User Manual

Allen-Bradley

Stratix 5100 Wireless Access Point/Workgroup Bridge

Catalog Numbers 1783-WAPAK9, 1783-WAPBK9, 1783-WAPCK9, 1783-WAPEK9, 1783-WAPNK9, 1783-WAPTK9, 1783-WAPZK9

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

	**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.
	**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.

	**SHOCK HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.
	**BURN HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.
	**ARC FLASH HAZARD:** Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

Summary of Changes

New and Updated Information 15

Preface

Audience 17
Purpose 17
Organization 18
Conventions 19
Additional Resources 19
Rockwell Automation Support 20

Chapter 1

Get Started with the Stratix 5100 Wireless Access Point/Workgroup Bridge

Regulatory Domains 23
Support for -B Domain FCC (USA) Rule 23
Configure the Access Point 24
Management Options 24
Roaming Client Devices 24
Network Configuration Examples 25
Root Access Point 25
Workgroup Bridge 25
Repeater Access Point 26
Unpack the WAP 27
Items Shipped with the WAP 27

Chapter 2

Install the Stratix 5100 Wireless Access Point/Workgroup Bridge

Prepare the Access Point 30
Prevent Damage to the WAP 30
Ports and Connections 31
Install the WAP 31
Ethernet Cable Recommendation 32
Access Point Spacing Recommendation 32
IDF Closets (telecommunications or other electrical equipment) 32
Very High Altitudes 32
Common or Distributed Antenna System (DAS) 33
Mount the Access Point 33
Ground the Access Point 36
Secure the Access Point 37
Secure the Access Point to the Mounting Plate 37
Security Cable 38
Stratix 5100 WAP Specifications 38
External Antennas 39
Antenna Cable Recommendation 39
Stratix 5100 WAP Status Indicators 42
Configure the Access Point 43

Chapter 3

Stratix 5100 Device Manager Configuration Startup

Device Manager 46
Before You Start 47
Connect to the Stratix 5100 WAP Access Point Locally 47
Obtain and Assign an IP Address 48
    Default IP Address Behavior 48
Login to the Stratix 5100 WAP 48
Default Radio Settings 48
Reset the WAP to Default Settings 49
    Reset to WAP Default Settings by Using the MODE Button . . 49
    Reset to Default Settings by Using the GUI 49
Online Help 51
Configure the Basic Settings for an Access Point 51
Enable the Radio on the Network 55
VLANs 57
Configure Security 58
    Easy Set-up Page Security Types 59
    Easy Setup Network Configuration Security Limitations 59
    Create an SSID from the Security Menu 60
    Enable HTTPS for Secure Browsing 62
CLI Configuration Example 66
Delete an HTTPS Certificate 66
Disable the Web Browser Interface 66

Chapter 4

Stratix 5100 Device Manager Parameter Definitions

Device Manager System Management Tabs 71
Easy Setup Network Configuration Page 72
    Network Configuration Settings on the Easy Setup Page 73
    Radio Configuration Settings on the Easy Setup Page 75
    Security Configuration Settings on the Easy Setup Page 78
Network Page 79
    Network Interface Summary Page 80
    Network Interface IP Address Page 83
    Network Interface GigabitEthernet Status Page 84
    Network Interface: GigabitEthernet Settings 87
    Network Interface: Radio0-802.11n 2 GHz and Radio1-802.11n 5 GHz Status 88
    Detailed Status 90
    Network Interface Radio Settings Page 92
    Carrier Busy Test 97
Association Page 97
Wireless Page 99
    AP 99
    WDS 100
Security Page 104
    Admin Access Page 106

Encryption Manager Page 107
SSID Manager Page 109
Server Manager Page 115
Server Manager Global Properties 117
AP Authentication 119
AP Authentication Certificates 121
Intrusion Detection 123
Local RADIUS Server 125
Advanced Security 128
Services Page 131
Telnet/SSH 131
Hot Standby Page 133
CDP Page 134
DNS Page 136
Filters Page 137
MAC Address Filters Page 138
IP Filters Page 140
Ethertype Filters Page 142
HTTP Page 143
QoS Policies Page 145
QoS: Radio Page 147
Stream Page 150
SNMP Page 151
SNTP Page 154
VLAN Page 155
ARP Caching Page 157
Band Select Page 158
Management Page 160
Webauth Login 161
Software Page 162
Software Upgrade HTTP Page 163
Software Upgrade TFTP Page 164
System Configuration Page 165
Event Log Page 167
Configuration Options Page 169

Chapter 5

Access the Stratix 5100 Wireless Access Point/Workgroup Bridge in Logix Designer

General Dialog Box 172
Connection Dialog Box 174
Module Information Dialog Box 175
Internet Protocol Configuration Dialog Box 177
Access Point Dialog Box 180
Access Point Parameters 180
Service Set Identifiers (SSID) Dialog Box 181
Event Log Dialog Box 182
Radios Dialog Box 183
2.4 GHz or 5 GHz Radio Dialog Box 184

Counters Dialog Box 186
Statistics Per Rate Dialog Box. 188
Module-Defined Data Types 189
Save/Restore Dialog Box 190

Chapter 6

Configure the Stratix 5100 WAP Using the Command-Line Interface

Cisco IOS Command Modes. 191
Get Help 192
Abbreviate Commands 193
Use No and Default Forms of Commands. 193
Understand CLI Messages 194
Command History 194
Change the Command History Buffer Size 194
Recall Commands 195
Disable the Command History Feature. 195
Use Editing Features. 195
Enable and Disable Editing Features 195
Edit Commands by Using Keystrokes 196
Edit Command Lines that Wrap. 197
Search and Filter Output of show and more Commands. 198
Access CLI 198
Open CLI with Telnet 198
Open CLI with Secure Shell. 199
Reset Default Settings by Using CLI 199
Security CLI Configuration Examples 200
Example 1: No Security 200
Example 2: WPA with Pre-shared Keys (WPA2-PSK) 201
Example 3: WPA and EAP 204
Assign an IP Address by Using CLI 206
Configure the 802.1X Supplicant. 206
Create a Credentials Profile 208
Apply the Credentials Profile to an SSID Used for the Uplink 209
Create and Apply EAP Method Profiles 210

Chapter 7

Administer the WAP Access

Disable the Mode Button 212
Prevent Unauthorized Access to Your Access Point 213
Protect Access to Privileged EXEC Commands 213
Default Password and Privilege Level Configuration 214
Set or Change a Static Enable Password 214
Protect Enable and Enable Secret Passwords with Encryption 215
Configure Username and Password Pairs 216
Configure Multiple Privilege Levels 218
Set the Privilege Level for a Command 218
Log Into and Exiting a Privilege Level 219

Control Access Point Access with RADIUS 219
Default RADIUS Configuration. 220
Configure RADIUS Login Authentication 220
Define AAA Server Groups 222
Configure RADIUS Authorization for User Privileged Access and Network Services 224
Display the RADIUS Configuration 225
Control Access Point Access with TACACS+. 226
Default TACACS+ Configuration 226
Configure TACACS+ Login Authentication 226
Configure TACACS+ Authorization for Privileged EXEC Access and Network Services 228
Display the TACACS+ Configuration 229
Configure Ethernet Speed and Duplex Settings 229
Configure the Access Point for Local Authentication and Authorization. 230
Configure the Authentication Cache and Profile. 232
Configure the Access Point to Provide DHCP Service. 236
Set up the DHCP Server 236
Monitor and Maintain the DHCP Server Access Point 238
Show Commands. 238
Clear Commands. 238
Debug Command 238
Configure the Access Point for Secure Shell 239
Understand SSH 239
Configure SSH. 239
Configure Client ARP Caching 240
Optional ARP Caching 240
Configure ARP Caching 240
Manage the System Time and Date 241
Configure SNTP 242
Configure Time and Date Manually. 242
Set the System Clock. 242
Display the Time and Date Configuration 243
Configure the Time Zone 243
Configure Summer Time (Daylight Saving Time) 244
Define HTTP Access. 246
Configure a System Name and Prompt. 246
Default System Name and Prompt Configuration. 247
Configure a System Name. 247
Understand DNS 248
Default DNS Configuration. 248
Set Up DNS 248
Display the DNS Configuration 250

