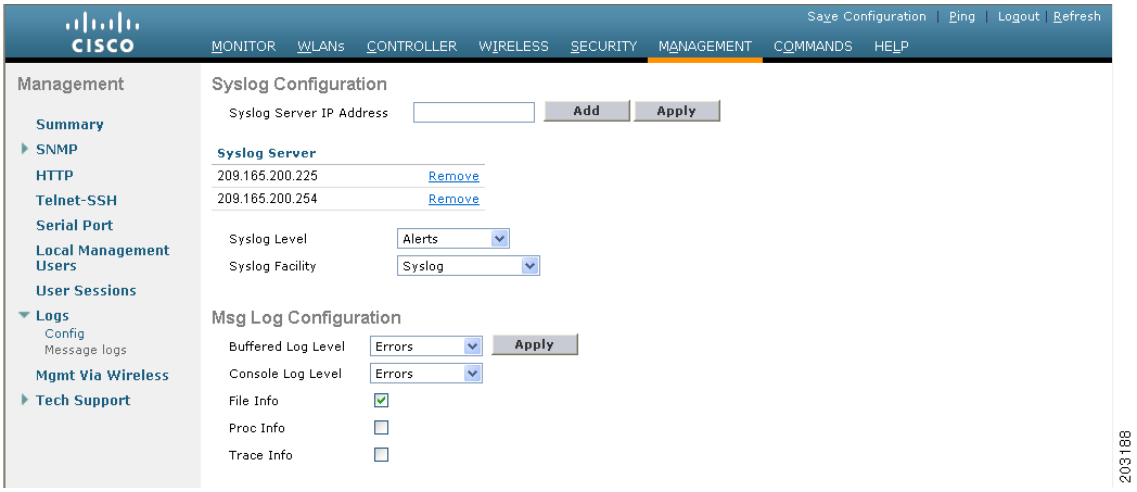
You can use the controller GUI or CLI to configure system and message logging.

Using the GUI to Configure System and Message Logging

Using the GUI, follow these steps to configure system and message logging.

Step 1 Click **Management** > **Logs** > **Config**. The Syslog Configuration page appears (see Figure D-1).

Figure D-1 Syslog Configuration Page



Syslog Configuration

Syslog Server IP Address

Syslog Server	
209.165.200.225	Remove
209.165.200.254	Remove

Syslog Level: Alerts

Syslog Facility: Syslog

Msg Log Configuration

Buffered Log Level: Errors

Console Log Level: Errors

File Info ☑

Proc Info □

Trace Info □

Step 2 In the Syslog Server IP Address field, 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 field.

Note If you ever 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 box:

- **Emergencies** = Severity level 0
- **Alerts** = Severity level 1 (default value)
- **Critical** = Severity level 2
- **Errors** = Severity level 3
- **Warnings** = Severity level 4
- **Notifications** = Severity level 5
- **Informational** = Severity level 6
- **Debugging** = Severity level 7

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 To set the facility for outgoing syslog messages to the syslog servers, choose one of the following options from the Syslog Facility drop-down box:

- **Kernel** = Facility level 0
- **User Process** = Facility level 1
- **Mail** = Facility level 2
- **System Daemons** = Facility level 3
- **Authorization** = Facility level 4
- **Syslog** = Facility level 5 (default value)
- **Line Printer** = Facility level 6
- **USENET** = Facility level 7
- **Unix-to-Unix Cop**y = Facility level 8
- **Cron** = Facility level 9
- **FTP Daemon** = Facility level 11
- **System Use 1** = Facility level 12
- **System Use 2** = Facility level 13
- **System Use 3** = Facility level 14
- **System Use 4** = Facility level 15
- **Local Use 0** = Facility level 16
- **Local Use 1** = Facility level 17
- **Local Use 2** = Facility level 18
- **Local Use 3** = Facility level 19
- **Local Use 4** = Facility level 20
- **Local Use 5** = Facility level 21
- **Local Use 6** = Facility level 22
- **Local Use 7** = Facility level 23

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 boxes:

- **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

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 7 Check 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 Check the **Proc Info** check box if you want the message logs to include process information. The default value is disabled.

Step 9 Check the **Trace Info** check box if you want the message logs to include traceback information. The default value is disabled.

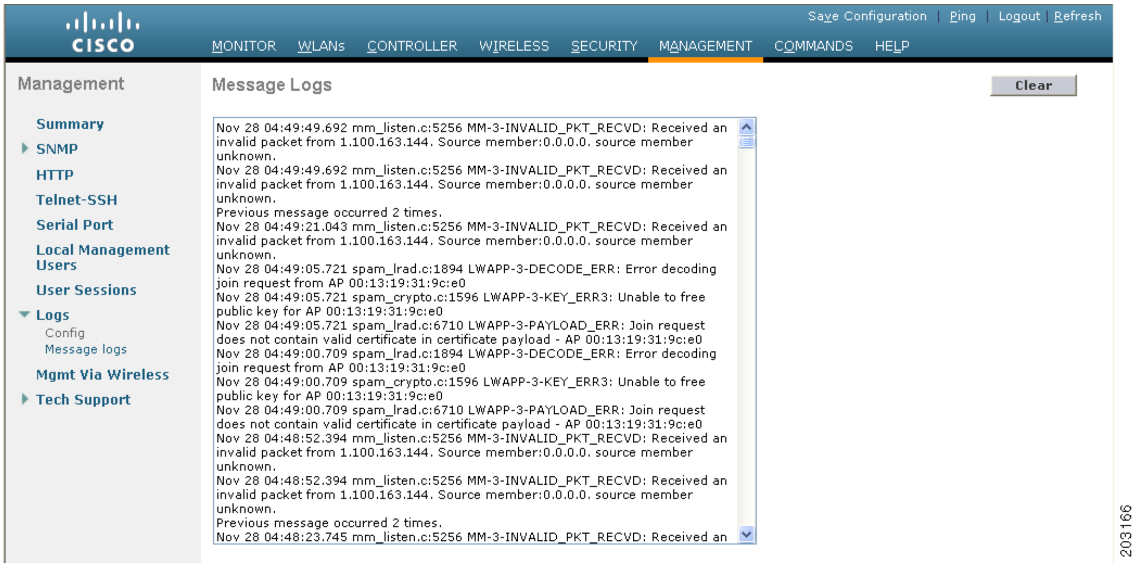
Step 10 Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Using the GUI to View Message Logs

To view message logs using the controller GUI, click **Management** > **Logs** > **Message Logs**. The Message Logs page appears (see Figure D-2).

Figure D-2 Message Logs Page



```
Nov 28 04:49:49.692 mm_listen.c:5256 MM-3-INVALID_PKT_RECVD: Received an
invalid packet from 1.100.163.144. Source member:0.0.0.0. source member
unknown.
Nov 28 04:49:49.692 mm_listen.c:5256 MM-3-INVALID_PKT_RECVD: Received an
invalid packet from 1.100.163.144. Source member:0.0.0.0. source member
unknown.
Previous message occurred 2 times.
Nov 28 04:49:21.043 mm_listen.c:5256 MM-3-INVALID_PKT_RECVD: Received an
invalid packet from 1.100.163.144. Source member:0.0.0.0. source member
unknown.
Nov 28 04:49:05.721 spam_lrad.c:1894 LWAPP-3-DECODE_ERR: Error decoding
join request from AP 00:13:19:31:9c:e0
Nov 28 04:49:05.721 spam_crypto.c:1596 LWAPP-3-KEY_ERR3: Unable to free
public key for AP 00:13:19:31:9c:e0
Nov 28 04:49:05.721 spam_lrad.c:6710 LWAPP-3-PAYLOAD_ERR: Join request
does not contain valid certificate in certificate payload - AP 00:13:19:31:9c:e0
Nov 28 04:49:00.709 spam_lrad.c:1894 LWAPP-3-DECODE_ERR: Error decoding
join request from AP 00:13:19:31:9c:e0
Nov 28 04:49:00.709 spam_crypto.c:1596 LWAPP-3-KEY_ERR3: Unable to free
public key for AP 00:13:19:31:9c:e0
Nov 28 04:49:00.709 spam_lrad.c:6710 LWAPP-3-PAYLOAD_ERR: Join request
does not contain valid certificate in certificate payload - AP 00:13:19:31:9c:e0
Nov 28 04:48:52.394 mm_listen.c:5256 MM-3-INVALID_PKT_RECVD: Received an
invalid packet from 1.100.163.144. Source member:0.0.0.0. source member
unknown.
Nov 28 04:48:52.394 mm_listen.c:5256 MM-3-INVALID_PKT_RECVD: Received an
invalid packet from 1.100.163.144. Source member:0.0.0.0. source member
unknown.
Previous message occurred 2 times.
Nov 28 04:48:23.745 mm_listen.c:5256 MM-3-INVALID_PKT_RECVD: Received an
```

Note To clear the current message logs from the controller, click **Clear**.

Using the CLI to Configure System and Message Logging

Using the CLI, follow these steps to configure system and message logging.

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.

Note 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 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 4 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 5 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 6 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 7 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 8 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 9 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 10 To save your changes, enter this command:

save config

Using the CLI to View System and Message Logs

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 debug messages dropped.............. 0
- Number of remote syslog hosts................. 0
  - Host 0...................................... Not Configured
  - 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........................
- 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

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.

Use these CLI commands to view or clear the access point event log from the controller:

- To view 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
*Sep 22 11:44:53.539: *** Access point reloading. Reason: NEW IMAGE DOWNLOAD ***
*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 00:00:43.143: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1,
changed state to up
*Mar 1 00:00:43.151: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0,
changed state to up
*Mar 1 00:00:48.078: %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER
*Mar 1 00:01:42.144: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
*Mar 1 00:01:48.121: %CAPWAP-3-CLIENTERRORLOG: Set Transport Address: no more AP
manager IP addresses remain
*Mar 1 00:01:48.122: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN
*Mar 1 00:01:48.122: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
*Mar 1 00:01:48.122: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
administratively down
...
```

- 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

Follow the instructions in this section to upload logs and crash files from the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP or FTP server available for the file upload. Keep these guidelines in mind when setting up a TFTP or FTP server:

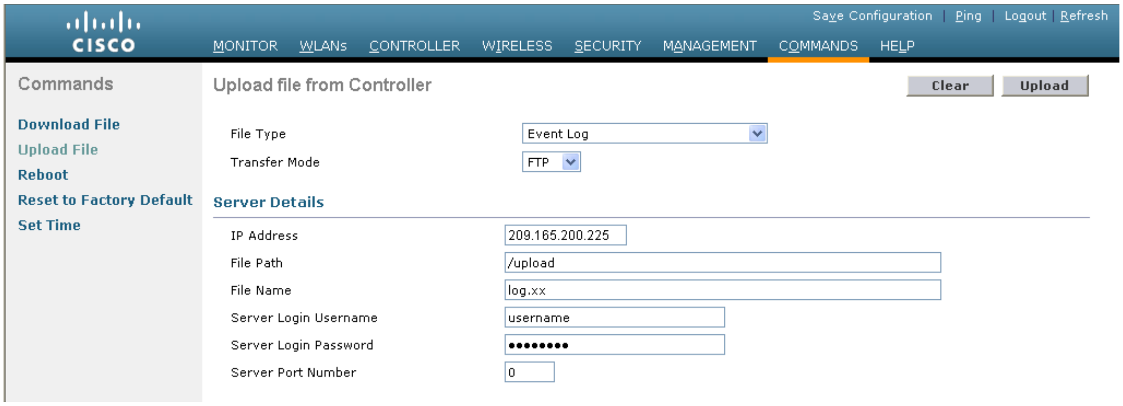
- If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are uploading through the distribution system network port, the TFTP or FTP server 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.

Using the GUI to Upload Logs and Crash Files

Using the controller GUI, follow these steps to upload logs and crash files.

Step 1 Click **Command** > **Upload File**. The Upload File from Controller page appears (see Figure D-3).

Figure D-3 Upload File from Controller Page



Upload file from Controller

File Type: Event Log
Transfer Mode: FTP

Server Details

IP Address: 209.165.200.225
File Path: /upload
File Name: log.xx
Server Login Username: username
Server Login Password: ••••••••
Server Port Number: 0

Step 2 From the File Type drop-down box, choose one of the following:

- **Event Log**
- **Message Log**
- **Trap Log**
- **Crash File**

Step 3 From the Transfer Mode drop-down box, choose **TFTP** or **FTP**.

Step 4 In the IP Address field, enter the IP address of the TFTP or FTP server.

Step 5 In the File Path field, enter the directory path of the log or crash file.

Step 6 In the File Name field, 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 field, enter the FTP server login name.

b. In the Server Login Password field, enter the FTP server login password.

c. In the Server Port Number field, 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.

Using the CLI to Upload Logs and Crash Files

Using the controller CLI, follow these steps to upload logs and crash files.

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 non-operational 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 view the updated settings, enter this command:

transfer upload start

Step 6 When prompted to confirm the current settings and start the software upload, answer **y**.

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. This section provides instructions to do so using the controller CLI.

Using the CLI to Upload Controller Core Dumps

Using the controller CLI, follow these steps to enable the controller to automatically upload a core dump file of the controller.

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, and

  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

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).

Using the controller CLI, follow these steps to monitor the controller for memory leaks.

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.

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 save your changes, enter this command:

save config

Step 4 To view 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 5 To view 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(0xabcd),poison(0xreadceef),
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 179a7afc 00000001
(179a7b00): 00000003 00000006 00000001 00000004 00000001 00000009 00000009 0000020d
(179a7b20): 00000001 00000002 00000002 00000001 00000004 00000000 00000000 5d7b9aba
(179a7b40): cbddf004 192f465e 7791acc8 e5032242 5365788c a1b7cee6 00000000 00000000
(179a7b60): 00000000 00000000 00000000 00000000 00000000 ceeff00d readf00d 00000080
(179a7b80): 00000000 00000000 17958dc0 00000000 1175608c 00000078 00000000 readceef
(179a7ba0): 179a7ba4 00000001 00000003 00000006 00000001 00000004 00000001 00003763
(179a7bc0): 00000002 00000002 00000010 00000001 00000002 00000000 0000001e 00000013
```

```
(179a7be0): 0000001a 00000089 00000000 00000000 000000d8 00000000 00000000 17222194
(179a7c00): 1722246c 1722246c 00000000 00000000 00000000 00000000 00000000 ceeff00d
(179a7c20): readf00d 00000080 00000000 00000000 179a7b78 00000000 1175608c 00000078
```

Step 6 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

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 6-39 for more information on CCX.

Note 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.

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 Cisco recommends that you enable the diagnostic channel feature only for non-anchored SSIDs that use the management interface.

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.

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.

Using the GUI to Configure the Diagnostic Channel

Follow these steps to configure the diagnostic channel using the controller GUI.

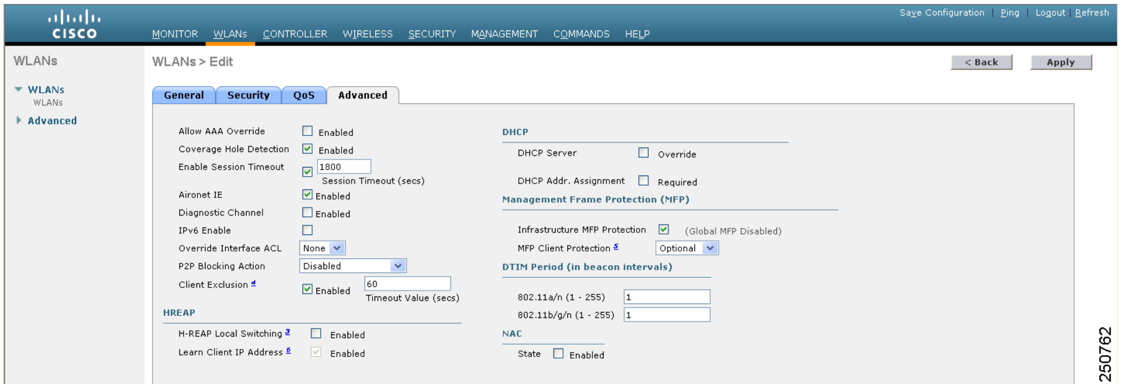
Step 1 Click **WLANs** to open the WLANs page.

Step 2 Create a new WLAN or click the ID number of an existing WLAN.

Note Cisco recommends that you create a new WLAN on which to run the diagnostic tests.

Step 3 When the WLANs > Edit page appears, click the **Advanced** tab to open the WLANs > Edit (Advanced) page (see Figure D-4).

Figure D-4 WLANs > Edit (Advanced) Page



WLANs > Edit

Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion ☑ Enabled 60 Timeout Value (secs)

HREAP

H-REAP Local Switching □ Enabled
Learn Client IP Address ☑ Enabled

DHCP

DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)

Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC

State □ Enabled

Step 4 If you want to enable diagnostic channel troubleshooting on this WLAN, check the **Diagnostic Channel** check box. Otherwise, leave this check box unchecked, which is the default value.

Note You can use the CLI to initiate diagnostic tests on the client. See the "Using the CLI to Configure the Diagnostic Channel" section on page D-21 for details.

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

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

Using the CLI to Configure the Diagnostic Channel

Using the controller CLI, follow these steps to configure the diagnostic channel.