Chapter 8

Configure Radio Settings

Enable the Radio Interface 252
Configure the Role in Radio Network. 252
Universal Workgroup Bridge Mode. 254
Radio Tracking 255
Gigabit Ethernet Tracking 255
MAC-Address Tracking 256
Configure Radio Data Rates. 256
Access Points Send Multicast and Management Frames at Highest Basic Rate. 257
Configuring Data Rates 258
Configure MCS Rates 260
Configure Radio Transmit Power 262
Limit the Power Level for Associated Client Devices 263
Configure Radio Channel Settings. 264
802.11n Channel Widths 264
Dynamic Frequency Selection 265
Radar Detection on a DFS Channel. 267
CLI Commands. 267
Confirm that DFS is Enabled. 267
Configure a Channel 269
Block Channels from DFS Selection 270
Set the 802.11n Guard Interval. 270
Configure Transmit and Receive Antennas. 271
Enable and Disable Gratuitous Probe Response 272
Disable and Enable Aironet Extensions 273
Configure the Ethernet Encapsulation Transformation Method . 274
Enable and Disable Reliable Multicast to Workgroup Bridges 275
Enable and Disable Public Secure Packet Forwarding. 277
Configure the Beacon Period and the DTIM 277
Configure RTS Threshold and Retries 279
Configure the Maximum Data Retries 280
Configuring the Fragmentation Threshold 280
Perform a Carrier Busy Test. 282
Configure ClientLink 282
Use CLI to Configure ClientLink 282
Debug Radio Functions. 283

Chapter 9

Configure Multiple Service Set Identifiers (SSIDs)

Understand Multiple SSIDs. 285
Configure Multiple SSIDs 286
Default SSID Configuration. 286
Create an SSID Globally 286
View SSIDs Configured Globally 289
Restrict SSIDs by Using a RADIUS Server 289
Configure Multiple Basic SSIDs 290

Configuration Requirements for Multiple BSSIDs 291
Guidelines for Multiple BSSIDs 291
Configure Multiple BSSIDs 292
CLI Configuration Example. 294
Display Configured BSSIDs 294
Assign IP Redirection for an SSID 295
Guidelines for Using IP Redirection. 296
Configure IP Redirection 296
Include an SSID in an SSIDL IE. 297

Chapter 10

Configure Spanning Tree Protocol

Spanning Tree Protocol (STP) 299
Configure STP Features 300
Default STP Configuration 301
Configure STP Settings 301
Display Spanning-tree Status 302

Chapter 11

Configure an Access Point as a Local Authenticator

Local Authentication 303
Configure a Local Authenticator 304
Configuration Overview 304
Configure/Enable Local MAC Authentication 305
Configure the SSID. 305
Create Local MAC Address Lists 306
Create and Enable MAC Authentication by
Using RADIUS Server. 307
Add the RADIUS Server 308
Set the MAC Authentication Method. 310
Configure Network EAP 311
Configure Advanced EAP Parameters 314
Configure the Local Authenticator Access Point by Using CLI. . . 315
Configure Other Access Points to Use the Local Authenticator 318
Configure EAP-FAST Settings 320
Configure PAC Settings 320
PAC Expiration Times. 320
Generate PACs Manually 320
Configure an Authority ID. 321
Configure Server Keys 321
Possible PAC Failures Caused by Access Point Clock. 322
Limit the Local Authenticator to One Authentication Type 323
Unblock Locked Usernames 323
View Local Authenticator Statistics 323
Debug Messages. 325

Chapter 12

Configure Cipher Suites

Cipher Suites 327
Configure Cipher Suites 328
Enable Cipher Suites 328
Match Cipher Suites with WPA or CCKM 329
Enable and Disable Broadcast Key Rotation 329

Chapter 13

Configure Authentication Types

Authentication Types 331
Open Authentication to the Access Point 332
Shared Key Authentication to the Access Point 332
EAP Authentication to the Network 332
MAC Address Authentication to the Network 333
Combine MAC-Based, EAP, and Open Authentication 334
Using CCKM for Authenticated Clients 335
WPA Key Management 336
Configure Authentication Types 337
Assigning Authentication Types to an SSID 337
Configure Additional WPA Settings 341
Set a Pre-shared Key 341
Configure Group Key Updates 342
Configure MAC Authentication Caching 343
Configure Authentication Hold-off, Timeout, and Interval 345
Create and Apply EAP Method Profiles for the 802.1X Supplicant 347
Create an EAP Method Profile 347
Apply an EAP Profile to an Uplink SSID 348

Chapter 14

Configure Wireless Domain Services and Fast Secure Roaming

WDS 349
Role of the WDS Device 349
Role of Access Points by Using the WDS Device 350
Fast Secure Roaming 351
Configure WDS 353
Guidelines for WDS 353
Requirements for WDS 353
Configuration Overview 353
Configure Access Points as Potential WDS Devices 355
Configure a Group of Servers 358
Configure Access Points to Use the WDS Device 361
CLI Configuration Example 362
Configure WDS-Only Mode 362
View WDS Information 363
Debug Messages 364
Configure Fast Secure Roaming 364
Requirements for Fast Secure Roaming 364
Configure Access Points to Support Fast Secure Roaming 365

CLI Configuration Example 367
Management Frame Protection 367
Overview 368
Protection of Unicast Management Frames 368
Protection of Broadcast Management Frames 368
Client MFP for Access Points in Root Mode 368
Configure Client MFP 369
Configure an Authentication Failure Limit 370

Chapter 15

Configure RADIUS and TACACS+ Servers

Configure and Enable RADIUS 373
RADIUS Operation 375
Configure RADIUS 375
Default RADIUS Configuration 376
Identify the RADIUS Server Host 376
Configure RADIUS Login Authentication 379
Define AAA Server Groups 381
Configure RADIUS Authorization for User Privileged Access and Network Services 384
Start RADIUS Accounting 385
Select the CSID Format 386
Configure All RADIUS Servers 387
Configure the Access Point to Use Vendor-specific RADIUS Attributes 389
Configure the Access Point for Vendor-proprietary RADIUS Server Communication 390
Display the RADIUS Configuration 391
RADIUS Attributes Sent by the Access Point 392
Configure and Enable TACACS+ 395
TACACS+ Operation 396
Configure TACACS+ 397
Default TACACS+ Configuration 397
Identify the TACACS+ Server Host and Setting the Authentication Key 397
Configure TACACS+ Login Authentication 399
Configure TACACS+ Authorization for Privileged EXEC Access and Network Services 401
Start TACACS+ Accounting 402
Display the TACACS+ Configuration 402

Chapter 16

Configure Virtual Local Area Networks (VLAN)

VLANs 403
Incorporate Wireless Devices into VLANs 405
Configure VLANs 406
Assigning SSIDs to VLANs 406
Assign Names to VLANs 408

Assign Users to VLAN by Using a RADIUS Server 409
View VLANs Configured on the Access Point 410
Configure and Enable a VLAN with SSID by Using Stratix 5100 Device Manager 411
Set the Encryption for the VLAN 413

Chapter 17

Configure Quality of Service (QoS)

QoS for Wireless LANs 415
QoS for Wireless LANs Versus QoS on Wired LANs 416
Impact of QoS on a Wireless LAN 416
Precedence of QoS Settings 417
Configure QoS by Using Stratix 5100 Device Manager 418
Wi-Fi Multimedia Mode 423
Adjust Radio Access Categories 425

Chapter 18

Configure Filters

Filters 429
Configure Filters by Using CLI Commands 430
Create a Time-base ACL 430
Configure Filters by Using Stratix 5100 Device Manager 432
Configure and Enable MAC Address Filters 433
Configure and Enable IP Filters 438
Configure and Enable Ethertype Filters 444

Chapter 19

Configure Cisco Discovery Protocol (CDP)

CDP 447
Configure CDP 448
Default CDP Configuration 448
Configure the CDP Characteristics 448
Disable and Enable CDP 449
Disable and Enable CDP on an Interface 450
Monitor and Maintain CDP 451

Chapter 20

Configure Simple Network Management Protocol (SNMP)

SNMP 453
SNMP Versions 454
SNMP Manager Functions 455
SNMP Agent Functions 455
SNMP Community Strings 456
Access MIB Variables by Using SNMP 456
Configure SNMP 457
Default SNMP Configuration 457
Enable the SNMP Agent 457
Configure Community Strings 457
Specify SNMP-Server Group Names 459

Configure SNMP-Server Hosts 460
Configure SNMP-Server Users 460
Configure Trap Managers and Enabling Traps 460
Set the Agent Contact and Location Information 462
snmp-server view Command 462
SNMP Examples 463
Display SNMP Status 465

Chapter 21

Configure Workgroup Bridge Mode, Repeater Mode, and Standby Access Points

Workgroup Bridge Mode 467
Treat Workgroup Bridges as Infrastructure Devices or as Client Devices 469
Configure a Workgroup Bridge for Roaming 470
Configure a Workgroup Bridge for Limited Channel Scanning . . 470
Configure the Limited Channel Set 470
Ignore the CCX Neighbor List 471
Workgroup Bridge VLAN Tagging 472
Configuring Workgroup Bridge Mode 472
Use Workgroup Bridges in a Lightweight Environment 474
Guidelines for Using Workgroup Bridges in a Lightweight Environment 475
Sample Workgroup Bridge Configuration 477
Repeater Access Points 478
Configure a Repeater Access Point 480
Default Configuration 480
Guidelines for Repeaters 480
Set Up a Repeater 481
Align Antennas 482
Verify Repeater Operation 483
Set Up a Repeater as a WPA Client 483
Hot Standby 484
Configure Hot Standby 485
Configure a Hot Standby Access Point by Using CLI 486
Verify Standby Operation 488

Chapter 22

Configure System Message Logging

System Message Logging 491
Configure System Message Logging 492
Default System Message Logging Configuration 493
Disable and Enable Message Logging 493
Set the Message Display Destination Device 495
Enable and Disable Timestamps on Log Messages 496
Enable and Disable Sequence Numbers in Log Messages 497
Define the Message Severity Level 498
Limit Syslog Messages Sent to the History Table and to SNMP 500

Set a Logging Rate Limit 501
Configure UNIX Syslog Servers 502
Display the Logging Configuration 504

Chapter 23

Troubleshoot

Check the Status Indicators 505
Check Basic Settings 505
SSID 505
Pre-shared Keys 506
Security Settings 506
Reset to the Default Configuration 506
MODE Button 507
Web Browser Interface 507
Set Factory Defaults by Using CLI 508
Reload the Access Point Image 510
HTTP Interface 510
TFTP Interface 511
CLI 513
Obtain TFTP Server Software 515

Appendix A

Supported Management Information Bases (MIBs)

MIB List 517
Access the MIB Files 518

Appendix B

Error and Event Messages

Conventions 519
Software Auto Upgrade Messages 520
Association Management Messages 521
Unzip Messages 521
System Log Messages 522
802.11 Subsystem Messages 522
Inter-Access Point Protocol Messages 527
Local Authenticator Messages 527
WDS Messages 528
Mini IOS Messages 529
Access Point/Bridge Messages 529
Cisco Discovery Protocol Messages 529
External Radius Server Error Messages 530
Sensor Messages 530
SNMP Error Messages 531
SSH Error Messages 531

Glossary

This manual contains new and updated information.

New and Updated Information

This table contains the changes made to this revision.

Topic	Page
Updated the front cover to include the catalog numbers 1783-WAPTK9 (Brazil) and 1783-WAPNK9 (Mexico)	Front cover

Notes:

Audience

This user manual is for the networking professional who installs and manages Stratix® 5100 Wireless Access Points and Workgroup Bridges. To use this guide, you must have some experience working with the Cisco IOS software and be familiar with the concepts and terminology of wireless local area networks.

This user manual covers IOS Release 15.3(3)JC1 that supports the Stratix 5100 WAP, 32 Mb platform.

Purpose

This user manual provides the information you need to install and configure your access point. It provides procedures for using the Cisco IOS software commands that have been created or changed for use with the access point. It does **not** provide detailed information about these commands.

For detailed information about these commands, see Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, Cisco IOS Release 15.3(3)JC1.

IMPORTANT Before using this manual to configure the Stratix 5100 WAP, you must perform a site survey.

A radio frequency (RF) site survey is the first step in the deployment of a Wireless network and the most important step to make sure appropriate operation. A site survey is a task-by-task process that the surveyor studies the facility to understand the RF behavior, discovers RF coverage areas, checks for RF interference and determines the appropriate placement of Wireless devices.

See Cisco's Wireless Site Survey FAQ for more information about site surveys.

This user manual includes an overview of Stratix 5100 Device Manager, the Rockwell Automation web-based configuration software on the Stratix 5100 WAP. It also provides configuration examples.

Organization

This user manual is organized into these sections.