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..................................... employee1
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........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
CCX - Diagnostics Channel Capability............. Enabled
...
```

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 host name, 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. Note however that 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 85  1e 00 00 89 00 0f 00 ff  l...............
00000040: 03 19 00 41 50 32 33 2d  31 30 00 00 00 00 00 00  ...AP23-10......
00000050: 00 00 00 00 00 00 26 96  06 00 40 96 00 ff ff dd  ......&...@.....
00000060: 18 00 50 f2 01 01 00 00  50 f2 05 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: 00 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
Last Frame Number:............................... 1120
Direction:....................................... 1
Timestamp:....................................... 0d 00h 50m 39s 878289us
Frame Length:.................................... 147
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 0d ed c3 a0 22  ..............."
00000010: 00 0d ed c3 a0 22 00 bd  4d 50 a5 f7 78 08 00 00  ....."..MP..x...
00000020: 64 00 01 00 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 01 02 00 00 85  1e 00 00 84 00 0f 00 ff  l...............
00000040: 03 19 00 72 6f 67 75 65  2d 74 65 73 74 31 00 00  ...rogue-test1..
00000050: 00 00 00 00 00 00 23 96  06 00 40 96 00 10 00 dd  ......#...@.....
00000060: 06 00 40 96 01 01 00 dd  05 00 40 96 03 04 dd 05  ..@.......@.....
00000070: 00 40 96 0b 01 dd 18 00  50 f2 02 01 01 81 00 03  .@......P.......

00000080: a4 00 00 27 a4 00 00 42  43 5e 00 62 32 2f 00 d2  ...'...BC^.b2/..
00000090: b4 ab 84                                          ...

LOG Frames:

Frame Number:.................................... 3
Last Frame Number:............................... 1120
Direction:....................................... 1
Timestamp:....................................... 0d 00h 50m 39s 881513us
Frame Length:.................................... 189
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 12 44 bd 80 30  ............D..0
00000010: 00 12 44 bd 80 30 60 f7  46 c0 8b 4b d1 05 00 00  ..D..0`.F..K....
00000020: 64 00 11 08 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 00 02 00 00 85  1e 00 00 89 00 0f 00 ff  l...............
00000040: 03 19 00 41 50 34 30 2d  31 37 00 00 00 00 00 00  ...AP40-17......
00000050: 00 00 00 00 00 00 26 dd  18 00 50 f2 01 01 00 00  ......&...P.....
00000060: 50 f2 05 01 00 00 50 f2  05 01 00 00 40 96 00 28  P.....P.....@..(
00000070: 00 dd 06 00 40 96 01 01  00 dd 05 00 40 96 03 04  ....@.......@...

00000080: dd 16 00 40 96 04 00 05  07 a4 00 00 23 a4 00 00  ...@........#...
00000090: 42 43 00 00 62 32 00 00  dd 05 00 40 96 0b 01 dd  BC..b2.....@....
000000a0: 18 00 50 f2 02 01 01 85  00 03 a4 00 00 27 a4 00  ..P..........'..
000000b0: 00 42 43 5e 00 62 32 2f  00 0b 9a 1d 6f           .BC^.b2/....o
...
```

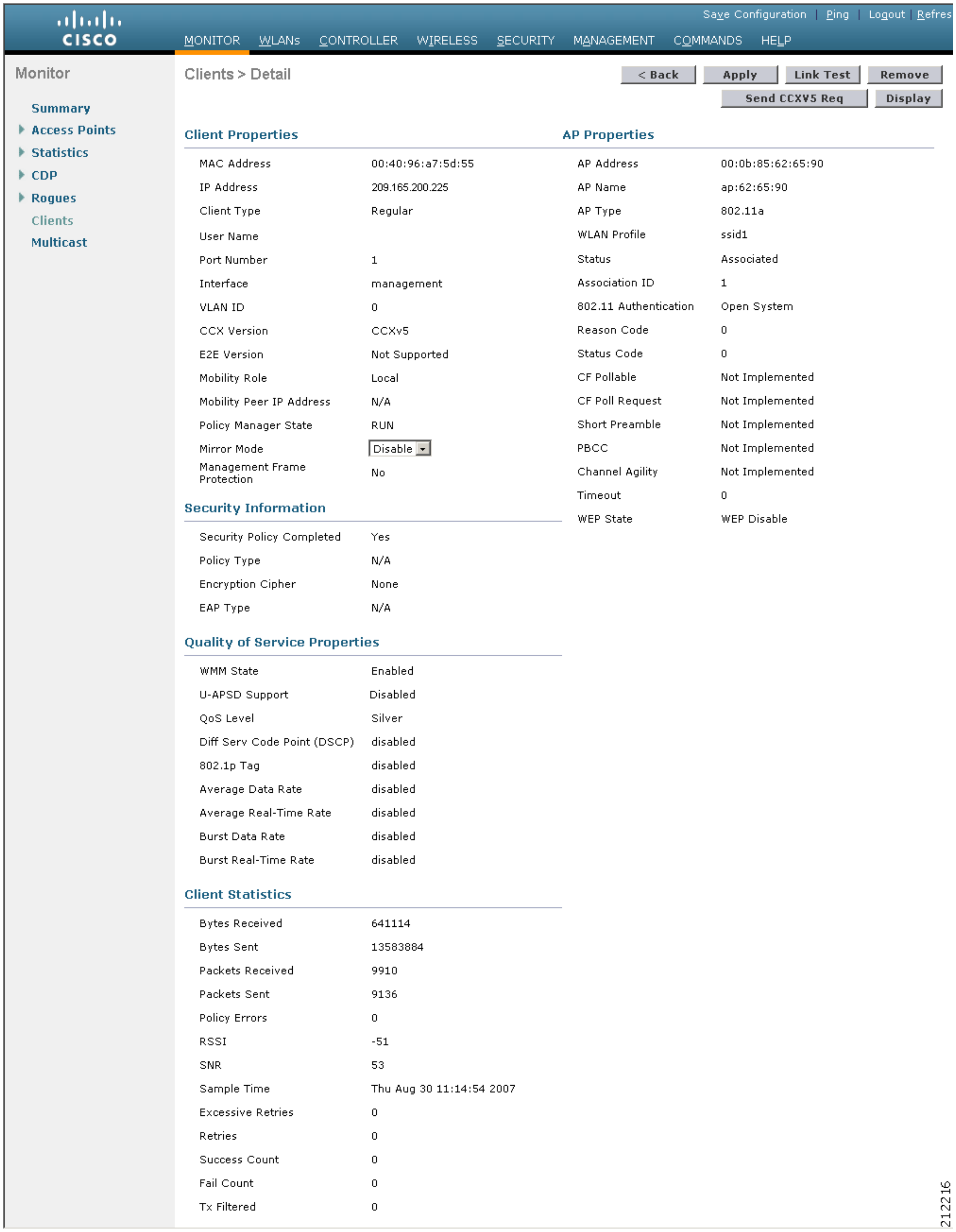
Using the GUI to Configure Client Reporting

Follow these steps to configure client reporting using the controller GUI.

Step 1 Click **Monitor** > **Clients** to open the Clients page.

Step 2 Click the MAC address of the desired client. The Clients > Detail page appears (see Figure D-5).

Figure D-5 Clients > Detail Page



Clients > Detail

Client Properties

MAC Address	00:40:96:a7:5d:55
IP Address	209.165.200.225
Client Type	Regular
User Name	
Port Number	1
Interface	management
VLAN ID	0
CCX Version	CCXv5
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Mirror Mode	Disable
Management Frame Protection	No

AP Properties

AP Address	00:0b:85:62:65:90
AP Name	ap:62:65:90
AP Type	802.11a
WLAN Profile	ssid1
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Disable

Security Information

Security Policy Completed	Yes
Policy Type	N/A
Encryption Cipher	None
EAP Type	N/A

Quality of Service Properties

WMM State	Enabled
U-APSD Support	Disabled
QoS Level	Silver
Diff Serv Code Point (DSCP)	disabled
802.1p Tag	disabled
Average Data Rate	disabled
Average Real-Time Rate	disabled
Burst Data Rate	disabled
Burst Real-Time Rate	disabled

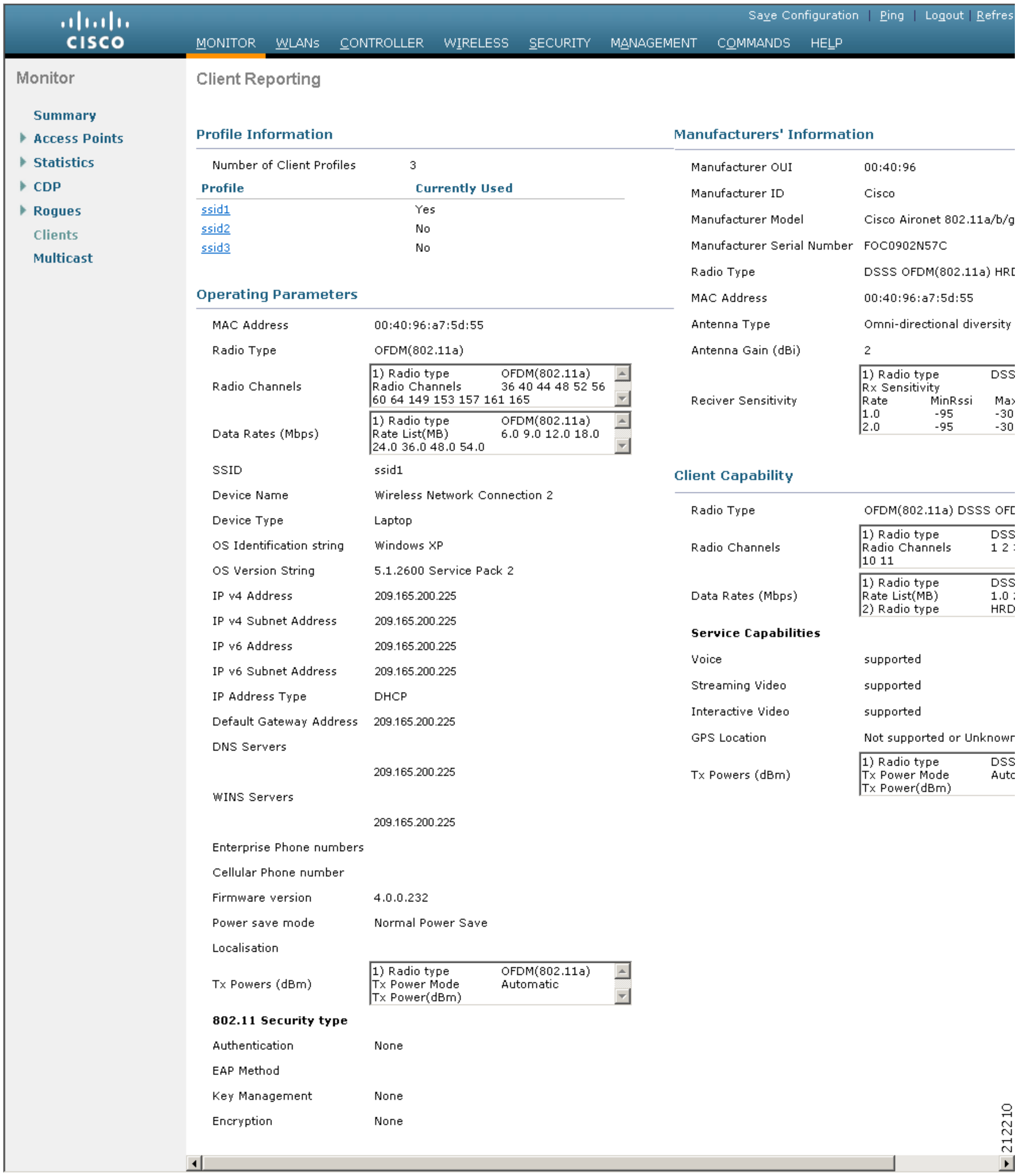
Client Statistics

Bytes Received	641114
Bytes Sent	13583884
Packets Received	9910
Packets Sent	9136
Policy Errors	0
RSSI	-51
SNR	53
Sample Time	Thu Aug 30 11:14:54 2007
Excessive Retries	0
Retries	0
Success Count	0
Fail Count	0
Tx Filtered	0

Step 3 To send a report request to the client, click the **CCXv5 Req** button.

Step 4 To view the parameters from the client, click **Display**. The Client Reporting page appears (see Figure D-6).

Figure D-6 Client Reporting Page



Client Reporting

Profile Information

Number of Client Profiles	3
Profile	**Currently Used**
ssid1	Yes
ssid2	No
ssid3	No

Operating Parameters

MAC Address	00:40:96:a7:5d:55
Radio Type	OFDM(802.11a)
Radio Channels	1) Radio type OFDM(802.11a) Radio Channels 36 40 44 48 52 56 60 64 149 153 157 161 165
Data Rates (Mbps)	1) Radio type OFDM(802.11a) Rate List(MB) 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
SSID	ssid1
Device Name	Wireless Network Connection 2
Device Type	Laptop
OS Identification string	Windows XP
OS Version String	5.1.2600 Service Pack 2
IP v4 Address	209.165.200.225
IP v4 Subnet Address	209.165.200.225
IP v6 Address	209.165.200.225
IP v6 Subnet Address	209.165.200.225
IP Address Type	DHCP
Default Gateway Address	209.165.200.225
DNS Servers	209.165.200.225
WINS Servers	209.165.200.225
Enterprise Phone numbers	
Cellular Phone number	
Firmware version	4.0.0.232
Power save mode	Normal Power Save
Localisation	
Tx Powers (dBm)	1) Radio type OFDM(802.11a) Tx Power Mode Automatic Tx Power(dBm)
802.11 Security type	
Authentication	None
EAP Method	
Key Management	None
Encryption	None

Manufacturers' Information

Manufacturer OUI	00:40:96
Manufacturer ID	Cisco
Manufacturer Model	Cisco Aironet 802.11a/b/g
Manufacturer Serial Number	FOC0902N57C
Radio Type	DSSS OFDM(802.11a) HRD
MAC Address	00:40:96:a7:5d:55
Antenna Type	Omni-directional diversity
Antenna Gain (dBi)	2
Reciver Sensitivity	1) Radio type DSS Rx Sensitivity Rate MinRssi Max 1.0 -95 -30 2.0 -95 -30

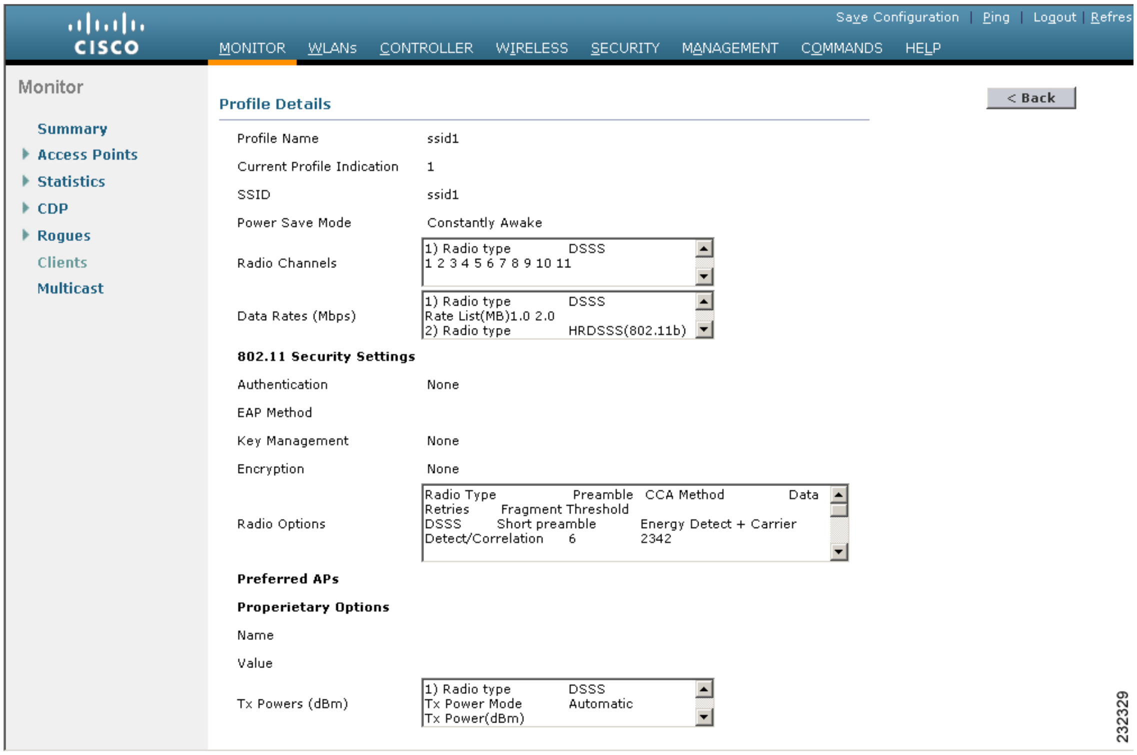
Client Capability

Radio Type	OFDM(802.11a) DSSS OFD
Radio Channels	1) Radio type DSS Radio Channels 1 2 10 11
Data Rates (Mbps)	1) Radio type DSS Rate List(MB) 1.0 2) Radio type HRD
Service Capabilities	
Voice	supported
Streaming Video	supported
Interactive Video	supported
GPS Location	Not supported or Unknowr
Tx Powers (dBm)	1) Radio type DSS Tx Power Mode Autc Tx Power(dBm)

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 (see Figure D-7).

Figure D-7 Profile Details Page


CISCO
Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Access Points
Statistics
CDP
Rogues
Clients
Multicast
< Back
232329

Profile Details

Profile Name	ssid1
Current Profile Indication	1
SSID	ssid1
Power Save Mode	Constantly Awake
Radio Channels	1) Radio type DSSS 1 2 3 4 5 6 7 8 9 10 11
Data Rates (Mbps)	1) Radio type DSSS Rate List(MB)1.0 2.0 2) Radio type HRDSSS(802.11b)
802.11 Security Settings	
Authentication	None
EAP Method	
Key Management	None
Encryption	None
Radio Options	Radio Type Preamble CCA Method Data Retries Fragment Threshold DSSS Short preamble Energy Detect + Carrier Detect/Correlation 6 2342
Preferred APs	
Properietary Options	
Name	
Value	
Tx Powers (dBm)	1) Radio type DSSS Tx Power Mode Automatic Tx Power(dBm)

This page shows the client profile details, including the SSID, power save mode, radio channel, data rates, and 802.11 security settings.