Item	Description
Chapter 1, Get Started with the Stratix 5100 Wireless Access Point/Workgroup Bridge	Provides an overview of the Stratix 5100 Wireless Access Point/Workgroup Bridge, including its features and network configuration.
Chapter 2, Install the Stratix 5100 Wireless Access Point/ Workgroup Bridge	Provides details on how to install the access point.
Chapter 3, Stratix 5100 Device Manager Configuration Startup	Describes how to use the web browser interface to configure the access point.
Chapter 4, Stratix 5100 Device Manager Parameter Definitions	Defines the parameter settings for each page in Device Manager.
Chapter 5, Access the Stratix 5100 Wireless Access Point/ Workgroup Bridge in Logix Designer	Provides information about the basic access point/workgroup bridge parameters that you can configure and review status information in Logix Designer.
Chapter 6, Configure the Stratix 5100 WAP Using the Command-Line Interface	Describes how to use the command-line interface (CLI) to configure the access point.
Chapter 7, Administer the WAP Access	Describes how to perform one-time operations to administer your access point, such as preventing unauthorized access to the access point, setting the system date and time, and setting the system name and prompt.
Chapter 8, Configure Radio Settings	Describes how to configure settings for the access point radio such as the role in the radio network, transmit power, channel settings, and others.
Chapter 9, Configure Multiple Service Set Identifiers (SSIDs)	Describes how to configure and manage multiple service set identifiers (SSIDs) and multiple basic SSIDs (BSSIDs) on your access point. You can configure up to 16 SSIDs and up to eight BSSIDs on your access point.
Chapter 10, Configure Spanning Tree Protocol	Describes how to configure Spanning Tree Protocol (STP) on your access point, bridge, or access point operating in a bridge mode. STP prevents bridge loops from occurring in your network.
Chapter 11, Configure an Access Point as a Local Authenticator	Describes how to configure the access point to act as a local RADIUS server for your wireless LAN. If the WAN connection to your main RADIUS server fails, the access point acts as a back-up server to authenticate wireless devices.
Chapter 12, Configure Cipher Suites	Describes how to configure the cipher suites required to use authenticated key management, Wired Equivalent Privacy (WEP), and WEP features including MIC, CMIC, TKIP, CKIP, and broadcast key rotation.
Chapter 13, Configure Authentication Types	Describes how to configure authentication types on the access point. Client devices use these authentication methods to join your network.
Chapter 14, Configure Wireless Domain Services and Fast Secure Roaming	Describes how to configure the access point to participate in WDS, to allow fast reassociation of roaming client services, and to participate in radio management.
Chapter 15, Configure RADIUS and TACACS+ Servers	Describes how to enable and configure the RADIUS and Terminal Access Controller Access Control System Plus (TACACS+), that provides detailed accounting information and flexible administrative control over authentication and authorization processes.
Chapter 16, Configure Virtual Local Area Networks (VLAN)	Describes how to configure your access point to interoperate with the VLANs set up on your wired LAN.
Chapter 17, Configure Quality of Service (QoS)	Describes how to configure and manage MAC address, IP, and Ethertype filters on the access point by using the web browser interface.
Chapter 18, Configure Filters	Describes how to configure and manage MAC address, IP, and Ethernet type filters on the access point by using the web browser interface.
Chapter 19, Configure Cisco Discovery Protocol (CDP)	Describes how to configure Cisco Discovery Protocol (CDP) on your access point. CDP is a device-discovery protocol that runs on all Cisco network equipment.
Chapter 20, Configure Simple Network Management Protocol (SNMP)	Describes how to configure the Simple Network Management Protocol (SNMP) on your access point.
Chapter 21, Configure Workgroup Bridge Mode, Repeater Mode, and Standby Access Points	Describes how to configure your access point as a workgroup bridge.
Chapter 22, Configure System Message Logging	Describes how to configure system message logging on your access point.
Chapter 23, Troubleshoot	Provides troubleshooting procedures for basic problems with the access point.
Appendix A Protocol Filters	Lists some of the protocols that you can filter on the access point.
Appendix A Supported Management Information Bases (MIBs)	Lists the Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) that the access point supports for this software release.
Appendix B Error and Event Messages	Lists the CLI error and event messages and provides an explanation and recommended action for each message.

Conventions

The Stratix 5100 Wireless Access Point/Workgroup Bridge is referred to as the Stratix 5100 WAP, WAP, unit, access point, or WGB, workgroup bridge in this document This publication uses these conventions to convey instructions and information.

Command descriptions use these conventions:

- 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.
- Terminal sessions and system appear in `screen` font.
- *Italics* are used for user input.

Additional Resources

These resources contain additional information that concern the product and contain supplemental information from Cisco Systems, Inc.

Resource	Description
Using the Cisco IOS Command-Line Interface Configuration Guide 15.3	Provides comprehensive information about using the Cisco IOS Command-Line Interface.
Cisco IOS 15.2(4)JA Release Notes	Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 15.2(4)JA.
Cisco IOS 15.3(3)JC1 Release Notes	Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 15.3(3)JC1.
Cisco IOS Configuration Guide for Autonomous Cisco Aironet Access Points - Release 15.3(3)JC	Describes Cisco IOS commands used to configure and manage an access point, bridge, and wireless LAN. The commands are listed alphabetically.
Cisco's Wireless Site Survey FAQ	Provides instructions on how to conduct a site survey. A radio frequency (RF) site survey is the **first step** in the deployment of a Wireless network and the most important step to an effective site configuration.
20 Myths of Wi-Fi Interference	Provides information on how RF interference can be a major inhibitor to wireless performance, creating security vulnerabilities and wireless network instability.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, http://www.ab.com	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at http:/www.rockwellautomation.com/literature/. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products.
At http://www.rockwellautomation.com/support you can find technical and application notes, sample code, and links to software service packs. You can also visit our Support Center at https://rockwellautomation.custhelp.com/ for software updates, support chats and forums, technical information, FAQs, and to sign up for product notification updates.

In addition, we offer multiple support programs for installation, configuration, and troubleshooting. For more information, contact your local distributor or Rockwell Automation representative, or visit http://www.rockwellautomation.com/services/online-phone.

Get Started with the Stratix 5100 Wireless Access Point/Workgroup Bridge

This chapter provides an overview of the Stratix 5100 Wireless Access Point/Workgroup Bridge (WAP), including its features and network configuration. The Stratix 5100 Wireless Access Point/Workgroup Bridge is referred to as the Stratix 5100 WAP, WAP, unit, access point, or WGB, workgroup bridge in this document.

Topic	Page
Regulatory Domains	23
Configure the Access Point	24
Management Options	24
Roaming Client Devices	24
Network Configuration Examples	25
Repeater Access Point	26
Unpack the WAP	27
Items Shipped with the WAP	27

The Stratix 5100 Wireless Access Point/Workgroup Bridge provides a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals. With a management system based on Cisco IOS software, the Stratix 5100 WAP is a wireless LAN transceiver, Wi-Fi certified and compliant in:

- 802.11a
- 802.11b
- 802.11g
- 802.11n

The Stratix 5100 WAP offers dual-band radios (2.4 GHz and 5 GHz) with external antennas. The access point supports full interoperability with leading 802.11n clients, and supports a mixed deployment with other access points and wireless controllers.

An access point serves as the connection point between wireless and wired networks or as the center point of a standalone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

The Stratix 5100 WAP supports high-performing Spectrum Intelligence that sustains three spatial stream rates over a deployable distance with high reliability when serving clients.

These are some of the features of the Stratix 5100 WAP:

- 2.4 GHz and 5 GHz 802.11n radios with dual-band antennas
- Wi-Fi Standards 802.11 a/b/g/n
- 3TX (transmit) x 4RX (receive)
- 3 spatial streams, 450 Mbps PHY rate
- Maximum Data Rate 450 Mbps
- Workgroup Bridge (WGB) support that enables wired-only client connectivity to a wireless network
- Band Select
- Cisco Beamforming for .11ag clients, 1 spatial-stream, and 2 spatial-stream clients
- Radio hardware that is capable of explicit compressed beamforming (ECBF) per 802.11n standard
- External Antennas
- CDP (Cisco Discovery Protocol)
- Processing sub-systems (including CPUs and memory) and radio hardware that support
  - Network management
  - 32 MB nonvolatile memory
  - Security functions
  - SNMP Community SNMP
  - Network Configuration
  - Security
  - Secure Shell (SSH)
- ClientLink 2.0 (128 clients)

Regulatory Domains

The Stratix 5100 supports the following regulatory domains.