Using the CLI to Configure Client Reporting

Using the controller CLI, follow these steps to configure client reporting.

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+CCKM
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).................................. 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).................................. 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).................................. 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).................................. 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)

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

Power Save Mode.................................. Normal Power Save
SSID............................................. wifi
Security Parameters[EAP Method,Credential]....... None
Auth Method...................................... None
Key Management................................... None
Encryption....................................... None
Device Name...................................... Wireless Network Connection 15
Device Type...................................... 0
OS Id............................................ Windows XP
OS Version....................................... 5.1.2600 Service Pack 2
IP Type.......................................... DHCP address
IPv4 Address..................................... Available
IP Address....................................... 70.0.4.66
Subnet Mask...................................... 255.0.0.0
Default Gateway.................................. 70.1.0.1
IPv6 Address..................................... Not Available
IPv6 Address.....................................  0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0:
0: 0: 0:
IPv6 Subnet Mask.................................  0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0:
0: 0: 0:
DNS Servers...................................... 103.0.48.0
WINS Servers.....................................
System Name...................................... URAVAL3777
Firmware Version................................. 4.0.0.187
Driver Version................................... 4.0.0.187
```

Step 8 To see the client manufacturer information, enter this command:

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
Manufacturer Serial.............................. 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
Rx Sensitivity .................................. Rate:1.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity .................................. Rate:2.0 Mbps, MinRssi:-95, MaxRssi:-30
Radio Type....................................... HRDSSS(802.11b)
Rx Sensitivity .................................. Rate:5.5 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity .................................. Rate:11.0 Mbps, MinRssi:-95, MaxRssi:-30
```

```
Radio Type...................................... ERP(802.11g)
Rx Sensitivity ................................. Rate:6.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ................................. Rate:9.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ................................. Rate:12.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ................................. 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
```

Using the CLI to Configure Roaming and Real-Time Diagnostics

Using the controller CLI, follow these steps to configure roaming and real-time diagnostics.

Step 1 To send a log request, enter this command:

config client ccx 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 ccx 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:

```
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 13s 322396us
                          Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2,
Transition Time=3125(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 16s 599006us
                          Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2,
Transition Time=3235(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
                          Event Timestamp=0d 00h 00m 19s 882921us
                          Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2,
Transition Time=3234(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 08s 815477us
                          Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:d2,
Transition Time=3281(ms)
                          Transition Reason: First association to WLAN
                          Transition Result: Success
                          Event Timestamp=0d 00h 00m 26s 637084us
                          Source BSSID=00:0b:85:81:06:d2, Target BSSID=00:0b:85:81:06:c2,
Transition Time=3313(ms)
```

Information similar to the following appears for a log response with a *log_type* of rsna:

```
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 00s 246578us
                          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
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 00s 246625us
                          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
```

```
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:

```
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          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'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 278993us
                          Client SysLog = '<11> Jun 19 11:49:53 uraval3777 Mandatory
elements missing in the OID response'
                          Event Timestamp=0d 00h 19m 42s 278996us
                          Client SysLog = '<11> Jun 19 11:49:56 uraval3777 Mandatory
elements missing in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 279000us
                          Client SysLog = '<11> Jun 19 11:50:00 uraval3777 Mandatory
elements missing in the OID response'
                          Event Timestamp=0d 00h 19m 42s 279003us
                          Client SysLog = '<11> Jun 19 11:50:03 uraval3777 Mandatory
elements missing in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 279009us
                          Client SysLog = '<11> Jun 19 11:50:09 uraval3777 Mandatory
elements missing in the OID response'
                          Event Timestamp=0d 00h 19m 42s 279012us
                          Client SysLog = '<11> Jun 19 11:50:12 uraval3777 Mandatory
elements missing in the OID response'
```

Step 3 To send a request for statistics, enter this command:

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:

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
     dot11RTSSuccessCount                = 7
     dot11RTSFailureCount                = 8
     dot11ACKFailureCount                = 9
```

```
dot11ReceivedFragmentCount          = 10
dot11MulticastReceivedFrameCount    = 11
dot11FCSErrorCount                  = 12
dot11TransmittedFrameCount        = 13
```

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
  - 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.

Follow these steps to use the debug facility.

Step 1 To enable the debug facility, enter this command:

debug packet logging enable {**rx** | **tx** | **all**} *packet_count display_size*

where

- **rx** displays all received packets, **tx** displays all transmitted packets, and **all** displays both transmitted and received packets.
- *packet_count* is the maximum number of packets to log. You can enter a value between 1 and 65535 packets, and the default value is 25 packets.
- *display_size* is the number of bytes to display when printing a packet. By default, the entire packet is displayed.

Note To disable the debug facility, enter this command: **debug packet logging disable**.

Step 2 Use these commands to configure packet-logging ACLs:

- **debug packet logging acl driver** *rule_index action npu_encap port*

  where

  - *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-ping, iapp, ip, lwapp, multicast, orphan-from-sta, orphan-to-sta, rbcp, 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, ddp, idpr-cmtp, rspf, vmtp, 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, systat, daytime, netstat, qotd, msp, chargen, ftp-data, ftp, fsp, ssh, telnet, smtp, time, rlp, nameserver, whois, re-mail-ck, domain, mtp, bootps, 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, ntp, netbios-ns, netbios-dgm, netbios-ssn, imap2, snmp, snmp-trap, cmip-man, cmip-agent, xdmcp, nextstep, bgp, prospero, irc, smux, at-rtmp, at-nbp, at-echo, at-zis, qmtp, z3950, ipx, imap3, ulistserv, https, snpp, 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 accepts a numeric or any string recognized by getservbyname(). 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*

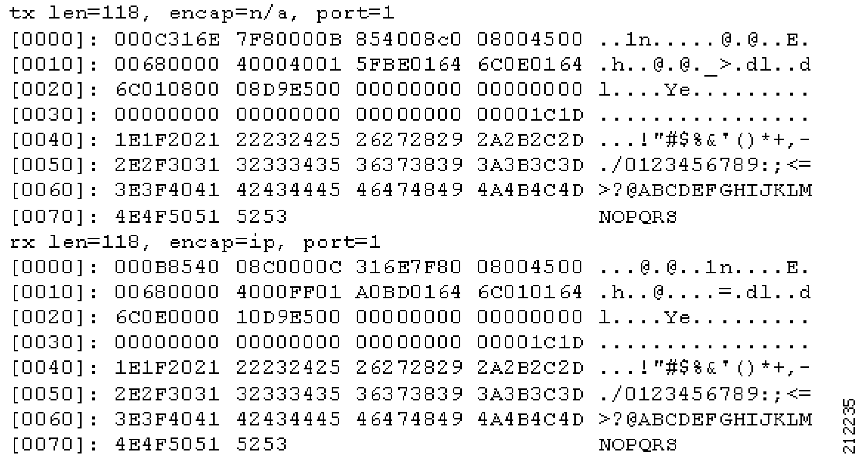
Note To remove all configured ACLs, enter this command: **debug packet logging acl clear-all**.

Step 3 To configure the format of the debug output, enter this command:

debug packet logging format {**hex2pcap** | **text2pcap**}

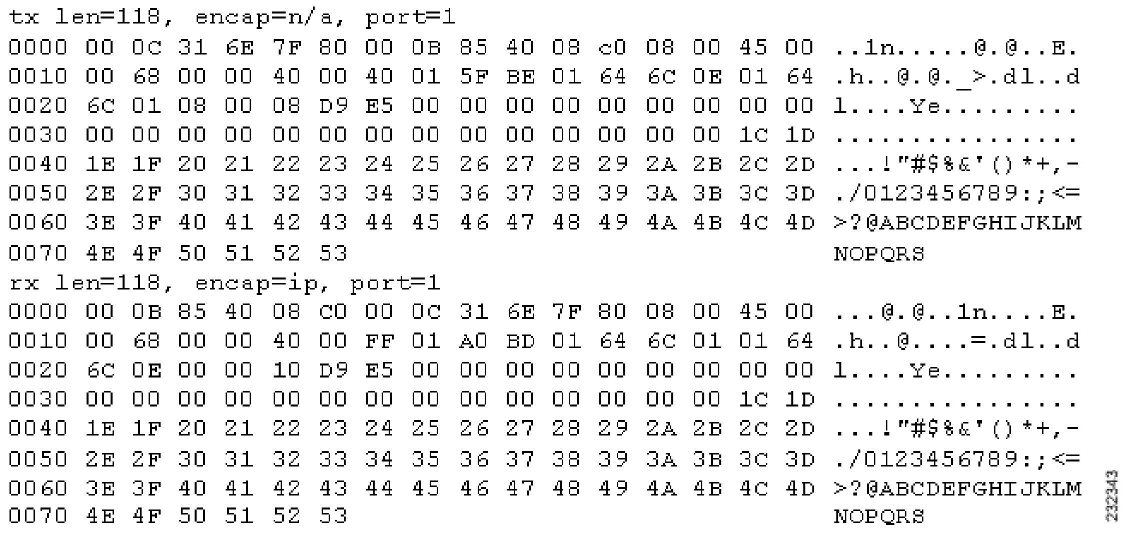
The debug facility supports two output formats: hex2pcap and text2pcap. The standard format used by IOS supports the use of hex2pcap and can be decoded using an HTML front end. The text2pcap option is provided as an alternative so that a sequence of packets can be decoded from the same console log file. Figure D-8 shows an example of hex2pcap output, and Figure D-9 shows an example of text2pcap output.

Figure D-8 Sample Hex2pcap Output



```
tx len=118, encap=n/a, port=1
[0000]: 000C316E 7F80000B 854008c0 08004500 ..1n.....@.@..E.
[0010]: 00680000 40004001 5FBE0164 6C0E0164 .h..@.@._>.dl..d
[0020]: 6C010800 08D9E500 00000000 00000000 l....Ye.........
[0030]: 00000000 00000000 00000000 00001C1D ................
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                       NOPQRS
rx len=118, encap=ip, port=1
[0000]: 000B8540 08C0000C 316E7F80 08004500 ...@.@..1n....E.
[0010]: 00680000 4000FF01 A0BD0164 6C010164 .h..@....=.dl..d
[0020]: 6C0E0000 10D9E500 00000000 00000000 l....Ye.........
[0030]: 00000000 00000000 00000000 00001C1D ................
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                       NOPQRS
```

Figure D-9 Sample Text2pcap Output



```
tx len=118, encap=n/a, port=1
0000 00 0C 31 6E 7F 80 00 0B 85 40 08 c0 08 00 45 00 ..1n.....@.@..E.
0010 00 68 00 00 40 00 40 01 5F BE 01 64 6C 0E 01 64 .h..@.@._>.dl..d
0020 6C 01 08 00 08 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                               NOPQRS
rx len=118, encap=ip, port=1
0000 00 0B 85 40 08 C0 00 0C 31 6E 7F 80 08 00 45 00 ...@.@..1n....E.
0010 00 68 00 00 40 00 FF 01 A0 BD 01 64 6C 01 01 64 .h..@....=.dl..d
0020 6C 0E 00 00 10 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
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

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 timestamp, signal strength, packet size, and so on. Sniffers allow you to monitor and record network activity and to detect problems.

Supported third-party network analyzer software applications include:

- Wildpackets Omnipeek or Airopeek (http://www.wildpackets.com)
- AirMagnet Enterprise Analyzer (http://www.airmagnet.com)
- Wireshark (http://www.wireshark.org)

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.
- **Software and supporting files, plug-ins, or adapters**—Your analyzer software may require specialized files before you can successfully enable sniffing:
  - **Omnipeek or Airopeek**—Go to http://www.wildpackets.com and follow the instructions to purchase, install, and configure the software.
  - **AirMagnet**—Go to http://www.airmagnet.com/products/ea_cisco/#top and follow the instructions to purchase, install, and configure the software.
  - **Wireshark**—Go to http://tools.cisco.com/support/downloads and follow the instructions to download Wireshark and the correct installation wizard for your operating system.

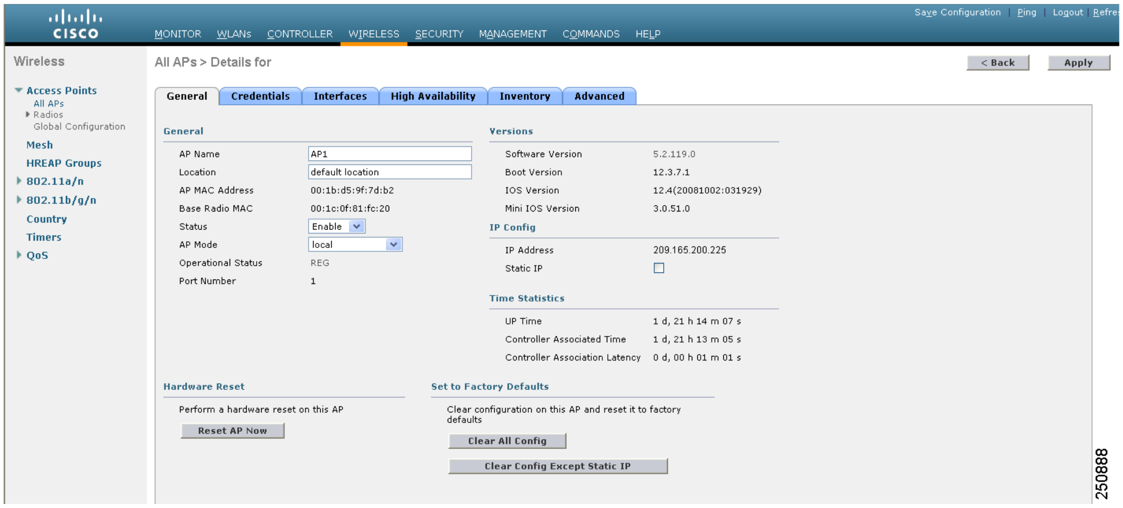
Using the GUI to Configure Sniffing on an Access Point

Using the controller GUI, follow these steps to configure sniffing on an access point.

Step 1 Click **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 (see Figure D-10).

Figure D-10 All APs > Details for Page



All APs > Details for

General

AP Name	AP1
Location	default location
AP MAC Address	00:1b:d5:9f:7d:b2
Base Radio MAC	00:1c:0f:81:fc:20
Status	Enable
AP Mode	local
Operational Status	REG
Port Number	1

Versions

Software Version	5.2.119.0
Boot Version	12.3.7.1
IOS Version	12.4(20081002:031929)
Mini IOS Version	3.0.51.0

IP Config

IP Address	209.165.200.225
Static IP	□

Time Statistics

UP Time	1 d, 21 h 14 m 07 s
Controller Associated Time	1 d, 21 h 13 m 05 s
Controller Association Latency	0 d, 00 h 01 m 01 s

Hardware Reset

Perform a hardware reset on this AP

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

Step 3 From the AP Mode drop-down box, choose **Sniffer**.

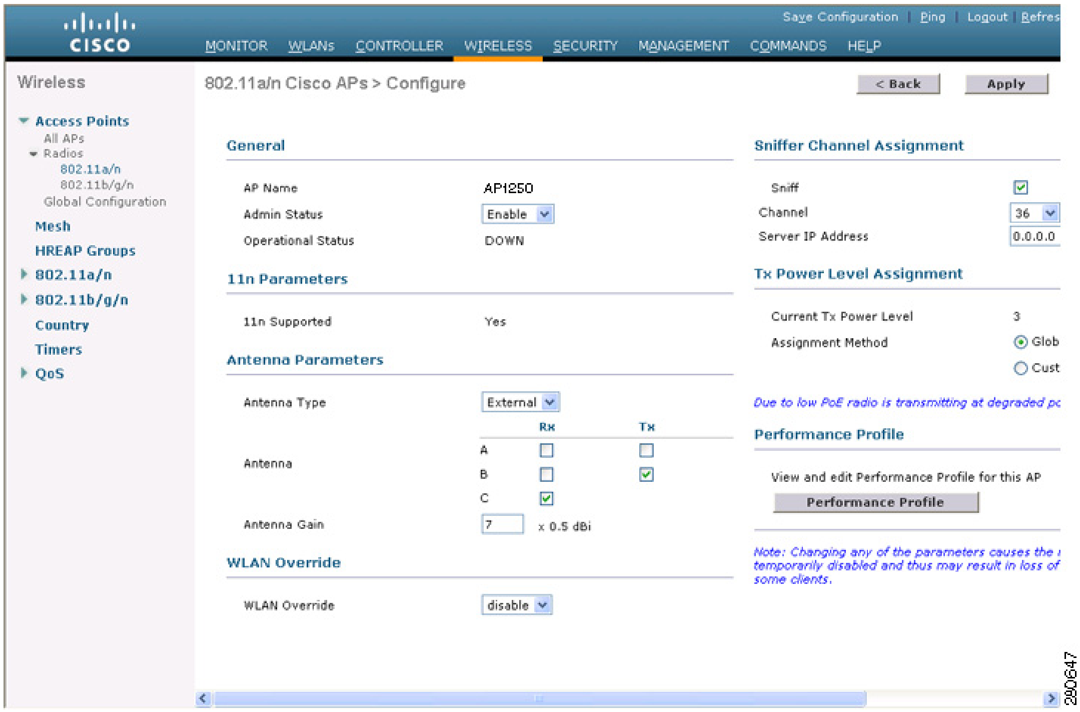
Step 4 Click **Apply** to commit your changes.

Step 5 Click **OK** when warned that the access point will be rebooted.

Step 6 Click **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 (see Figure D-11).

Figure D-11 802.11b/g/n Cisco APs > Configure Page



802.11a/n Cisco APs > Configure

General

AP Name	AP1250
Admin Status	Enable
Operational Status	DOWN

11n Parameters

11n Supported	Yes

Antenna Parameters

Antenna Type	External		
		Rx	Tx
Antenna	A	□	□
	B	□	☑
	C	☑	
Antenna Gain	7 x 0.5 dBi		

WLAN Override

WLAN Override	disable

Sniffer Channel Assignment

Sniff	☑
Channel	36
Server IP Address	0.0.0.0

Tx Power Level Assignment

Current Tx Power Level	3
Assignment Method	● Glob ○ Cust

Due to low PoE radio is transmitting at degraded pc

Performance Profile

View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the r temporarily disabled and thus may result in loss of some clients.

Step 8 Check the **Sniff** check box to enable sniffing on this access point, or leave it unchecked 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 box, choose the channel on which the access point sniffs for packets.

b. In the Server IP Address field, 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.

Using the CLI to Configure Sniffing on an Access Point

Using the controller CLI, follow these steps to configure sniffing on an access point.

Step 1 To configure the access point as a sniffer, enter this command:

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:

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 this command:
config ap sniff {802.11a | 802.11b} disable *Cisco_AP*

Step 4 To save your changes, enter this command:

save config

Step 5 To view the sniffer configuration settings for an access point, enter this command:

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

Information similar to the following appears:

```
Cisco AP Identifier.............................. 17
Cisco AP Name.......................................... AP1131:46f2.98ac
...
AP Mode ......................................... Sniffer
Public Safety .................................... Global: Disabled, Local: Disabled
Sniffing ............................................. No
...
```

Troubleshooting Access Points Using Telnet or SSH

The controller supports the use of Telnet or 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**, **where**.

Using the controller CLI, follow these steps to enable Telnet or SSH access on lightweight access points.

Step 1 To enable Telnet or SSH connectivity on an access point, enter this command:

config ap {**telnet | ssh**} **enable** *Cisco_AP*

Note To disable Telnet or SSH connectivity on an access point, enter this command:
config ap {**telnet | ssh**} **disable** *Cisco_AP*

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
Reg. Domain allowed by Country.................. 802.11bg:-ABCENR 802.11a:-ABCEN
AP Country code................................ US - United States
AP Regulatory Domain........................... 802.11bg:-A 802.11a:-A
Switch Port Number ............................ 2
MAC Address.................................... 00:19:2f:11:16:7a
IP Address Configuration....................... Static IP assigned
IP Address..................................... 10.22.8.133
IP NetMask..................................... 255.255.248.0
```

```
Gateway IP Addr................................. 10.22.8.1
Domain...........................................
Name Server......................................
Telnet State.................................... Enabled
Ssh State....................................... Enabled
...
```

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.

Using the CLI to Debug Access Point Monitor Service Issues

If you experience any problems with the access point monitor service, enter this command:

debug 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, and
- **packet** configures debugging of access point monitor packets.

APPENDIX E

Logical Connectivity Diagrams

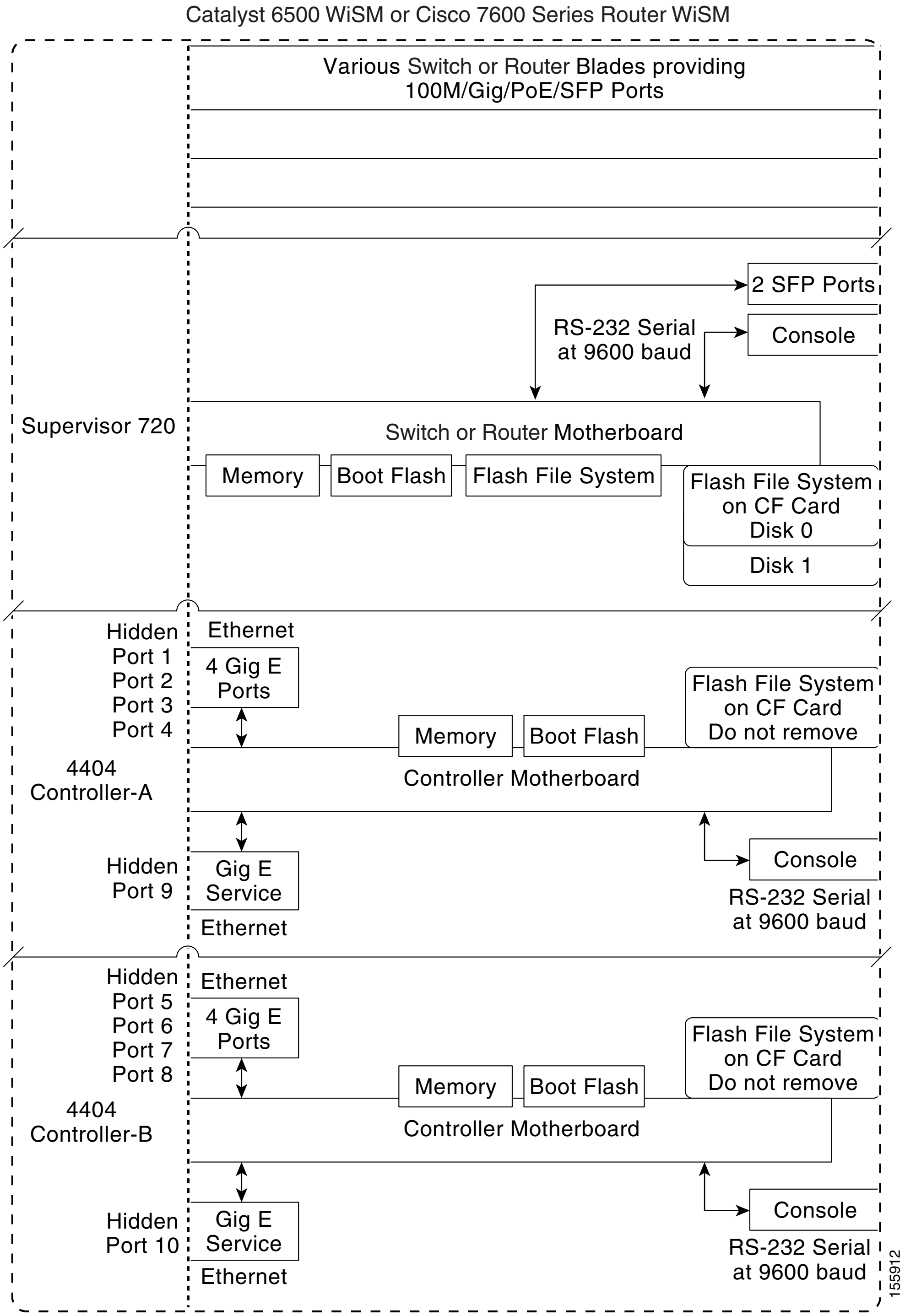
This appendix provides logical connectivity diagrams and related software commands for integrated controllers. It contains these sections:

- Cisco WiSM, page E-2
- Cisco 28/37/38xx Integrated Services Router, page E-3
- Catalyst 3750G Integrated Wireless LAN Controller Switch, page E-4

This section provides logical connectivity diagrams for the controllers integrated into other Cisco products, specifically the Catalyst 3750G Integrated Wireless LAN Controller Switch, the Cisco WiSM, and the Cisco 28/37/38xx Series Integrated Services Router. These diagrams show the internal connections between the switch or router and the controller. The software commands used for communication between the devices are also provided.

Cisco WiSM

Figure E-1 Logical Connectivity Diagram for the Cisco WiSM

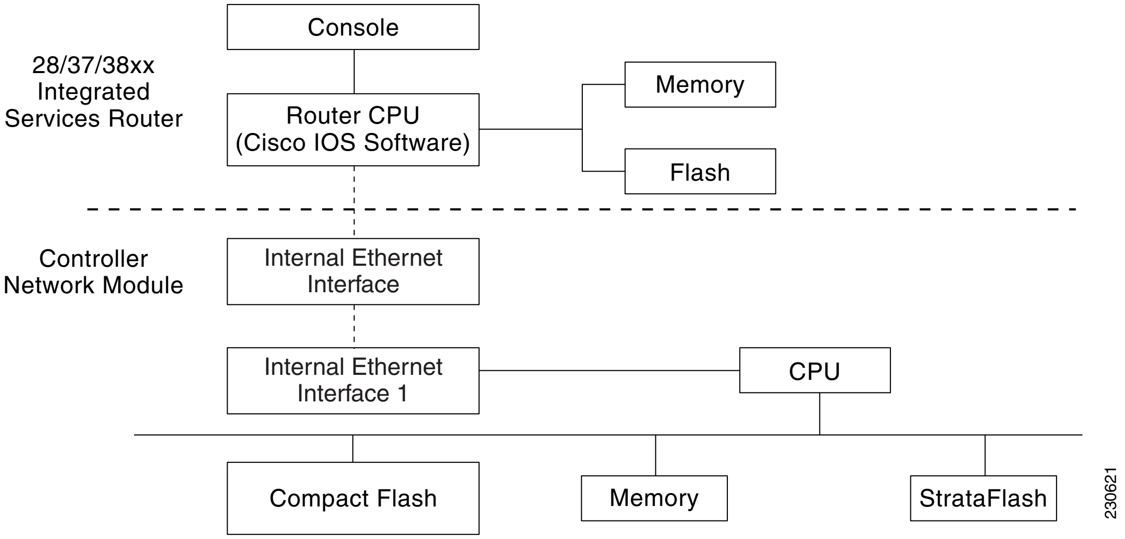

Catalyst 6500 WiSM or Cisco 7600 Series Router WiSM
Various Switch or Router Blades providing 100M/Gig/PoE/SFP Ports
2 SFP Ports
RS-232 Serial at 9600 baud
Console
Supervisor 720
Switch or Router Motherboard
Memory
Boot Flash
Flash File System
Flash File System on CF Card Disk 0
Disk 1
Hidden Port 1 Port 2 Port 3 Port 4
Ethernet
4 Gig E Ports
Memory
Boot Flash
Flash File System on CF Card Do not remove
4404 Controller-A
Controller Motherboard
Hidden Port 9
Gig E Service
Ethernet
Console
RS-232 Serial at 9600 baud
Hidden Port 5 Port 6 Port 7 Port 8
Ethernet
4 Gig E Ports
Memory
Boot Flash
Flash File System on CF Card Do not remove
4404 Controller-B
Controller Motherboard
Hidden Port 10
Gig E Service
Ethernet
Console
RS-232 Serial at 9600 baud
155912

The commands used for communication between the Cisco WiSM, the Supervisor 720, and the 4404 controllers are documented in *Configuring a Cisco Wireless Services Module and Wireless Control System* at this URL:

http://www.cisco.com/en/US/docs/wireless/technology/wism/technical/reference/appnote.html#wp39498

Cisco 28/37/38xx Integrated Services Router

Figure E-2 Logical Connectivity Diagram for the Cisco 28/37/38xx Integrated Services Router


28/37/38xx Integrated Services Router
Console
Router CPU (Cisco IOS Software)
Memory
Flash
Controller Network Module
Internal Ethernet Interface
Internal Ethernet Interface 1
CPU
Compact Flash
Memory
StrataFlash
230621

These commands are used for communication between the 28/37/38xx Integrated Services Router and the controller network module. They are initiated from the router. The commands vary depending on the version of the network module.

These commands are used for communication between the router and Fast Ethernet versions of the controller network module:

- **interface wlan-controller** *slot/unit* (and support for subinterfaces with **dot1q encap**)
- **show interfaces wlan-controller** *slot/unit*
- **show controllers wlan-controller** *slot/unit*
- **test service-module wlan-controller** *slot/unit*
- **test HW-module wlan-controller** *slot/unit* **reset** {**enable** | **disable**}
- **service-module wlan-controller** *slot/port* {**reload** | **reset** | **session** [**clear**] | **shutdown** | **status**}

These commands are used for communication between the router and Gigabit Ethernet versions of the controller network module:

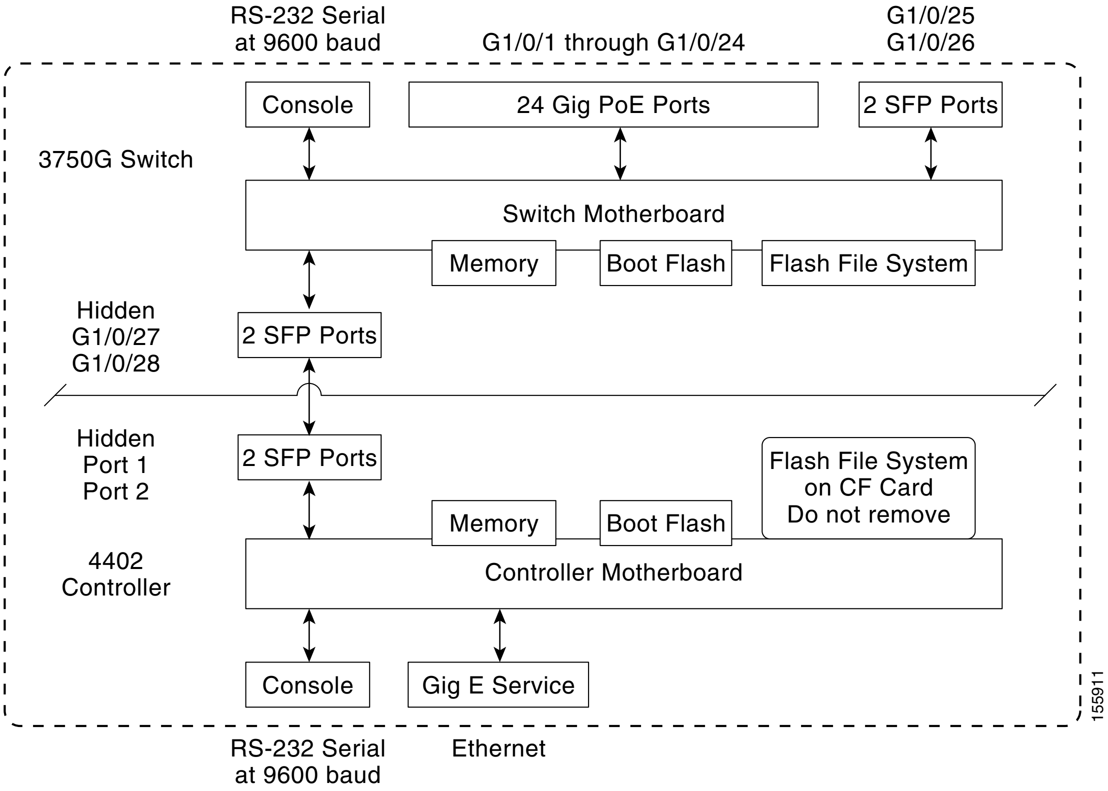
- **interface integrated-service-engine** *slot/unit* (and support for subinterfaces with **dot1q encap**)
- **show interfaces integrated-service-engine** *slot/unit*
- **show controllers integrated-service-engine** *slot/unit*
- **test service-module integrated-service-engine** *slot/unit*

- **test HW-module integrated-service-engine** *slot/unit* **reset** {**enable** | **disable**}
- **service-module integrated-service engine** *slot/port* {**reload** | **reset** | **session** [**clear**] | **shutdown** | **status**}

Note Refer to the *Cisco Wireless LAN Controller Network Module Feature Guide* for more information. You can find this document at this URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124limit/124x/124xa2/boxernm.htm#wp2033271

Catalyst 3750G Integrated Wireless LAN Controller Switch

Figure E-3 Logical Connectivity Diagram for the Catalyst 3750G Integrated Wireless LAN Controller Switch



These commands are used for communication between the Catalyst 3750G switch and the 4402 controller.

Login Command

This command is used to initiate a telnet session from the switch to the controller:

session *switch_number* **processor 1**

Because there can be several switches in a stack, the *switch_number* parameter is used to indicate to which controller in the stack this session should be directed. Once a session is established, the user interacts with the controller CLI. Entering **exit** terminates the session and returns the user to the switch CLI.

Show Commands

These commands are used to view the status of the internal controller. They are initiated from the switch.

- **show platform wireless-controller** *switch_number* **summary**

  Information similar to the following appears:

```
Switch  Status  State
1       up      operational
2       up      operational
```

- **show platform wireless-controller** *switch_number* **status**

  Information similar to the following appears:

```
Switch  Service IP      Management IP   SW Version      Status
------+---------------+---------------+---------------+-------
 1      127.0.1.1       70.1.30.1       4.0.52.0        operational
 2      127.0.1.2       70.1.31.1       4.0.45.0        operational
```

- **show platform wireless-controller** *switch_number* **management-info**

```
sw vlan ip                 gateway         http https mac            version
1  0    70.1.30.1/16       70.1.1.1        1    1     0016.9dca.d963 4.0.52.0
2  0    70.1.31.1/16       70.1.1.1        0    1     0016.9dca.dba3 4.0.45.0
```

Debug Commands

The Wireless Control Protocol (WCP) is an internal keep-alive protocol that runs between the switch and the controller. It enables the switch to monitor the health of the controller and to report any problems. It uses UDP and runs over the two internal Gigabit ports, but it creates an internal VLAN 4095 to separate control traffic from data traffic. Every 20 seconds the switch sends a keep-alive message to the controller. If the controller does not acknowledge 16 consecutive keep-alive messages, the switch declares the controller dead and sends a reset signal to reboot the controller.

These commands are used to monitor the health of the internal controller.

This command is initiated from the controller.

- **debug wcp** *?*

  where *?* is one of the following:

  packet—Debugs WCP packets.

  events—Debugs WCP events.