Table 1 - Stratix 5100 WAP Supported Regulatory Domains

Regulatory Domain	Catalog Number	Channels
A FCC	1783-WAPAK9	2.412 to 2.462 GHz; 11 channels 5.180 to 5.320 GHz; 8 channels 5.500 to 5.700 GHz, 8 channels (excludes 5.600 to 5.640 GHz) 5.745 to 5.825 GHz; 5 channels
B FCC	1783-WAPBK9	2.412 to 2.462 GHz; 11 channels 5.180 to 5.320 GHz; 8 channels 5.500 to 5.720 GHz; 12 channels 5.745 to 5.825 GHz; 5 channels
C	1783-WAPCK9	2.412 to 2.472 GHz; 13 channels 5.745 to 5.825 GHz; 5 channels
E ETSI	1783-WAPEK9	2.412 to 2.472 GHz; 13 channels 5.180 to 5.320 GHz; 8 channels 5.500 to 5.700 GHz, 8 channels, (excludes 5.600 to 5.640 GHz)
N Non FCC	1783-WAPNK9	2.412 to 2.462 GHz; 11 channels 5.180 to 5.320 GHz; 8 channels 5.745 to 5.825 GHz; 5 channels
T	1783-WAPTK9	2.412 to 2.462 GHz; 11 channels 5.280 to 5.320 GHz; 3 channels 5.500 to 5.700 GHz, 8 channels, (excludes 5.600 to 5.640 GHz) 5.745 to 5.825 GHz; 5 channels
Z	1783-WAPZK9	2.412 to 2.462 GHz; 11 channels 5.180 to 5.320 GHz; 8 channels 5.500 to 5.700 GHz, 8 channels, (excludes 5.600 to 5.640 GHz) 5.745 to 5.825 GHz; 5 channels

Support for -B Domain FCC (USA) Rule

The FCC (USA) rule on 5 GHz released on April 1, 2014 (FCC 14-30 Report and Order) goes into effect for products that are sold or shipped on or after June 2, 2016. The Stratix® 5100 Wireless Access Point/Workgroup Bridge now complies with new rules by supporting the new regulatory domain (-B) for the United States, Allen-Bradley® catalog number 1783-WAPBK9.

This catalog number must be purchased for United States deployments effective June 2, 2016. All United States Stratix 5100 deployments previous to June 2, 2016 leveraging the 1783-WAPAK9 catalog number is compatible with the 1783-WAPAK9 with no required configuration changes.

Examples of the rules include new 5-GHz band channels that are permitted for outdoor use, and transmission (Tx) power level increased to 1 W for indoor, outdoor, and point-to-point transmissions.

Configure the Access Point

You can configure and monitor the wireless device by using these methods.

- Command-line interface (CLI)
- Stratix 5100 WAP Device Manager, browser-based management system
- Simple Network Management Protocol (SNMP)

Management Options

You can use the wireless device management system through the following interfaces.

- A web browser interface, that you use through a web browser.

  See Stratix 5100 Device Manager Configuration Startup on page 45 for a detailed description of the web browser interface.

- The Cisco IOS command-line interface (CLI), that you use through a console port or Telnet session.

  For more information on CLI, see Configure the Stratix 5100 WAP Using the Command-Line Interface on page 191.

- Simple Network Management Protocol (SNMP).

  Configure Simple Network Management Protocol (SNMP) on page 453 explains how to configure the wireless device for SNMP management.

Roaming Client Devices

If you have more than one wireless device in your wireless LAN, wireless client devices can roam from one wireless device to another. The roaming functionality is based on signal quality, not proximity. When signal quality drops from a client, it roams to another access point.

Wireless LAN users are sometimes concerned when a client device stays associated to a distant access point instead of roaming to a closer access point. However, if a client signal to a distant access point remains strong and the signal quality is high, the client does not roam to a closer access point. Checking constantly for closer access points can be inefficient, and the extra radio traffic can slow throughput on the wireless LAN.

By using Cisco Centralized Key Management (CCKM) and a device providing WDS, client devices can roam from one access point to another so quickly that there is no perceptible delay in voice or other time-sensitive applications.

Network Configuration Examples

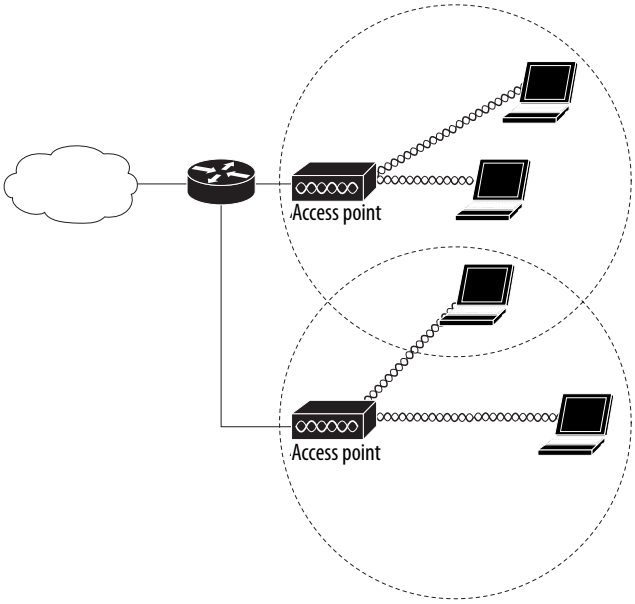
This section describes the role of an access point in common wireless network configurations. The access point default configuration is as a root unit connected to a wired LAN or as the central unit in a wireless network. You can configure access points as repeater access points, bridges, and workgroup bridges. These roles require specific configurations.

Root Access Point

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. Figure 1 shows access points acting as root units on a wired LAN.

See Configure the Basic Settings for an Access Point on page 51 for information on configuring your access point as a connection point.

Figure 1 - Access Points as Root Units on a Wired LAN

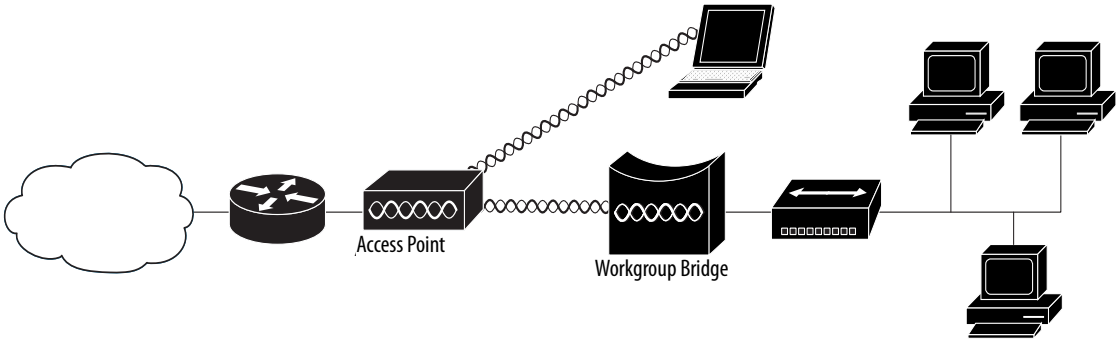


Workgroup Bridge

You can configure access points as workgroup bridges. In workgroup bridge mode, the unit associates to another access point as a client and provides a network connection for the devices connected to its Ethernet port. For example, if you need to provide wireless connectivity for a group of network printers, you can connect the printers to a hub or to a switch, connect the hub or switch to the access point Ethernet port, and configure the access point as a workgroup bridge. The workgroup bridge associates to an access point on your network. Both 5 GHz and 2.4 GHz radios can function in the workgroup bridge mode, but only one radio can be configured as WGB at a time.