  Information similar to the following appears:

```
Tue Feb  7 23:30:31 2006: Received WCP_MSG_TYPE_REQUEST
Tue Feb  7 23:30:31 2006: Received WCP_MSG_TYPE_REQUEST,of type WCP_TLV_KEEP_ALIVE
Tue Feb  7 23:30:31 2006: Sent WCP_MSG_TYPE_RESPONSE,of type WCP_TLV_KEEP_ALIVE
Tue Feb  7 23:30:51 2006: Received WCP_MSG_TYPE_REQUEST
Tue Feb  7 23:30:51 2006: Received WCP_MSG_TYPE_REQUEST,of type WCP_TLV_KEEP_ALIVE
Tue Feb  7 23:30:51 2006: Sent WCP_MSG_TYPE_RESPONSE,of type WCP_TLV_KEEP_ALIVE
Tue Feb  7 23:31:11 2006: Received WCP_MSG_TYPE_REQUEST
Tue Feb  7 23:31:11 2006: Received WCP_MSG_TYPE_REQUEST,of type WCP_TLV_KEEP_ALIVE
Tue Feb  7 23:31:11 2006: Sent WCP_MSG_TYPE_RESPONSE,of type WCP_TLV_KEEP_ALIVE
```

This command is initiated from the switch.

- **debug platform wireless-controller** *switch_number ?*

  where *?* is one of the following:

  all—All

  errors—Errors

  packets—WCP packets

  sm—State machine

  wcp—WCP protocol

Reset Commands

These two commands (in this order) are used to reset the controller from the switch. They are not yet available but will be supported in a future release.

- **test wireless-controller stop** *switch_number*
- **test wireless-controller start** *switch_number*

Note A direct console connection to the controller does not operate when hardware flow control is enabled on the PC. However, the switch console port operates with hardware flow control enabled.

INDEX

Numerics

11n Mode parameter 4-18

1250 series access points

  and PoE Status field 7-72

  operating modes when using PoE 7-70

  transmit power settings when using PoE 7-71

3DES IPSec data encryption 5-9

7920 AP CAC parameter 6-35

7920 Client CAC parameter 6-35

7920 support mode

  configuring 6-33

  described 6-32

7921 support mode 6-34

802.11a (or 802.11b) > Client Roaming page 4-42

802.11a (or 802.11b) > Video Parameters page 4-56

802.11a (or 802.11b) > Voice Parameters page 4-54

802.11a (or 802.11b/g) > EDCA Parameters page 4-67

802.11a (or 802.11b/g) Global Parameters > Auto RF page 11-8

802.11a (or 802.11b/g) Global Parameters page 4-14, 11-37

802.11a (or 802.11b/g) Network Status parameter 4-14

802.11a/n (4.9 GHz) > Configure page 8-52

802.11a/n (or 802.11b/g/n) Cisco APs > Configure page 11-27

802.11a/n (or 802.11b/g/n) Radios page 4-60, 11-26

802.11a > Pico Cell page 11-42

802.11a > Pico Cell page with pico cell mode V2 parameters 11-43

802.11a > RRM > Coverage page 11-16

802.11a > RRM > DCA page 11-12

802.11a > RRM > Dynamic Channel Assignment (DCA) page 11-12

802.11a > RRM > General page 11-18

802.11a > RRM > Tx Power Control (TPC) page 11-10

802.11b/g/n Cisco APs > Configure page 7-60, D-40

802.11 bands

  configuring using the CLI 4-15 to 4-17

  configuring using the GUI 4-14 to 4-15

802.11g Support parameter 4-14

802.11n

  clients 7-75

  configuring

    using the CLI 4-19 to 4-22

    using the GUI 4-17 to 4-19

  devices 4-17

802.11n (2.4 GHz) High Throughput page 4-18

802.1Q VLAN trunk port 3-5

802.1X

  configuring 6-21

  described 6-22

  dynamic key settings 6-21

802.1X+CCKM

  configuring 6-23

  described 6-22

802.1X authentication for access points

  configuring

    the switch 7-14

    using the CLI 7-12 to 7-13

    using the GUI 7-10 to 7-12

  described 7-9

802.1x Authentication parameter 7-10

802.3 bridging

  configuring using the CLI 4-33

  configuring using the GUI 4-32 to 4-33

802.3 Bridging parameter 4-33

802.3 frames 4-32

802.3X flow control, enabling 4-31

A

AAA override
- configuring
  - using the CLI 5-80
  - using the GUI 5-79 to 5-80
- described 5-78

AC adapter warning for Japan B-7

Access Control List Name parameter 5-56

access control lists (ACLs)
- applying to an interface
  - using the CLI 5-65
  - using the GUI 5-59 to 5-60
- applying to a WLAN
  - using the CLI 5-65
  - using the GUI 5-61 to 5-62
- applying to the controller CPU
  - using the CLI 5-65
  - using the GUI 5-60 to 5-61
- configuring
  - using the CLI 5-63 to 5-64
  - using the GUI 5-55 to 5-58
- configuring for the debug facility D-35 to D-36
- counters
  - configuring using the CLI 5-63
  - configuring using the GUI 5-55
- described 5-54
- identity networking 5-75
- rules 5-54, 5-56, 5-64
- using with the debug facility D-34 to D-35

Access Control Lists > Edit page 5-58

Access Control Lists > New page 5-55

Access Control Lists > Rules > New page 5-56

Access Control Lists page 5-55

Access Mode parameter 4-26, 4-28

access point core dumps, uploading
- using the CLI 7-32
- using the GUI 7-31

access point event logs, viewing D-13

access point groups
- assigning access points to
  - using the CLI 6-48
  - using the GUI 6-46 to 6-47
- creating
  - using the CLI 6-47 to 6-48
  - using the GUI 6-44 to 6-47
- default group 6-44
- described 6-42
- illustrated 6-43
- number supported 6-44
- removing
  - using the CLI 6-47
  - using the GUI 6-45
- viewing 6-48 to 6-49

access point manager interface, configuring using the configuration wizard 4-5

access point monitor service, debugging D-43

access points
- 20-MHz channelization 11-27
- 40-MHz channelization 11-27
- adding MAC address to controller filter list
  - using the GUI 8-12 to 8-13
- assisted roaming 4-41
- authorization list 7-23
- authorizing
  - using LSCs 7-19 to 7-22
  - using MICs 7-18
  - using SSCs 7-18
  - using the CLI 7-23
  - using the GUI 7-22
- configuring hybrid REAP using the CLI 13-14
- converting to mesh access points 8-48
- embedded 7-14
- guidelines for operating in Japan B-6, B-7
- LEDs
  - configuring 7-74

interpreting D-2

migrating from the -J regulatory domain to the -U regulatory domain 7-55 to ??

number supported per controller 3-4

priming 7-3

regulatory information B-2 to B-10

rules for operating in Taiwan B-8 to B-9

supported for use with hybrid REAP 13-2

supporting oversized images 7-33 to 7-34

troubleshooting

the join process 7-24 to 7-28

using Telnet or SSH D-42

VCI strings 7-24

verifying that they join the controller 7-4

viewing multicast client table 4-39

Accounting Server parameters 6-54

accounting servers, disabling per WLAN 6-53

ACL. *See* access control lists (ACLs)

ACL Name parameter 5-60, 5-61

ACS server configuration page 6-51

Action parameter 5-58

active exploits 5-122

Add AAA Client page (on CiscoSecure ACS) 5-5, 5-20

Add AP button 13-18

Add New Rule button 5-56

Add Web Server button 10-17

AdHoc Rogue AP parameter 5-85

administrator access 4-23

administrator usernames and passwords, configuring 4-23

Admin Status parameter 3-21

Admission Control (ACM) parameter 4-55, 4-56

AES CBS IPSec data encryption 5-9

AES-CCMP 6-22

AES parameter 6-23

Aggregated MAC Protocol Data Unit (A-MPDU) 4-20

Aggregated MAC Service Data Unit (A-MSDU) 4-20

aggregation method, specifying 4-20

AirMagnet Enterprise Analyzer D-39

Aironet IE parameter 6-25, 6-40

Aironet IEs

configuring using the CLI 6-42

configuring using the GUI 6-40

Airopeek D-39

Alarm Trigger Threshold parameter 11-35

All APs > Access Point Name > Link Details > Neighbor Name page 8-46

All APs > Access Point Name > Mesh Neighbor Stats page 8-46

All APs > Access Point Name > Neighbor Info page 8-45

All APs > Access Point Name > Statistics page 8-40

All APs > Access Point Name > VLAN Mappings page 13-13

All APs > Details (Advanced) page

configuring CDP 4-73

All APs > Details for (Advanced) page 7-31

configuring country codes 7-51

configuring link latency 7-68

configuring PoE 7-71

All APs > Details for (Credentials) page 7-7, 7-11

All APs > Details for (General) page 13-12

All APs > Details for (High Availability) page 7-43, 7-47

All APs > Details for (H-REAP) page 13-12

All APs > Details for (Inventory) page 7-64

All APs > Details for page D-40

All APs > Details page 8-28, 11-34

All APs page 8-39, 11-34, 13-12

Allow AAA Override parameter 5-80

anchor controller in inter-subnet roaming 12-4

AnchorTime parameter 11-13

anonymous local authentication bind method 5-34, 5-37

Anonymous Provision parameter 5-44

Antenna Gain parameter 11-28

Antenna parameter 11-28

Antenna Type parameter 11-28

AP > Clients > Traffic Stream Metrics page 4-61

AP > Clients page 4-61

AP801 access point

described 7-14

using with a controller 7-14

AP Authentication Policy page 5-68, 11-35
AP Core Dump parameter 7-31
AP Ethernet MAC Addresses parameter 7-20
AP Failover Priority parameter 7-47
AP Group Name parameter 6-45
AP Groups > Edit (APs) page 6-46
AP Groups > Edit (General) page 6-45
AP Groups > Edit (WLANs) page 6-46, 6-60
AP Groups page 6-44, 6-59
AP-manager interface
  configuring
    using the CLI 3-14
    using the GUI 3-10 to 3-12
  creating multiple interfaces 3-38 to 3-39
  described 3-6
  illustration
    of four AP-manager interfaces 3-38
    of three AP-manager interfaces 3-37
    of two AP-manager interfaces 3-36
  using multiple 3-35 to 3-39
AP Mode parameter 11-35, 13-12, D-40
AP Name parameter 6-47
AP Policies page 7-22
AP Primary Discovery Timeout parameter 7-42
ASLEAP detection 5-122
Assignment Method parameter 11-27, 11-29
asymmetric tunneling
  described 12-26
  illustrated 12-26
audience of document xxiv
authenticated local authentication bind method 5-34, 5-37
Authentication Priority parameter 5-11, 5-25
Authentication Protocol parameter 4-28
Auth Key Mgmt parameter 6-23
Authority ID Information parameter 5-44, 13-21, 13-22
Authority ID parameter 5-44, 13-21
Authorize LSC APs against auth-list parameter 7-22
Authorize MIC APs against auth-list or AAA parameter 7-22
authorizing access points
  using the CLI 7-23
  using the GUI 7-22
auto-anchor mobility
  configuring
    using the CLI 12-23 to 12-24
    using the GUI 12-21 to 12-23
  guidelines 12-21
  overview 12-20 to 12-21
AutoInstall
  described 4-6, 4-9
  example operation 4-9
  obtaining
    DHCP addresses for interfaces 4-7
    TFTP server information 4-7
  overview 4-6
  selecting configuration file 4-8
  using 4-6
auto RF, configuring using the configuration wizard 4-6
Average Data Rate parameter 4-46, 4-49
Average Real-Time Rate parameter 4-46, 4-50
Avoid Cisco AP Load parameter 11-13
Avoid Foreign AP Interference parameter 11-13, 12-18
Avoid Non-802.11a (802.11b) Noise parameter 11-13

B

Backhaul Client Access parameter 8-17, 8-52
backup controllers
  configuring
    using the CLI 7-44 to 7-46
    using the GUI 7-42 to 7-44
  described 7-41
Back-up Primary Controller IP Address parameter 7-43
Back-up Primary Controller Name field 7-43
Back-up Secondary Controller IP Address parameter 7-43
Back-up Secondary Controller Name parameter 7-43
bandwidth-based CAC
  described 4-52

enabling
using the CLI 4-62
using the GUI 4-55
for mesh networks 8-32
Base MAC Address parameter 3-27
Beacon Period parameter 4-14
Bind Password parameter 5-34
Bind Username parameter 5-34
bootup script for configuration wizard 4-4
Bridge Data Rate parameter 8-30
Bridge Group Name parameter 8-29
bridge protocol data units (BPDUs) 3-23
bridging parameters
configuring using the CLI 8-31
configuring using the GUI 8-28 to 8-30
browsers supported 2-2
Buffered Log Level parameter D-8
Burst Data Rate parameter 4-46, 4-50
Burst Real-Time Rate parameter 4-46, 4-50

C

CAC
configuring for 7920 phones 6-33
described 4-52
enabling
using the CLI 4-63
using the GUI 4-56
in mesh networks 8-32
viewing in mesh networks 8-35 to 8-37
viewing using the CLI 4-64
Canadian compliance statement B-3
CA Server URL parameter 7-19
Catalyst 3750G Integrated Wireless LAN Controller Switch
described 1-11
logical connectivity diagram and associated software commands E-4 to E-6
ports 3-3, 3-5
cautions xxv
CCA Sensitivity Threshold parameter 11-44
CCKM
configuring 6-23
described 6-22
hybrid-REAP groups 13-16
with mobility 12-7
CCX
configuring Aironet IEs
using the CLI 6-42
using the GUI 6-40
described 6-39
link test 7-64
viewing a client’s version
using the CLI 6-42
using the GUI 6-40 to 6-41
CCX Layer 2 client roaming
configuring
using the CLI 4-43
using the GUI 4-42 to 4-43
debugging using the CLI 4-44
described 4-41
obtaining information using the CLI 4-43
CCX radio management
configuring
using the CLI 11-39
using the GUI 11-37 to 11-38
debugging using the CLI 11-41
features 11-36
hybrid-REAP considerations 11-36
obtaining information using the CLI 11-39 to 11-40
CCXv5 clients
enabling location presence 4-87
troubleshooting D-19 to D-34
CCXv5 Req button D-26
CCX Version parameter 6-41
CDP > AP Neighbors > Detail page 4-76
CDP > AP Neighbors page 4-75
CDP > Global Configuration page 4-72

CDP > Interface Neighbors > Detail page 4-74

CDP > Interface Neighbors page 4-74

CDP > Traffic Metrics page 4-76

CDP Advertisement Version parameter 4-72

CDP AP Neighbors page 4-75

CDP Protocol Status parameter 4-72

CDP State parameter 4-73

Certificate Authority (CA) certificates

  downloading

    using the CLI 9-17 to 9-18

    using the GUI 9-16

  overview 9-16

  using with local EAP 5-40, 5-45

Certificate Issuer parameter 5-43

Certificate Password parameter 9-14

Certificate Type parameter 7-23

Change Rules Priority parameter 5-90

Channel Assignment Leader parameter 11-14

Channel Assignment Method parameter 11-13

channel bonding in the 5-GHz band 11-28

Channel parameter 11-26, D-41

channels

  statically assigning using the CLI 11-30

  statically assigning using the GUI 11-26 to 11-30

Channel Scan Duration parameter 11-19

Channel Width parameter 11-14, 11-27

Check Against CA Certificates parameter 5-43

Check Certificate Date Validity parameter 5-43

chokepoints for RFID tag tracking 4-80

CIDS Sensor Add page 5-103

CIDS Sensors List page 5-103

CIDS Shun List page 5-106

ciphers

  configuring 6-23, 6-24

  described 6-23

Cisco 2100 Series Wireless LAN Controllers

  AutoInstall interfaces 4-7

  described 1-8

  FCC statement B-10

  features not supported 1-8

  network connections 1-17

  ports 3-2, 3-3, 3-4

Cisco 28/37/38xx Integrated Services Router

  described 1-11

  logical connectivity diagram and associated software commands E-3

  ports 3-3, 3-4, 4-91

  using 4-91

  versions 1-11

Cisco 3200 Series Mobile Access Router (MAR)

  described 8-51

  operating with mesh access points

    using the CLI to configure 8-53

    using the GUI to configure 8-52

Cisco 3300 Series Mobility Services Engine (MSE), using with wIPS 5-119

Cisco 4400 Series Wireless LAN Controllers

  AutoInstall interfaces 4-7

  described 1-8

  FCC statement B-10

  models 3-4

  network connections 1-18

  ports 3-2, 3-3, 3-4

  supporting more than 48 access points 3-34 to 3-39

Cisco 7920 Wireless IP Phones 6-34

Cisco 7921 Wireless IP Phones 6-34

Cisco AV-pairs 6-49, 6-50, 6-51

Cisco Centralized Key Management (CCKM). *See* CCKM

Cisco Clean Access (CCA) 6-55

Cisco Client Extensions (CCX). *See* CCX

Cisco Discovery Protocol (CDP)

  configuring

    using the CLI 4-77 to 4-78

    using the GUI 4-72 to 4-73

  debugging using the CLI 4-79

  described 4-69

  enabling using the GUI 4-72 to 4-73

  sample network 4-71

supported devices 4-69
viewing neighbors
using the CLI 4-78 to 4-79
using the GUI 4-73 to 4-77
viewing traffic information
using the CLI 4-78
using the GUI 4-76
Cisco Discovery Protocol parameter 4-73
Cisco high-power switches 7-72
Cisco Logo parameter 10-10
Cisco NAC Appliance 6-55
CiscoSecure Access Control Server (ACS) 5-4
Cisco Unified Wireless Network (UWN) Solution
described 1-2 to 1-4
illustrated 1-3
Cisco Wireless Control System (WCS) 1-2
Cisco WiSM
configuring the Supervisor 720 4-89 to 4-91
described 1-9 to 1-11
guidelines 4-90
logical connectivity diagram and associated software commands E-2 to E-3
maximum number supported by router chassis 1-10
ports 3-3, 3-4
SSC key-hash 7-16
CKIP
configuring
using the CLI 6-26
using the GUI 6-25 to 6-26
described 6-25
Clear Filter link 6-7
clearing the controller configuration 9-28
Clear Stats button 12-19
CLI
basic commands 2-9
enabling wireless connections 2-9
logging into 2-7 to 2-8
logging out 2-9
navigating 2-9
troubleshooting commands D-5 to D-6
using 2-7 to 2-9
Client Certificate Required parameter 5-43
client location, using WCS 1-7
client MFP 5-66
Client Protection parameter 5-70
client reporting
configuring using the CLI D-28 to D-31
configuring using the GUI D-25 to D-28
described D-19
Client Reporting page D-27
client roaming, configuring 4-40 to 4-44
clients
connecting to WLANs 13-15
viewing
using the CLI 7-78 to 7-79
using the GUI 7-74 to 7-78
viewing CCX version
using the CLI 6-42
using the GUI 6-40 to 6-41
Clients > AP > Traffic Stream Metrics page 4-59
Clients > AP page 4-59
Clients > Detail page
configuring client reporting D-26
viewing a client’s CCX version 6-41
viewing client details 7-39, 7-77
viewing the status of workgroup bridges 7-38
viewing voice and video settings 4-58
Clients page
performing a link test 7-66
viewing clients 7-75
viewing the status of workgroup bridges 7-38
viewing voice and video settings 4-57
Client Type parameter 7-38, 7-39
Commands > Reset to Factory Defaults page 4-3
comma-separated values (CSV) file, uploading 13-20
Community Name parameter 4-26
conditional web redirect 6-49
configuring

using the CLI 6-52
using the GUI 6-51 to 6-52
described 6-49
Conditional Web Redirect parameter 6-52
Configuration File Encryption parameter 9-24
configuration files
downloading
using the CLI 9-25 to 9-26
using the GUI 9-23 to 9-24
editing 9-27 to 9-28
uploading
using the CLI 9-22 to 9-23
using the GUI 9-21 to 9-22
configuration wizard
described 4-2
running 4-4 to 4-6
Configure option for RRM override 11-26
Confirm Password parameter 13-10
Console Log Level parameter D-8
Control and Provisioning of Wireless Access Points protocol (CAPWAP) 1-6
debugging 7-5
described 7-2
guidelines 7-2
viewing MTU information 7-5
controller failure detection time, reducing 7-41
controller network module
baud rate 3-3
versions 3-4
controllers
configuration
clearing 9-28
erasing 9-28
saving 9-26
connections 1-12
discovery process 7-2
guidelines for operating in Japan B-6 to B-7
multiple-controller deployment 1-4
overview 1-6 to 1-7
platforms 1-7 to 1-12
resetting factory default settings
using the CLI 4-3
using the GUI 4-3
single-controller deployment 1-3 to 1-4
synchronizing with location appliance 4-86
types of memory 1-15
upgrading software
guidelines 9-2 to 9-3
using the CLI 9-10 to 9-12
using the GUI 9-8 to 9-10
uploading core dump files from D-17
Controller Spanning Tree Configuration page 3-26
Controller Time Source Valid parameter 5-70
Control Path parameter 12-23
conventions of document xxv to xxvii
core dump files, uploading from the controller D-17
Country Code parameter 7-51
country codes
commonly used 7-49
configuring
using the CLI 7-52 to 7-54
using the configuration wizard 4-5
using the GUI 7-50 to 7-51
described 7-49
Japanese 7-55
viewing using the CLI 7-53
Country page 7-50
Coverage Exception Level per AP parameter 11-16
coverage hole detection
configuring per controller
using the CLI 11-21
using the GUI 11-15 to 11-17
disabling on a WLAN
described 6-54
using the CLI 6-55
using the GUI 6-54 to 6-55
coverage hole detection and correction 11-4
Coverage Hole Detection Enabled parameter 6-54

CPU Access Control Lists page 5-61

CPU ACL Mode parameter 5-61

crash files

  uploading

    using the CLI D-15 to D-16

    using the GUI D-14 to D-15

Current Channel parameter 11-29

Custom Signatures page 5-111

D

Data Path parameter 12-23

Data Rates parameter 4-15

date

  configuring manually 4-10

  configuring through NTP server 4-10

  setting

    using the CLI 4-11

    using the GUI 4-10

DCA Channel Sensitivity parameter 11-13

DCA Channels parameter 11-14

debug commands, sending 7-28

debug facility

  configuring D-35 to D-38

  described D-34 to D-35

  output D-36 to D-37

default enable password 7-5

default-group access point group 6-44

Default Mobility Group parameter 12-11

Default Routers parameter 6-12

Delivery Traffic Indication Map (DTIM). *See* DTIM period

Deny Counters parameter 5-58

Description parameter 5-31, 8-13, 13-10

Designated Root parameter 3-27

DES IPSec data encryption 5-9

Destination parameter 5-57

Destination Port parameter 5-57

Detect and Report Ad-Hoc Networks parameter 5-85

device certificates

  downloading

    using the CLI 9-15 to 9-16

    using the GUI 9-13 to 9-14

  overview 9-13

  using with local EAP 5-40, 5-45

DHCP

  configuring using the CLI 6-10

  configuring using the GUI 6-9

  debugging 6-11

DHCP Addr. Assignment Required parameter 6-10

DHCP Allocated Lease page 6-13

DHCP option 43, in controller discovery process 7-3

DHCP option 82

  configuring 5-53 to 5-54

  described 5-53

  example 5-53

DHCP Parameters page 4-22

DHCP proxy

  configuring

    using the CLI 4-23

    using the GUI 4-22 to 4-23

  described 4-22

DHCP Scope > Edit page 6-12

DHCP scopes

  configuring

    using the CLI 6-13 to 6-14

    using the GUI 6-11 to 6-12

  described 6-11

DHCP Scopes page 6-11

DHCP server discovery 7-3

DHCP Server IP Addr parameter 6-10

DHCP Server Override parameter 6-10

DHCP servers

  configuring using the configuration wizard 4-5

  external 6-8 to 6-9

  internal 6-8

diagnostic channel

  configuring

using the CLI D-21 to D-25

using the GUI D-20 to D-21

described D-19

Diagnostic Channel parameter D-21

directed roam request 4-41

Direction parameter 5-57

disabled clients, configuring a timeout 6-15

discovery request timer, configuring 7-45

distribution system ports 3-4 to 3-5

Diversity parameter 11-29

DNS Domain Name parameter 6-12

DNS Servers parameter 6-12

document

audience xxiv

conventions xxv to xxvii

organization xxiv to xxv

purpose xxiv

domain name server (DNS) discovery 7-3

Download button

downloading a CA certificate 9-17

downloading a configuration file 9-24

downloading a customized web authentication login page 10-19

downloading a device certificate 9-14

downloading a signature file 5-111

Download File to Controller page

downloading a customized web authentication login page 10-18

downloading CA certificates 9-16

downloading configuration files 9-23

downloading device certificates 9-14

downloading IDS signatures 5-110

DSCP parameter 5-57

DTIM period, configuring for MAC filtering 6-16

DTPC Support parameter 4-15

dynamic channel assignment (DCA)

20-MHz channelization 11-4, 11-14

40-MHz channelization 11-4, 11-14

configuring

using the CLI 11-20 to 11-21

using the GUI 11-12 to 11-15

described 11-3

sensitivity thresholds 11-14

dynamic frequency selection 7-58 to 7-59

dynamic interface

configuring

using the CLI 3-18

using the GUI 3-16 to 3-17

described 3-8

dynamic transmit power control, configuring 4-15

dynamic WEP, configuring 6-21

Dynamic WEP Key Index parameter 5-41

E

EAP-FAST Method Parameters page 5-44

EAP-FAST parameter 5-42

EAPOL-Key Max Retries parameter 5-41

EAPOL-Key Timeout parameter 5-41

EAP Profile Name parameter 5-45

EAP-TLS parameter 5-42

EDCA Profile parameter 4-67

Edit QoS Profile page 4-45

Edit QoS Role Data Rates page 4-49

Egress Interface parameter 10-27

Email Input parameter 10-28

Enable AP Local Authentication parameter 13-19

Enable AP Provisioning parameter 7-20

Enable Check for All Standard and Custom Signatures parameter 5-112

Enable Controller Management to be accessible from Wireless Clients parameter 2-10, 5-52

Enable Counters parameter 5-55

Enable Coverage Hole Detection parameter 11-16

Enable CPU ACL parameter 5-61

Enable DHCP Proxy parameter 4-23

Enable Dynamic AP Management parameter 3-39

Enable EAP-FAST Authentication parameter 13-21

Enable IGMP Snooping parameter 4-37

Enable LEAP Authentication parameter 13-21

Enable Link Latency parameter 7-68

Enable Low Latency MAC parameter 4-68

Enable LSC on Controller parameter 7-19

Enable Password parameter 7-7

Enable Server Status parameter 5-34

Enable Tracking Optimization parameter 7-60

Encryption Key parameter 6-26

end user license agreement C-2 to C-4

enhanced distributed channel access (EDCA) parameters

- configuring using the CLI 4-68 to 4-69
- configuring using the GUI 4-67 to 4-68

enhanced neighbor list

- described 4-41, 8-25
- request (E2E) 4-41

EoIP port 12-23, 12-28

epings 12-23, 12-29

erasing the controller configuration 9-28

Ethernet connection, using remotely 2-8

Ethernet Multicast Mode parameter 4-36

European declaration of conformity B-4 to B-5

event reporting for MFP 5-67

Expedited Bandwidth parameter 4-55

expedited bandwidth requests

- described 4-53
- enabling
  - using the CLI 4-63
  - using the GUI 4-55

Expiration Timeout for Rogue AP and Rogue Client Entries parameter 5-85

Extensible Authentication Protocol (EAP)

- configuring 6-21
- setting local timers 5-46
- timeout and failure counters
  - per access point 5-49
  - per client 5-49

extension channel 11-29

F

factory default settings

- resetting using the CLI 4-3
- resetting using the GUI 4-3

failover priority for access points

- configuring
  - using the CLI 7-48
  - using the GUI 7-46 to 7-48
- described 7-46
- viewing using the CLI 7-48

failover protection 1-16

fake access point detection 5-122

Fast Ethernet port 3-4

fast heartbeat timer

- configuring
  - using the CLI 7-44
  - using the GUI 7-42
- described 7-41

fast SSID changing

- configuring using the CLI 4-31
- configuring using the GUI 4-31

FCC declaration of conformity B-2 to B-3

FCC statement

- 2100 series controllers B-10
- 4400 series controllers B-10

Federal Information Processing Standards (FIPS) 5-11

File Compression parameter 7-31

file transfers 1-14

File Type parameter

- downloading a CA certificate 9-17
- downloading a configuration file 9-24
- downloading a customized web authentication login page 10-18
- downloading a device certificate 9-14
- upgrading controller software 9-9
- uploading a configuration file 9-22
- uploading PACs 9-19

filter, using to view clients 7-75 to 7-76

Fingerprint parameter 5-104

flashing LEDs, configuring 7-74

foreign controller in inter-subnet roaming 12-4

Forward Delay parameter 3-27, 3-28

forwarding plane architecture 4-32

Fragmentation Threshold parameter 4-14

Friendly Rogue > Create page 5-90

FTP server guidelines 9-2

G

General (controller) page
- configuring 802.3 bridging 4-33
- configuring an RF group 11-7
- enabling link aggregation 3-33
- enabling multicast mode 4-36

General (security) page 5-30, 5-122

General page 5-41

Generate Password parameter 10-5

gigabit Ethernet port 3-4

Global AP Failover Priority parameter 7-47

Global Configuration page
- configuring authentication for access points 7-10
- configuring backup controllers 7-42
- configuring failover priority for access points 7-46
- configuring global credentials for access points 7-6

global credentials for access points
- configuring
  - using the CLI 7-8 to 7-9
  - using the GUI 7-6 to 7-7
- described 7-5
- overriding
  - using the CLI 7-8
  - using the GUI 7-7

Group Mode parameter 11-8, 12-17

Group Name parameter 12-12, 13-17

Group Setup page (on CiscoSecure ACS) 5-22

Guest LAN parameter 10-26

guest N+1 redundancy 12-20

guest user accounts
- creating 10-2 to 10-7
- creating as a lobby ambassador 10-4 to 10-6
- viewing
  - using the CLI 10-7
  - using the GUI 10-6

Guest User parameter 5-31, 13-10

Guest User Role parameter 5-31, 13-10

guest WLAN, creating 10-5

GUI
- browsers supported 2-2
- enabling wireless connections 2-9
- guidelines 2-2
- opening 2-2
- using 2-2

H

Headline parameter 10-10

Hello Time parameter 3-27, 3-28

help, obtaining 2-2

hex2pcap sample output D-37

high-density network
- benefits 11-41
- example 11-41
- overview 11-41

Holdtime parameter 3-27, 4-72

Honeypot access point detection 5-122

HREAP Group Name parameter 13-13

HREAP Groups > Edit (Local Authentication > Local Users) page 13-20

HREAP Groups > Edit (Local Authentication > Protocols) page 13-21

HREAP Groups > Edit page 13-18

HREAP Groups page 13-17

H-REAP Local Switching parameter 13-8

H-REAP Mode AP Fast Heartbeat Timeout parameter 7-42

H-REAP Mode AP Fast Heartbeat Timer State parameter 7-42

HTTP Access parameter 2-3
HTTP Configuration page 2-3
HTTPS Access parameter 2-3
hybrid REAP
  access points supported 13-2
  authentication process 13-2 to 13-4
  bandwidth restriction 13-2
  configuring
    access points using the CLI 13-14
    access points using the GUI 13-11 to 13-13
    controller using the GUI 13-6 to 13-10
  guidelines 13-4
  illustrated 13-2
  number of access points supported 13-2
  overview 13-2
hybrid-REAP
  debugging 13-11, 13-14
hybrid-REAP groups
  backup RADIUS server 13-16
  CCKM 13-16
  configuring
    using the CLI 13-22
    using the GUI 13-17 to 13-21
  described 13-15
  example 13-16
  local authentication 13-17
Hysteresis parameter 4-42

I

identity networking
  configuring 5-74 to 5-77
  described 1-13 to 1-14
  overview 5-74
  RADIUS attributes 5-75 to 5-77
Identity Request Max Retries parameter 5-41
Identity Request Timeout parameter 5-41
IDS 5-103
IDS sensors
  configuring
    using the CLI 5-105 to 5-106
    using the GUI 5-103 to 5-105
  described 5-103
IDS signature events
  viewing using the CLI 5-117 to 5-118
  viewing using the GUI 5-114 to 5-115
IDS signatures
  configuring
    using the CLI 5-115 to 5-117
    using the GUI 5-109 to 5-114
  described 5-107
  frequency 5-113
  MAC frequency 5-113, 5-116
  measurement interval 5-113
  pattern 5-113
  quiet time 5-113, 5-116
  tracking method 5-113
  uploading or downloading using the GUI 5-110 to 5-111
  viewing
    using the CLI 5-117 to 5-118
    using the GUI 5-114 to 5-115
IGMP Timeout parameter 4-37
IKE Diffie Hellman Group parameter 5-10
IKE Phase 1 parameter 5-10
Index parameter for IDS 5-104
indoor access points
  converting to mesh access points 8-48
infrastructure MFP
  components 5-67
  described 5-66
Infrastructure MFP Protection parameter 5-69
Infrastructure Protection parameter 5-70
Infrastructure Validation parameter 5-70
Ingress Interface parameter 10-27
Injector Switch MAC Address parameter 7-72
inline power 7-70
intelligent power management (IPM) 7-72

inter-controller roaming
- described 4-40
- example 12-3

Interface Name parameter 6-46, 6-57, 6-60, 8-13

Interface parameter 6-10

interfaces
- and identity networking 5-76
- assigning WLANs 6-15
- configuring
  - using the CLI 3-13 to 3-15
  - using the GUI 3-11 to 3-12
- overview 3-6 to 3-8

Interfaces > Edit page
- applying an ACL to an interface 5-60
- configuring dynamic interfaces 3-17
- configuring NAC out-of-band integration 6-58
- configuring wired guest access 10-26
- creating multiple AP-manager interfaces 3-38

Interfaces > New page 3-16, 3-38

Interfaces page 3-11

interference 11-3

Interference threshold parameter 11-18

Internet Group Management Protocol (IGMP)
- configuring
  - using the CLI 4-38
  - using the GUI 4-37
- snooping 4-34

inter-subnet mobility 12-7

inter-subnet roaming
- described 4-40
- illustrated 12-3 to 12-4

Interval parameter 11-13, 11-38

intra-controller roaming
- described 4-40
- illustrated 12-2

Inventory page 7-63

Invoke Channel Update Now button 11-13

Invoke Power Update Now button 11-11

IP address-to-MAC address binding
- configuring 4-44 to 4-45
- described 4-44

IP Mask parameter 4-26

IPSec parameter 5-9

IPv6 bridging
- configuring
  - using the CLI 6-39
  - using the GUI 6-38 to 6-39
- described 6-36
- guidelines 6-37

IPv6 bridging and IPv4 web authentication example 6-38

IPv6 Enable parameter 6-39

J

Japanese country codes 7-55

Japanese regulations for migrating access points from the -J to the -U regulatory domain 7-55 to ??