Figure 2 shows an access point configured as a workgroup bridge. See Workgroup Bridge Mode on page 467 and Configuring Workgroup Bridge Mode on page 472 for information on configuring your access point as a workgroup bridge.

Figure 2 - Access Point as a Workgroup Bridge



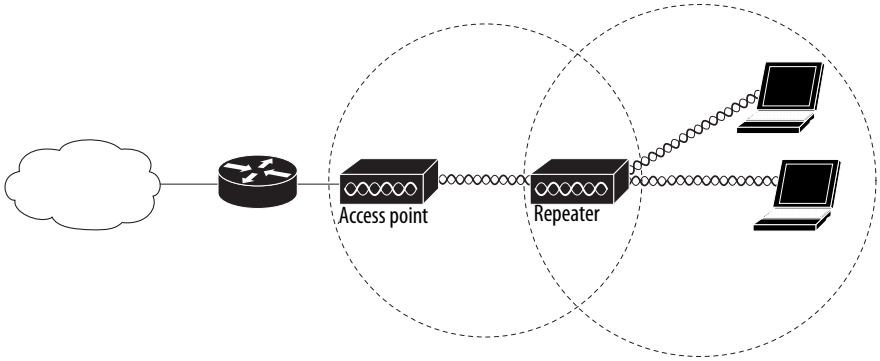
Repeater Access Point

An access point can be configured as a standalone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client.

Consult the Configure Workgroup Bridge Mode, Repeater Mode, and Standby Access Points on page 467 for instructions on how to set up an access point as a repeater.

TIP Client devices that are not manufactured by Rockwell Automation or Cisco can have difficulty communicating with repeater access points.

Figure 3 - Access Point Acting as a Repeater



Unpack the WAP

To unpack the access point, follow these steps:

1. Unpack and remove the access point and the accessory kit from the shipping box.
2. Return any packing material to the shipping container and save it for future use.
3. Verify that you have received the items listed below.
   - Stratix 5100 Wireless Access Point/Workgroup Bridge
   - Mounting bracket, screws included
   - Power adapter
   - 4 Wi-Fi antennas
   - Console cable
   - Stratix 5100 Wireless Access Point Product Information

   If any item is missing or damaged, contact your Rockwell Automation, see Rockwell Automation Support on the back cover of this manual.

Items Shipped with the WAP

The following items are included with the Stratix 5100 Wireless Access Point/ Workgroup Bridge.

Item	Description
Stratix 5100 Wireless Access Point/ Workgroup Bridge	1783-WAPAK9, 1783-WAPBK9, 1783-WAPCK9, 1783-WAPEK9, 1783-WAPNK9, 1783-WAPTK9, 1783-WAPZK9
Mounting bracket, screws included	700-30482-04 REV. A0
Power adapter	AIR-PWR-B Input: 100…240 50/60 Hz VAC Output: 48V DC, 380 mA
4 Wi-Fi antennas	AIR-ANT2524DG-R
Console cable	Cisco part number 72-3383-01. Rev. A2

Notes:

Install the Stratix 5100 Wireless Access Point/ Workgroup Bridge

This chapter provides basic instructions on how to install and configure your Stratix 5100 Wireless Access Point/Workgroup Bridge.

Topic	Page
Prepare the Access Point	30
Prevent Damage to the WAP	30
Ports and Connections	31
Install the WAP	31
Mount the Access Point	33
Ground the Access Point	36
Secure the Access Point	37
Stratix 5100 WAP Specifications	38
External Antennas	39
Stratix 5100 WAP Status Indicators	42
Stratix 5100 WAP Status Indicators	42
Configure the Access Point	43

Prepare the Access Point

Before you mount and deploy your access point, perform a site survey to determine the best location to install your access point. You can find more information about site surveys here http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html.

Obtain this information about your wireless network:

- Access point locations
- Access point mounting options: below a suspended ceiling, on a flat horizontal surface, or on a desktop

  TIP You can mount the access point above a suspended ceiling but you must purchase additional mounting hardware.

  See Mount the Access Point on page 33 for additional mounting information.

- Access point power options:
  - AC Adapter Power over Ethernet (PoE)
  - Recommended external power supply (Cisco AIR-PWR-B)
  - PoE capable switch, such as the Stratix 8000, 5700, 5400, or 5410
  - Recommended external PoE power injector (Cisco AIR-PWR-INJ4)

Access points that are mounted in an environmental air-space must be powered by using PoE to comply with safety regulations. Make a site map that shows the access point locations so that you can record the device MAC IDs from each location. Provide this information to the manager of your wireless network.

Prevent Damage to the WAP

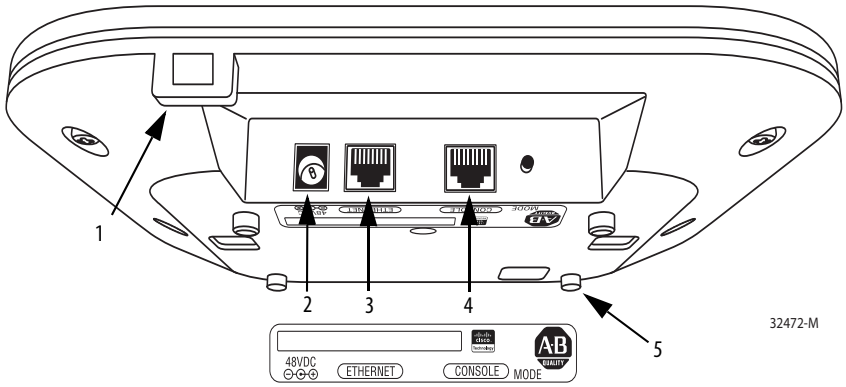
To prevent damage to your WAP, follow these guidelines when connecting devices to the access point.

ATTENTION: Turn off power to the devices and to the wireless access point until all connections are completed. Do not turn on the devices until after you have completed all connections to the access point.

You can mount the access point above a suspended ceiling, but you must purchase additional mounting hardware. Install the Stratix WAP above the ceiling tiles only when mounting below the ceiling is not an option.

Ports and Connections

The ports and connections are on the bottom of the access point.



Item	Description
1	Kensington lock slot
2	Power connection
3	Gigabit Ethernet port
4	Console port
5	Mounting bracket pins

Install the WAP

Install the Stratix 5100 WAP on a flat surface.

1. Unpack and remove the access point and the accessory kit from the shipping box.
2. Return any packing material to the shipping container and save it for future use.
3. Verify that you have received the items listed below.
   - Access point
   - Mounting bracket
   - Power adapter, Cisco AIR-PWR-B
   - Console cable
   - Antennas, see External Antennas on page 39

   If any item is missing or damaged, contact your Rockwell Automation representative, see Rockwell Automation Support on the back cover of this manual.

Other items you need to install the unit:

- ESD-preventive cord and wrist strap
- Ethernet cable
- Grounding wire
- Mounting screws

Ethernet Cable Recommendation

While the Stratix 5100 WAP works well with the CAT-5e cable for 10/100 MB installations, we recommend that you use CAT-6a cable for 1 GB installations.

Access Point Spacing Recommendation

If you have a Wi-Fi device such as a WAP and want to use another WAP in the vicinity on the same or different channel, space the WAPs approximately 2 m (6 ft) apart. This recommended distance is based on the assumption that both devices operate in the unlicensed band and do not transmit RF energy more than 23 dB, that is, 200 mW. If higher power is used, space farther apart. Avoid clustering the WAPs or the antennas from different WAPs together, because this could degrade performance.

If you have other devices that transmit, follow these instructions.