K

Keep Alive Count parameter 12-22

Keep Alive Interval parameter 12-22

Key Encryption Key (KEK) parameter 5-8

Key Format parameter 6-26

Key Index parameter 6-26

key permutation
- configuring 6-26, 6-27
- described 6-25

Key Permutation parameter 6-26

Key Size parameter 6-26

Key Wrap Format parameter 5-8

Key Wrap parameter 5-8

L

LAG. *See* link aggregation (LAG)

LAG Mode on Next Reboot parameter 3-33

Last Auto Channel Assignment parameter 11-14

Last Power Level Assignment parameter 11-11
Layer 1 security 5-2
Layer 2
  operation 1-6
  security
    configuring 6-20 to 6-27
    described 5-2
Layer 2 Security parameter 6-23, 6-26, 6-51
Layer 3
  operation 1-6
  security
    configuring 6-28 to 6-30
    described 5-3
Layer 3 Security parameter
  for VPN passthrough 6-29
  for web authentication 6-30
  for web redirect 6-52
  for wired guest access 10-28
LDAP
  choosing server priority order 5-35
  configuring
    using the CLI 5-36 to 5-38
    using the GUI 5-33 to 5-36
  local EAP methods supported 5-33, 5-39
LDAP server
  assigning to WLANs 5-35 to 5-36
  choosing local authentication bind method
    using the CLI 5-37
    using the GUI 5-34
LDAP Servers > New page 5-33
LDAP Servers page 5-33
LDAP Servers parameter 5-45
LEAP parameter 5-42
Learn Client IP Address parameter 13-9
Lease Time parameter 6-12
LEDs
  configuring 7-74
  interpreting D-2
license agreement C-2 to C-4
Lifetime parameter 5-31, 10-5, 13-10
Lightweight Access Point Protocol (LWAPP) 1-6, 7-2
lightweight mode, reverting to autonomous mode 7-17
limited warranty C-4 to C-6
link aggregation (LAG)
  configuring neighboring devices 3-34
  described 3-29 to 3-30
  enabling
    using the CLI 3-34
    using the GUI 3-33
  example 3-30
  guidelines 3-32
  illustrated 3-31
  verifying settings using the CLI 3-34
link latency
  configuring
    using the CLI 7-69 to 7-70
    using the GUI 7-68 to 7-69
  described 7-67
Link Status parameter 3-20
Link Test
  button 7-66
  option 7-66, 8-45
  page 7-66
link test
  described 7-64
  performing
    using the CLI 7-67
    using the GUI 7-65 to 7-66, 8-45 to 8-46
  types of packets 7-64
Link Trap parameter 3-22
Load-based AC parameter 4-55
load-based CAC
  described 4-52 to 4-53
  enabling
    using the CLI 4-62
    using the GUI 4-55
lobby ambassador account
  creating using the CLI 10-3

creating using the GUI 10-2 to 10-3

Lobby Ambassador Guest Management > Guest Users List > New page 10-4

Lobby Ambassador Guest Management > Guest Users List page 10-4, 10-6

Local Auth Active Timeout parameter 5-41

local EAP

configuring

using the CLI 5-45 to 5-50

using the GUI 5-40 to 5-45

debugging 5-50

described 5-38 to 5-40

example 5-39

viewing information using the CLI 5-48

Local EAP Authentication parameter 5-45

Local EAP Profiles > Edit page 5-42

Local EAP Profiles page 5-42

Local Management Users > New page 10-3

Local Management Users page 10-2

Local Mode AP Fast Heartbeat Timeout parameter 7-42

Local Mode AP Fast Heartbeat Timer parameter 7-42

Local Net Users > New page 5-31, 13-9

Local Net Users page 5-30, 10-6

local network users

configuring using the CLI 5-32

configuring using the GUI 5-29 to 5-32

local significant certificate (LSC)

configuring

using the CLI 7-20 to 7-22

using the GUI 7-19 to 7-20

described 7-19

Local Significant Certificates (LSC) page 7-19

local user database, capacity 10-2

location

calibration 11-37

viewing settings using the CLI 4-86 to 4-89

location appliance

installing certificate 4-84 to 4-85

synchronizing with controller 4-86

location-based services 11-37

location presence 4-87

logical connectivity diagram

Catalyst 3750G Integrated Wireless LAN Controller Switch E-4

Cisco 28/37/38xx Integrated Services Router E-3

Cisco WiSM E-2

logs

roaming D-20, D-31 to D-32

RSNA D-20, D-31 to D-33

syslog D-20, D-31 to D-33

uploading

using the CLI D-15 to D-16

using the GUI D-14 to D-15

long preambles

described 5-50

enabling on SpectraLink NetLink phones

using the CLI 5-51

using the GUI 5-50

LWAPP-enabled access points

configuring a static IP address 7-33

debug commands 7-28

disabling the reset button 7-33

guidelines 7-16

MAC addresses displayed on controller GUI 7-32

radio core dumps

described 7-28

receiving debug commands from controller 7-28

retrieving radio core dumps 7-29

reverting to autonomous mode 7-17 to 7-18

sending crash information to controller 7-28

uploading

access point core dumps 7-31 to 7-32

radio core dumps 7-29 to 7-30

M

MAC address of access point

adding to controller filter list

using the GUI 8-12 to 8-13, 8-31
displayed on controller GUI 7-32
MAC Address parameter 8-12
MAC filtering
configuring on WLANs 6-14 to 6-15
DTIM period 6-16
MAC Filtering page 8-12
MAC Filters > New page 8-12
management frame protection (MFP)
configuring
using the CLI 5-70 to 5-71
using the GUI 5-68 to 5-69
debugging 5-73
described 5-66 to 5-67
guidelines 5-67
types 5-66
viewing settings 5-71 to 5-73
Management Frame Protection parameter 5-70
Management Frame Protection Settings page 5-70
management frame validation 5-67
management interface
configuring
using the CLI 3-13
using the GUI 3-11 to 3-12
described 3-6
management over wireless
described 5-52
enabling
using the CLI 5-52
using the GUI 5-52
Master Controller Configuration page 7-4
Master Controller Mode parameter 7-4
Max Age parameter 3-27
Maximum Age parameter 3-28
maximum local database entries
configuring using the CLI 5-122
configuring using the GUI 5-122
Maximum Local Database Entries parameter 5-30, 5-122
Maximum RF Usage Per AP parameter 4-46
Max-Login Ignore Identity Response parameter 5-41
Max RF Bandwidth parameter 4-55, 4-56
MCS data rates 4-18
Member MAC Address parameter 12-12
memory
types 1-15
memory leaks, monitoring D-17 to D-19
mesh
network example 8-34
parameters
configuring using the CLI 8-20, 8-24
configuring using the GUI 8-16 to 8-20
statistics
viewing for an access point using the CLI 8-34 to 8-37, 8-43 to 8-44
viewing for an access point using the GUI 8-39 to 8-43
Mesh > LinkTest Results page 8-45
mesh access points
converting to non-mesh access points 8-50
operating with Cisco 3200 Series Mobile Access Routers
configuration guidelines 8-51
described 8-51
using the CLI to configure 8-53
using the GUI to configure 8-52
mesh access points (MAPs)
selecting 8-29
mesh network hierarchy 8-3
mesh node security statistics 8-42 to 8-43
mesh node statistics 8-41
Message Authentication Code Key (MACK) parameter 5-8, 5-12
message logs
configuring
using the CLI D-10 to D-12
using the GUI D-6
viewing
using the CLI D-12
using the GUI D-9 to D-10

See also system logging

Message Logs page D-9

Message parameter for web authentication 10-11

Metrics Collection parameter 4-55

MFP Client Protection parameter 5-69

MFP Frame Validation parameter 5-69

MIC 6-22, 6-25

migrating access points from the -J to the -U regulatory domain 7-55 to ??

Min Failed Client Count per AP parameter 11-16

Minimum RSSI parameter 4-42

mirror mode. *See* port mirroring, configuring

MMH MIC

- configuring 6-26, 6-27
- described 6-25

MMH Mode parameter 6-26

Mobile Announce messages 12-7

mobility

- failover 12-20
- overview 12-2

Mobility Anchor Config page 12-22, 12-27

Mobility Anchor Create button 12-23

mobility anchors. *See* auto-anchor mobility

Mobility Anchors option 12-22

Mobility Anchors page 12-22

Mobility Group Member > New page 12-11

Mobility Group Members > Edit All page 12-13

mobility groups

- configuring
  - using the CLI 12-14
  - using the configuration wizard 4-5
  - using the GUI 12-11 to 12-13
  - with one NAT device 12-8
  - with two NAT devices 12-9
- determining when to include controllers 12-7
- difference from RF groups 11-5
- examples 12-7
- illustrated 12-5
- messaging among 12-7
- number of access points supported 12-5, 12-6
- number of controllers supported 12-5
- prerequisites 12-9 to 12-10
- using with NAT devices 12-8 to 12-9

mobility group statistics

- types 12-16
- viewing
  - using the CLI 12-19
  - using the GUI 12-16 to 12-19

mobility list

- described 12-6
- detecting failed members 12-20
- number of controllers supported 12-7
- ping requests to members 12-20

Mobility Multicast Messaging > Edit page 12-14

Mobility Multicast Messaging page 12-13

mobility ping tests, running 12-28

mobility services information, viewing 4-89

Mobility Statistics page 12-17

MODE access point button 7-17, 7-33

Mode parameter 4-42, 11-38

monitor intervals, configuring using the GUI 11-19

mpings 12-23, 12-28

Multicast Appliance Mode parameter 3-22

multicast client table, viewing 4-39

multicast groups

- viewing using the CLI 4-39
- viewing using the GUI 4-37

Multicast Groups page 4-37

multicast mode

- configuring
  - using the CLI 4-38
  - using the GUI 4-36 to 4-37
- described 4-34 to 4-35
- guidelines 4-35 to 4-36, 7-35

Multicast page 4-37

multiple country codes

- configuration guidelines 7-49
- configuring

using the CLI 7-52

using the GUI 7-51

multiple country support, using the configuration wizard 4-5

N

NAC in-band mode 6-55

NAC out-of-band integration

and hybrid REAP 13-5

configuring

using the CLI 6-60 to 6-61

using the GUI 6-57 to 6-60

described 6-55 to 6-56

diagram 6-56

guidelines 6-56 to 6-57

NAC out-of-band support

configuring for a specific access point group

using the CLI 6-61

using the GUI 6-59

NAC State parameter 6-46, 6-59, 6-60

NAT devices in mobility groups 12-8 to 12-9

Native VLAN ID parameter 13-13

neighbor information

viewing for an access point using the CLI 8-47

viewing for an access point using the GUI 8-44 to 8-47

Neighbor Information option 8-44

Neighbor Packet Frequency parameter 11-19

neighbor statistics

viewing for an access point using the CLI 8-47

viewing for an access point using the GUI 8-44 to 8-47

Netbios Name Servers parameter 6-12

Netmask parameter 6-12

network analyzer supported software

AirMagnet D-39

Airopeek D-39

Omnipeek D-39

Wireshark D-39

Network Mobility Services Protocol (NMSP) 4-80

active connections 4-88

modifying the notification interval for clients, RFID tags, and rogues 4-85

viewing counters 4-88

Network parameter 6-12

notes xxv

NTP server

configuring to obtain time and date 4-10

setting in the configuration wizard 4-6

Number of Hits parameter 5-58

O

online help, using 2-2

open source terms C-8

OpenSSL license issues C-6 to C-8

operating system

security 1-5

software 1-4

organization of document xxiv to xxv

Override Global Config parameter 10-21, 10-28

Over-ride Global Credentials parameter 7-7, 7-11, 7-12

Override Interface ACL parameter 5-62

oversized access point images 7-33

over-the-air provisioning (OTAP) 7-3

P

P2P Blocking parameter 6-19

Params parameter 7-19

password

restoring 4-24

password guidelines 7-11

Password parameter

for access point authentication 7-11

for access points 7-7

for local net users 5-31, 13-10

for PACs 9-19

passwords

viewing in clear text D-6

PEAP parameter 5-42

peer-to-peer blocking

configuring

using the CLI 6-20

using the GUI 6-19 to 6-20

described 6-18

examples 6-18

guidelines 6-19, 6-56

Physical Mode parameter 3-21

Physical Status parameter 3-20

pico cell mode

configuring

using the CLI 11-44 to 11-45

using the GUI 11-42 to 11-44

debugging using the CLI 11-45

guidelines 11-42

overview 11-41 to 11-42

versions 11-43

Pico Cell Mode parameter 11-43

ping link test 7-64

ping tests 12-28

PMK cache lifetime timer 6-24

PMKID caching 6-25

PoE Status parameter 7-72

Pool End Address parameter 6-12

Pool Start Address parameter 6-12

Port > Configure page 3-20

port mirroring, configuring 3-22 to 3-23

Port Number parameter

for controller 3-20

for LDAP server 5-34

for RADIUS server 5-8

for TACACS+ server 5-24

for wired guest access 10-26

Port parameter for IDS 5-104

ports

configuring 3-19 to 3-29

on 2100 series controllers 3-2, 3-3, 3-4

on 4400 series controllers 3-2, 3-3, 3-4

on Catalyst 3750G Integrated Wireless LAN Controller Switch 3-3, 3-5

on Cisco 28/37/38xx Series Integrated Services Router 3-3 to 3-4, 4-91, 7-25

on Cisco WiSM 3-3, 3-4

overview 3-2 to 3-5

Ports page 3-19

Power Assignment Leader parameter 11-11

power cable warning for Japan B-7

Power Injector Selection parameter 7-72

Power Injector State parameter 7-72

Power Neighbor Count parameter 11-11

Power over Ethernet (PoE)

configuring

using the CLI 7-73

using the GUI 7-71 to 7-73

described 1-14, 7-70

Power Over Ethernet (PoE) parameter 3-21

Power Threshold parameter 11-11

preauthentication access control list (ACL)

applying to a WLAN

using the CLI 5-65

using the GUI 5-62 to 5-63

for external web server 10-16, 13-9

Preauthentication ACL parameter 5-63, 6-52

Pre-Standard State parameter 7-72

Primary Controller parameters 7-43

Primary RADIUS Server parameter 13-18

priming access points 7-3

Priority Order > Local-Auth page 5-35, 5-40

Priority Order > Management User page 5-11, 5-25

Priority parameter 3-28

Privacy Protocol parameter 4-28

probe request forwarding, configuring 7-62

probe requests, described 7-62

Profile Details page D-28

Profile Name parameter 6-5, 8-12, 10-27, 13-7

protected access credentials (PACs)

overview 9-19
uploading
using the CLI 9-20 to 9-21
using the GUI 9-19
using with local EAP 5-40, 13-21
Protection Type parameter 5-68, 11-35
Protocol parameter 5-57
Protocol Type parameter 4-47
PSK
configuring 6-24
described 6-22
with mesh 8-18
PSK Format parameter 6-24
public key cryptography (PKC), with mobility 12-7
purpose of document xxiv

Q

QBSS
configuring
using the CLI 6-36
using the GUI 6-35
described 6-32
guidelines 6-34
QoS
identity networking 5-75
levels 4-45, 6-30
translation values 6-31
with CAC 4-52
QoS profiles
assigning to a WLAN
using the CLI 6-32
using the GUI 6-31 to 6-32
configuring
using the CLI 4-47 to 4-48
using the GUI 4-45 to 4-47
QoS roles
assigning for use with hybrid REAP 13-10
configuring
using the CLI 4-50 to 4-51
using the GUI 4-48 to 4-50
QoS Roles for Guest Users page 4-49
Quality of Service (QoS) parameter 6-31
quarantined VLAN
configuring 3-11, 3-17
using 13-8
with hybrid REAP 13-4
with NAC out-of-band integration 6-58
Quarantine parameter
for dynamic interface 3-17
for management interface 3-11
NAC out-of-band integration 6-58
Query Interval parameter 5-104
Queue Depth parameter 4-46
queue statistics 8-41

R

radio core dumps
described 7-28
retrieving 7-29
uploading
using the CLI 7-30
using the GUI 7-29 to 7-30
radio measurement requests
configuring
on the CLI 11-39
on the GUI 11-38
overview 11-37
viewing status using the CLI 11-40
radio preamble 5-50
radio resource management (RRM)
benefits 11-5
CCX features. *See*CCX radio management
configuring
monitor intervals using the GUI 11-19
using the CLI 11-19 to 11-22
using the configuration wizard 4-6

using the GUI 11-9 to 11-19
coverage hole detection
configuring per controller using the CLI 11-21
configuring per controller using the GUI 11-15 to 11-17
described 11-4
debugging 11-25
disabling dynamic channel and power assignment
using the CLI 11-33
using the GUI 11-33
overriding RRM 11-25 to 11-33
overview 11-2
specifying channels 11-12 to 11-14
statically assigning channel and transmit power settings
using the CLI 11-30
using the GUI 11-26 to 11-30
update interval 11-6, 11-9
viewing using the CLI 11-23 to 11-24
Wireless > 802.11a/n (or 802.11b/g/n) > RRM > TPC parameter 11-10
radio resource monitoring 11-2
RADIUS
accounting 5-3
authentication 5-3
configuring
using the CLI 5-11 to 5-14
using the GUI 5-6 to 5-11
configuring on ACS 5-4
described 5-3
FIPS standard 5-11
KEK parameter 5-12
MACK parameter 5-12
server fallback behavior 5-10
using with hybrid REAP 13-16
RADIUS accounting attributes 5-17 to 5-18
Range (RootAP to MeshAP) parameter 8-17
Redirect URL After Login parameter 10-10
Refresh-time Interval parameter 4-72
regulatory information
for 2100 series controllers B-10
for 4400 series controllers B-10
for lightweight access points B-2 to B-10
related publications xxvii
Remote Authentication Dial-In User Service. *See* RADIUS
Request Max Retries parameter 5-41
Request Timeout parameter 5-41
Reserved Roaming Bandwidth parameter 4-55, 4-56
Reset Link Latency button 7-69
resetting the controller 9-28
restoring passwords 4-24
Re-sync button 5-106
reverse path filtering (RPF) 12-26
RF Channel Assignment parameter 11-33
RF domain. *See* RF groups
RF exposure declaration of conformity B-5
RF group leader
described 11-6
viewing 11-8
RF group name
described 11-6
entering 11-7
RF groups
configuring
using the CLI 11-7
using the configuration wizard 4-5
using the GUI 11-7
difference from mobility groups 11-5
overview 11-5 to 11-6
viewing status
using the CLI 11-9
using the GUI 11-8
RFID tags
described 4-79
formats supported 4-79
number supported per controller 4-80
tracking
configuring using the CLI 4-81
debugging using the CLI 4-83

viewing information using the CLI 4-82 to 4-83

RFID tracking on access points, optimizing

using the CLI 7-61 to 7-62

using the GUI 7-59 to 7-61

RF-Network Name parameter 11-7

RLDP. *See* Rogue Location Discovery Protocol (RLDP)

roaming and real-time diagnostics

configuring using the CLI D-31 to D-34

described D-20

logs

described D-20

viewing D-31 to D-32

roam reason report 4-41

roam reason report, described 8-25

rogue access points

alarm 11-35

automatically containing

using the CLI 5-86

using the GUI 5-85

classification mapping table 5-82

classifying 5-81

configuring RLDP 5-84 to 5-87

detecting

using the CLI 11-36

using the GUI 11-34 to 11-35

managing 5-80

rule-based classification support 5-81

tagging, location, and containment 5-81

viewing and classifying

using the CLI 5-98 to 5-102

using the GUI 5-93 to 5-98

WCS support for rule-based classification 5-84

Rogue AP Detail page 5-94

Rogue AP Ignore-List page 5-97

rogue classification rules

configuring using the CLI 5-90 to 5-93

configuring using the GUI 5-87 to 5-90

Rogue Client Detail page 5-95

Rogue Location Discovery Protocol (RLDP)

configuring

using the CLI 5-85 to 5-87

using the GUI 5-84 to 5-85

defined 5-81

Rogue Location Discovery Protocol parameter 5-84

Rogue on Wire parameter 5-85

Rogue Policies page 5-84

Rogue Rule > Edit page 5-89

Rogue Rules > Priority page 5-90

rogue states 5-82, 5-83

Role Name parameter 4-49

Role parameter 5-31, 13-10

root access points (RAPs)

selecting 8-29

root bridge 3-23

Root Cost parameter 3-27

Root Port parameter 3-27

RRM. *See* radio resource management (RRM)

RSNA logs

configuring D-31 to D-33

described D-20

Rx Sensitivity Threshold parameter 11-44

S

safety warnings A-1 to A-26

Save and Reboot button 9-14, 9-17

saving configuration settings 9-26

Scan Threshold parameter 4-42

Scope Name parameter 6-11

Search Clients page 7-76

Search WLANs window 6-7

Secondary Controller parameters 7-43

Secondary RADIUS Server parameter 13-18

secure web mode

described 2-2

enabling

using the CLI 2-4

using the GUI 2-3

security
- overview 5-2
- solutions 5-2 to 5-3

Security Mode parameter 8-18

Security Policy Completed parameter 6-38

security settings
- local and external authentication 8-16

Select APs from Current Controller parameter 13-19

self-signed certificate (SSC)
- used to authorize access points 7-18

Sequence parameter 5-56

serial port
- baud rate setting 2-8
- connecting 2-8
- timeout 2-8

Server Address parameter 5-104

Server Index (Priority) parameter 5-8, 5-24, 5-34

Server IP Address parameter
- for LDAP server 5-34
- for RADIUS server 5-8
- for TACACS+ server 5-24
- for wireless sniffer D-41

Server Key parameter 5-44, 13-21

Server Status parameter 5-9, 5-24

Server Timeout parameter 5-9, 5-25, 5-35

service port 3-5

service-port interface
- configuring
  - using the CLI 3-15
  - using the configuration wizard 4-4
  - using the GUI 3-10 to 3-12
- described 3-8

session timeout
- configuring
  - using the CLI 6-28
  - using the GUI 6-27
- described 6-27

Set to Factory Default button 11-19

Severity Level Filtering parameter D-7

Shared Secret Format parameter 5-8, 5-24

Shared Secret parameter 5-8, 5-24

Short Preamble Enabled parameter 5-50

short preambles 5-50

Show Wired Clients option 7-38

shunned clients
- described 5-106
- viewing
  - using the CLI 5-107
  - using the GUI 5-106

Signature Events Detail page 5-114

Signature Events Summary page 5-114

Signature Events Track Detail page 5-115

Simple Bind parameter 5-34

sniffing. *See* wireless sniffing D-39

Sniff parameter D-41

SNMP, configuring 4-24 to 4-25

SNMP community string
- changing default values using the CLI 4-27
- changing default values using the GUI 4-25 to 4-26

SNMP v1 / v2c Community > New page 4-26

SNMP v1 / v2c Community page 4-25

SNMP v3 users
- changing default values using the CLI 4-29
- changing default values using the GUI 4-27 to 4-29

SNMP V3 Users > New page 4-28

SNMP V3 Users page 4-27

software, upgrading
- guidelines 9-2 to 9-3
- using the CLI 9-10 to 9-12
- using the GUI 9-8 to 9-10

Source parameter for ACLs 5-56

Source Port parameter 5-57

Spanning Tree Algorithm parameter 3-28

Spanning Tree Protocol (STP)
- configuring
  - using the CLI 3-28 to 3-29
  - using the GUI 3-24 to 3-28
- described 3-23

spanning-tree root 3-23

Spanning Tree Specification parameter 3-27

SpectraLink NetLink phones

enabling long preambles

using the CLI 5-51

using the GUI 5-50

overview 5-50

Spectralink Voice Priority parameter 4-67

splash page web redirect 6-50

Splash Page Web Redirect parameter 6-52

SSC key-hash on Cisco WiSM 7-16

SSH, troubleshooting access points D-42

SSID

configuring

using the CLI 6-6

using the GUI 6-5

described 6-3

SSL certificate

generating

using the CLI 2-4

using the GUI 2-3

loading

using the CLI 2-6 to 2-7

using the GUI 2-5 to 2-6

SSL protocol 2-2

SSLv2, configuring for web administration 2-4

SSLv2 for web authentication, disabling 10-9

Standard Signature > Detail page 5-113

Standard Signatures page 5-111

State parameter 5-104, 5-114

Static Mobility Group Members page 12-11

Statistics option 8-40

Status parameter

for DHCP scopes 6-12

for guest LANs 10-27

for SNMP community 4-26

for WLANs 6-5

STP Mode parameter 3-25

STP Port Designated Bridge parameter 3-25

STP Port Designated Cost parameter 3-25

STP Port Designated Port parameter 3-25

STP Port Designated Root parameter 3-24

STP Port Forward Transitions Count parameter 3-25

STP Port ID parameter 3-24

STP Port Path Cost Mode parameter 3-25

STP Port Path Cost parameter 3-26

STP Port Priority parameter 3-25

STP State parameter 3-24

strong passwords 7-11

Supervisor 720

configuring 4-89 to 4-91

described 4-89

switch, configuring at the remote site 13-5 to 13-6

Switch IP Address (Anchor) parameter 12-23

SX/LC/T small form-factor plug-in (SFP) modules 3-4

symmetric mobility tunneling

configuring

using the configuration wizard 4-5

illustrated 12-27

overview 12-26 to 12-27

verifying status

using the CLI 12-28

using the GUI 12-27

Symmetric Mobility Tunneling Mode parameter 12-27

syslog

described D-20

levels D-8

logs D-31 to D-33

Syslog Configuration page D-7

Syslog Facility parameter D-8

syslog server

number supported by controller D-7

removing from controller D-7

severity level filtering D-7

Syslog Server IP Address parameter D-7

system logging

configuring

using the CLI D-10 to D-12

using the GUI D-6 to D-9

setting severity level D-8

system logs, viewing using the CLI D-12

system messages D-2 to D-5

T

TACACS+

accounting 5-19

authentication 5-18

authorization 5-18

choosing authentication priority order 5-11, 5-25

configuring

using the CLI 5-25 to 5-27

using the GUI 5-23 to 5-25

configuring on ACS 5-19 to 5-23

described 5-18 to 5-19

roles 5-18, 5-22

viewing administration server logs 5-27 to 5-29

TACACS+ (Authentication, Authorization, or Accounting) Servers > New page 5-24

TACACS+ (Authentication, Authorization, or Accounting) Servers page 5-23

TACACS+ (Cisco) page (on CiscoSecure ACS) 5-21

TACACS+ Administration .csv page (on CiscoSecure ACS) 5-28, 5-29

telemetry 4-79

Telnet, troubleshooting access points D-42

terminal emulator settings 2-8

Tertiary Controller parameters 7-44

text2pcap sample output D-37

TFTP server guidelines 9-2

time, configuring

using the CLI 4-11

using the GUI 4-10

using the NTP server 4-10

time-length-values (TLVs), supported for CDP 4-69 to 4-71

timeout, configuring for disabled clients 6-15

Time Since Topology Changed parameter 3-27

timestamps, enabling or disabling in log and debug messages D-12

Time to Live for the PAC parameter 5-44, 13-21

time zone

configuring using the CLI 4-12

configuring using the GUI 4-11

TKIP

configuring 6-23, 6-24

described 6-22

parameter 6-23

Topology Change Count parameter 3-27

traffic specifications (TSPEC) request

described 4-53

examples 4-53

traffic stream metrics (TSM)

configuring

using the CLI 4-63

using the GUI 4-55

described 4-54

viewing statistics

using the CLI 4-65 to 4-66

using the GUI 4-59 to 4-62

Transfer Mode parameter

downloading a CA certificate 9-17

downloading a configuration file 9-24

downloading a customized web authentication login page 10-18

downloading a device certificate 9-14

upgrading controller software 9-9

uploading a configuration file 9-22

uploading a PAC 9-20

Transition Time parameter 4-43

transmit power

statically assigning using the CLI 11-30

statically assigning using the GUI 11-26 to 11-30

transmit power levels 11-29

Transmit Power parameter 11-44

transmit power threshold, decreasing 11-20

troubleshooting

access point join process 7-24 to 7-28
CCXv5 clients D-19 to D-34
problems D-5 to D-6
using Telnet or SSH D-42
tunnel attributes and identity networking 5-77
Tx Power Level Assignment parameter 11-33
Type parameter 6-4, 10-27, 13-7

U

U-APSD
described 4-54
viewing status
using the CLI 4-65
using the GUI 4-58
UDP, use in RADIUS 5-4
UDP port 12-23, 12-28
unicast mode 4-34
unique device identifier (UDI)
described 7-63
retrieving
using the CLI 7-64
using the GUI 7-63 to 7-64
Upload button 5-111, 7-30, 9-20, D-15
Upload CSV File parameter 13-20
Upload File from Controller page 7-29, 9-19, 9-21, D-15
URL parameter 10-17
Use AES Key Wrap parameter 5-7
User Access Mode parameter 10-3
user accounts, managing 10-1 to 10-20
User Attribute parameter 5-34
User Base DN parameter 5-34
User Credentials parameter 5-35
User Name parameter 5-31, 13-10
Username parameter 7-7, 7-10, 7-11
User Object Type parameter 5-34
User parameter 9-19
User Profile Name parameter 4-28
Using Our SSID parameter 5-85

V

Validate Rogue Clients Against AAA parameter 5-85
Valid Client on Rogue AP parameter 5-85
Validity parameter 9-19
VCCI warnings for controllers B-7
VCI strings 7-24
Verify Certificate CN Identity parameter 5-43
video information, viewing for mesh networks using the CLI 8-34 to 8-37
video settings
configuring
using the CLI 4-63
using the GUI 4-56 to 4-57
viewing
using the CLI 4-64 to 4-66
using the GUI 4-57 to 4-62
virtual interface
configuring
using the CLI 3-14
using the configuration wizard 4-5
using the GUI 3-10 to 3-12
described 3-7 to 3-8
VLAN Identifier parameter
for AP-manager interface 3-12
for dynamic interface 3-16, 3-17
for management interface 3-11
VLAN ID parameter 6-57, 13-13
VLAN interface. *See* dynamic interface
VLAN Mappings
button 13-13
page 13-13
VLANs
described 3-8
guidelines 3-10
VLAN Support parameter 13-13
VLAN tag, and identity networking 5-76
Voice & Video Optimized parameter 4-67

voice information, viewing for mesh networks using the CLI 8-34 to 8-37

Voice Optimized parameter 4-67

voice-over-IP (VoIP) telephone roaming 4-40

Voice RSSI parameter 11-16

voice settings

- configuring
  - using the CLI 4-62 to 4-63
  - using the GUI 4-54 to 4-55
- viewing
  - using the CLI 4-64 to 4-66
  - using the GUI 4-57 to 4-62

VPN Gateway Address parameter 6-29

VPN passthrough

- configuring using the CLI 6-29
- configuring using the GUI 6-29

W

warnings

- defined xxvi to xxvii
- translated A-1 to A-26

warranty C-4 to C-6

webauth.tar files 10-21

webauth bundle 10-17

web authentication

- configuring a WLAN for
  - using the CLI 6-30
  - using the GUI 6-29
- described 10-7
- process 10-7 to 10-9
- successful login page 10-9

web authentication login page

- assigning per WLAN
  - using the CLI 10-22
  - using the GUI 10-21
- choosing the default
  - using the CLI 10-11 to 10-12
  - using the GUI 10-10 to 10-11
- customized example 10-20
- customizing from an external web server
  - using the CLI 10-17
  - using the GUI 10-16 to 10-17
- default 10-8
- downloading a customized login page
  - guidelines 10-17
  - using the CLI 10-19
  - using the GUI 10-18 to 10-19
- modified default example 10-13
- previewing 10-11, 10-19
- verifying settings using the CLI 10-20

Web Authentication option 10-28

Web Authentication Type parameter 10-10, 10-17, 10-19

Web Auth Type parameter 10-21, 10-28

web-browser security alert 10-7

Web Login page 10-10, 10-16

web mode

- configuring
  - using the CLI 2-4
  - using the GUI 2-3
- described 2-2

Web Passthrough option 10-28

Web Policy parameter 5-63, 6-52

web redirect 6-49

Web Server IP Address parameter 10-17

Web Session Timeout parameter 2-3

WEP keys, configuring 6-21

WGB parameter 7-38

WGB Wired Clients page 7-38

wired guest access

- configuration overview 10-25
- configuring
  - using the CLI 10-29 to 10-34
  - using the GUI 10-25 to 10-29
- described 10-23 to 10-25
- guidelines 10-25
- one-controller example 10-24
- two-controller example 10-24

wireless intrusion prevention system (wIPS)
configuring on an access point 5-119 to 5-120
described 5-119
viewing information 5-120 to 5-121
wireless sniffing
configuring
using the CLI D-41
using the GUI D-39 to D-41
prerequisites D-39
supported software D-39
WLAN ID parameter 6-5
WLAN Profile parameter 5-31, 13-10
WLANs
assigning web login, login failure, and logout pages
using the CLI 10-22
using the GUI 10-21
checking security settings 6-21
configuring
conditional web redirect 6-50 to 6-53
static and dynamic WEP 6-22
connecting clients to 13-15
creating
using the CLI 6-5
using the GUI 6-3 to 6-5
deleting
using the CLI 6-6
using the GUI 6-4
described 1-12, 3-9 to 3-10, 6-3
enabling or disabling
using the CLI 6-6
using the GUI 6-5
number supported 6-2
searching 6-7
session timeout
configuring 6-27
described 6-27
splash page web redirect 6-50
wired security solution 1-5
WLANs > Edit (Advanced) page 6-54
applying an ACL to a WLAN 5-62
configuring AAA override 5-80
configuring infrastructure MFP for a WLAN 5-69
configuring IPv6 bridging 6-39
configuring NAC out-of-band integration 6-59
configuring the diagnostic channel D-20
WLANs > Edit (QoS) page 6-35
WLANs > Edit (Security > AAA Servers) page
assigning LDAP servers to a WLAN 5-36
choosing RADIUS or LDAP servers for external authentication 10-21
disabling accounting servers on a WLAN 6-53
enabling local EAP on a WLAN 5-45
WLANs > Edit (Security > Layer 2) page 6-23, 6-26
WLANs > Edit (Security > Layer 3) page
applying a preauthentication ACL to a WLAN 5-62
configuring a WLAN for VPN Passthrough 6-29
configuring web redirect 6-52
configuring wired guest access 10-28
WLANs > Edit page 6-5, 10-27, 13-7
WLANs > New page 6-4, 8-25, 8-26, 8-46, 8-47, 10-27, 13-7
WLANs page 6-3, 12-22
WLAN SSID parameter
configuring for guest user 10-5
creating a centrally switched WLAN 13-7
creating WLANs 6-5
identifying the guest LAN 10-27
mapping an access point group to a WLAN 6-46, 6-60
WMM
configuring 4-19, 6-35, 6-36
described 6-32
with CAC 4-52
WMM parameter 4-67
WMM Policy parameter 6-35
workgroup bridges (WGBs)
debugging 7-40
described 7-34
guidelines 7-35
illustrated 7-34

sample configuration 7-37

viewing status

using the CLI 7-40

using the GUI 7-37 to 7-39

world mode 4-15, 4-16

WPA1+WPA2

configuring

using the CLI 6-24

using the GUI 6-23 to 6-24

described 6-22

WPA2 Policy parameter 6-23

WPA Policy parameter 6-23