1. Move or separate the devices as far apart as reasonable.

   This is especially important if they operate in the same frequency ranges; for example, frequency hopping legacy WAPs or other devices operate just below or above the 2.4 GHz and 5 GHz band.
2. Check for interference.
3. Test both types of devices at the same time under heavy use (load).
4. Characterize each system independently to see whether degradation exists.

IDF Closets (telecommunications or other electrical equipment)

When installing WAPs near other electrical or telecommunications equipment, keep all wiring and metal away from the antennas, and avoid placing the antennas near electrical lines. Do not route electrical wiring or Ethernet in the near field 38 cm (15 in.) of the antenna, and try not to install the WAP in an electrical closet. Local fire and safety regulations can require you to use a plenum-rated cable if your remote antenna cables originate from an electrical closet. Remember that the best place for the WAP is close to its users.

Very High Altitudes

While not defined in the specification sheet for the Stratix 5100 WAPs, the units have passed functional checks after a non-operational altitude test of 25 °C @ 4572 m (77 °F @ 15,000 ft) was performed. Additionally, the units passed a functional test during an operational altitude test of 40 °C @ 3000 m (104 °F @ 9843 ft). All units in the test group were connected to at least one WLAN client and were monitored for continual operation passing traffic, with constant ping testing throughout the operational altitude test.

Common or Distributed Antenna System (DAS)

Due to the dual-band nature of the antenna system on the Stratix 5100 WAP along with key features such as ClientLink 2.0 beamforming, the Stratix 5100 WAP is not recommended for deployments on distributed antenna systems (DAS).

Rockwell Automation does not certify, endorse, or provide RF support for Wi-Fi deployments over any DAS.

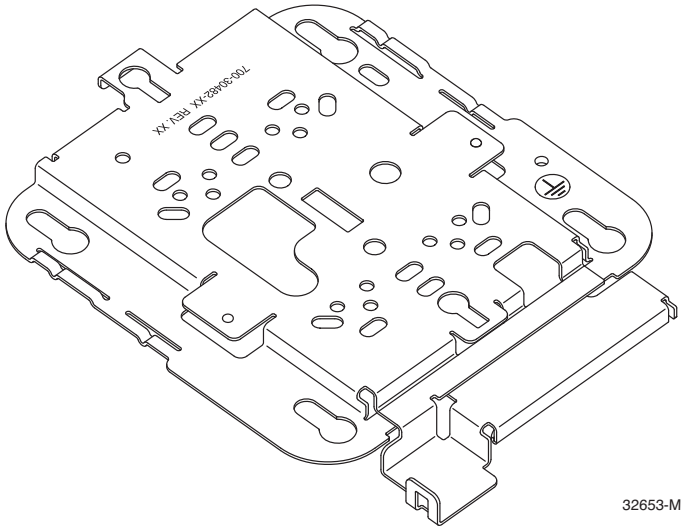
The DAS vendor and systems integrator are solely responsible for the support of the DAS products, adequate RF coverage, and any RF-related issues. This support includes, but is not exclusive to, location accuracy, RF coverage, roaming issues related to RF, multipath issues, and scalability.

The DAS vendor and system integrators are responsible for understanding that the deployed DAS system meets the requirements of all of the customer Wi-Fi devices and applications over the DAS system.

IMPORTANT While Rockwell Automation, Cisco Technical Assistance Center (TAC) and Cisco field teams do not provide support for RF issues that arise in a Cisco WLAN used over a DAS, they provide support for non-RF related issues observed with the Stratix 5100 Wireless Access Point according to the customer support agreement.

Mount the Access Point

The Stratix 5100 WAP comes with a low-profile access point mounting bracket. This bracket can be mounted flush on a flat surface or directly onto a ceiling, on grid-work.



Low profile bracket

This procedure describes the steps required to mount the access point with a the mounting bracket on a ceiling constructed of 19.05 mm (3/4-in.) or thicker plywood by using appropriate fasteners.

TIP Access points perform best when antennas are oriented vertically.

Follow these steps to mount the access point on a solid ceiling or wall.

1. Place the mounting bracket on the surface where you are going to mount the access point.
2. Use the mounting bracket as a template to mark the locations of the mounting holes (1) on the bracket.

Figure 4 - WAP Mounting Bracket

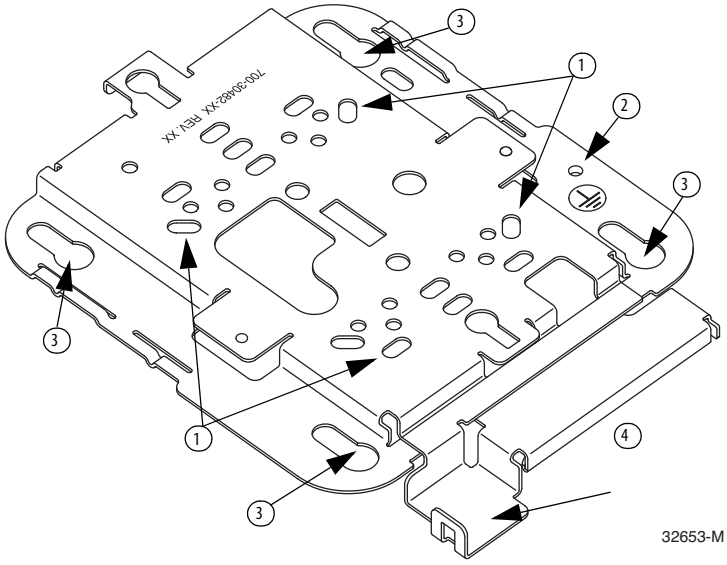


Table 2 - Mounting Bracket Description

1	Wall mount locations	3	Access point attachment slots
2	Grounding post	4	Padlock attachment

TIP Mark all four locations of the wall mounts. Make sure you have a secure installation. Use adequate fasteners to mount the access point and use no fewer than four fasteners.

IMPORTANT Do not use plastic wall anchors or the keyhole slots on the mounting bracket for ceiling installations. When mounting the access point on a hard ceiling, use four fasteners capable of maintaining a minimum pullout force of 9 kg (20 lbs).

3. Use a drill to create a pilot hole at the mounting hole locations you marked.

TIP The pilot hole size varies according to the material and thickness you are fastening. Test the material to determine the ideal hole size for your mounting application.

4. Drill or cut a cable access hole near and below the location of the mounting bracket cable-access cover large enough for the Ethernet cable, building ground wire, and power cables.
5. Route the cables through an access hole on the mounting bracket.
6. Use the ground screw to attach the building ground wire to the mounting bracket.

See Ground the Access Point on page 36 for general grounding instructions.

7. Position the mounting bracket mounting holes over the pilot holes.
8. Insert a fastener into each mounting hole and tighten.
9. Connect the Ethernet and power cables to the access point.
10. Align the access point feet with the large part of the keyhole mounting slots on the mounting plate.
11. When positioned correctly, the cable access cover fits inside the access-point connector bay.
12. Gently slide the access point onto the mounting-bracket keyhole slots until it clicks into place.

The Stratix 5100 access point can be mounted in several configurations, including, on a hard ceiling or wall, on an electrical or network box, on a suspended ceiling, and above a suspended ceiling. The Stratix 5100 access point is shipped with the flat mounting bracket for a hard ceiling or wall, and on applications that you need to mount on an electrical or network box.

Ground the Access Point

Grounding is not always required for indoor installations because the access point is classified as a low-voltage device and does not contain an internal power supply. However, check your local and national electrical codes to see if grounding is a requirement.

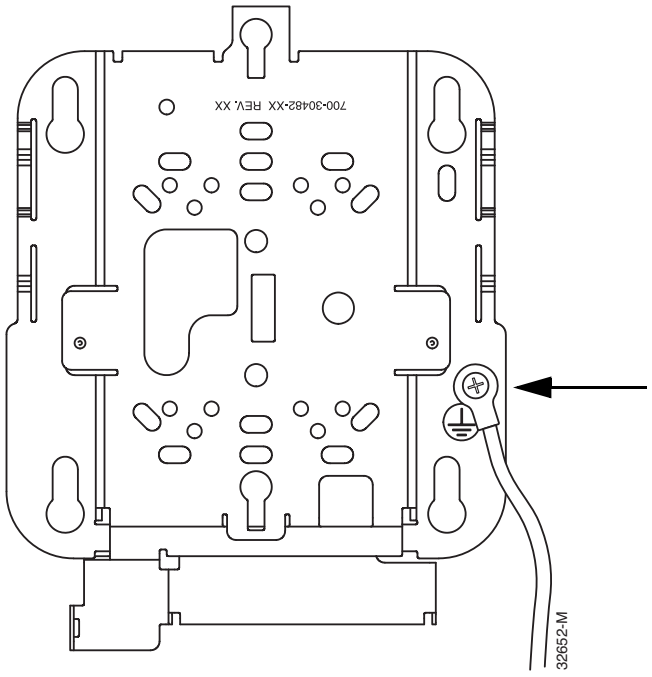
IMPORTANT	Make sure to ground the mounting plate before you attach the WAP to a flat surface.

Follow these steps to ground the access point/bridge.

1. Find a suitable building grounding point as close to the access point as possible.
2. Connect a user-supplied ground wire to the building grounding point.

   The minimum gauge of the wire is 2.5mm^2 (14 AWG), assuming a circuit length of 1 ft (30.5 cm). Consult your local electrical codes for additional information.
3. Route the ground wire to the access point.
4. Attach the wire to a suitable grounding O-ring lug (user-supplied).
5. Crimp or solder the wire to the lug.
6. Insert the grounding post screw into the O-ring lug and install it on the mounting bracket as shown in Figure 5.
7. Use a Phillips screwdriver to tighten the ground screw.

Figure 5 - Installing the O-Ring Lug to the Grounding Post



Secure the Access Point

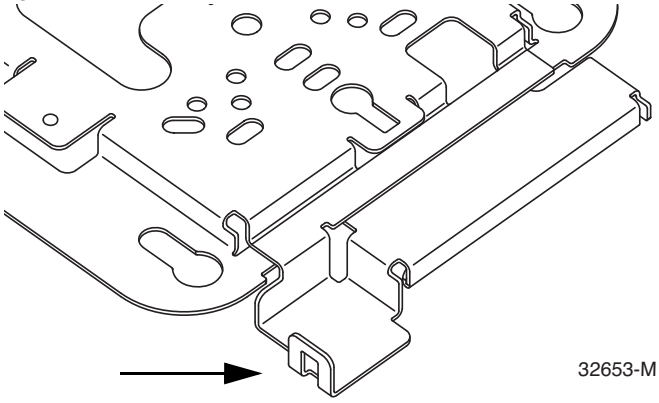
There are two ways to secure your access point:

- Attach it to an immovable object with a security cable.
- Lock it to the mounting plate with a padlock.

Secure the Access Point to the Mounting Plate

Use this location on the mounting plate to attach a padlock to secure the access point to the mounting plate and security cable.

Figure 6 - Padlock location



Compatible padlocks are Master Lock models 120T or 121T. The cable access cover on the mounting bracket covers the cable bay area (including the power port, Ethernet port, console port, and the mode button) to provide protection during the installation or removal of the cables or the activation of the mode button.

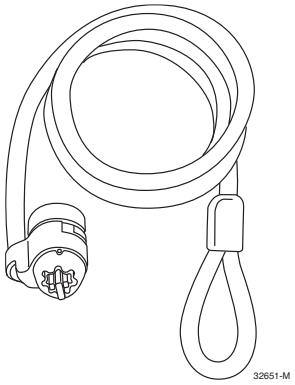
Follow these instructions to install the padlock:

1. With the access point installed on the mounting bracket, insert a padlock into the opening and the security hasp on both the access point and the mounting bracket.

   TIP Note If your access point is mounted to a hard ceiling, the clearance between the mounting bracket and the ceiling is small. Work slowly by using both hands to position and secure the lock into the mounting bracket hasp.

2. Rotate the lock clockwise and align the bail with the lock body.
3. Grasp the lock and push it into the bail to lock the lock.

Security Cable



You can secure the access point by installing a standard security cable into the access point security cable slot. The security cable can be used in combination with the padlock when using any of the mounting methods described in this document.

Follow these steps to install the security cable.

1.Loop the security cable around a nearby immovable object or in conjunction with the padlock and mounting bracket.

2.Insert the key into the security cable lock.

3. Insert the security cable latch into the security cable slot on the access point.
4. Rotate the key right or left to secure the security cable lock to the access point.
5. Remove the key.

Stratix 5100 WAP Specifications

This table lists the technical specifications for the Stratix 5100 Wireless Access Point/Workgroup Bridge.

Table 3 - Stratix 5100 Wireless Access Point/Workgroup Bridge Specifications

Category	Specification
Dimensions (LxWxD)	22.04 x 22.04 x 4.67 cm (8.68 x 8.68 x 1.84 in.)
Weight	1.22 kg (2.7 lb)
Operating temperature	-20…+55 °C (-4…+131 °F)
Storage temperature	-30…+85 °C (-22…+185 °F)
Humidity	10…90% noncondensing
Power rating	Input: 100…240 50/60 Hz VAC Output: 48V DC, 380 mA
Antennas	External
Compliance	Complies with UL 2043 for products installed in a building's environmental air handling spaces, such as above suspended ceilings.
Maximum power and channel settings	Maximum power and the channels allowed in your regulatory domain. See Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points. This document is available on Cisco.com.

External Antennas

The Stratix 5100 Wireless Access Point/Workgroup Bridge has external antenna connectors and a status indicator on the top. The antennas are rugged and designed for industrial use in locations such as hospitals, factories, warehouses, and other locations where there is a need for extended operating temperatures. The external antennas support mounting inside NEMA enclosures for use in the most demanding environments.

The Stratix 5100 WAP is configured with up to four external dual-band dipole antennas, and 2.4 GHz and 5 GHz dual-band radios in a 3 x 4 multiple-input/multiple-output (MIMO) configuration with three spatial streams. The radios and antennas support frequency bands 2400...2500 MHz and 5150...5850 MHz through a common dual-band RF interface.

The following Cisco antennas are supported on the Stratix 5100 WAP:

Figure 7 - Supported Cisco Antennas

Antenna (Cisco part number)	Antenna Gain (dBi)		Antenna Gain Parameter to be configured in CLI interface (dBi)		Description
	2.4 GHz	5 GHz	2.4 GHz	5 GHz	
AIR-ANT2524DG-R (shipped with product)	2	4	4	8	Dual-resonant grey dipole
AIR-ANT2524V4C-R	2	4	4	8	Dual-resonant, ceiling-mount omni(1)
AIR-ANT2544V4M-R	4	4	8	8	Dual-resonant omni(1)
AIR-ANT2566P4W-R	6	6	8	8	Dual-resonant directional antenna(1)

(1) 4-element (4 antenna lead cables)

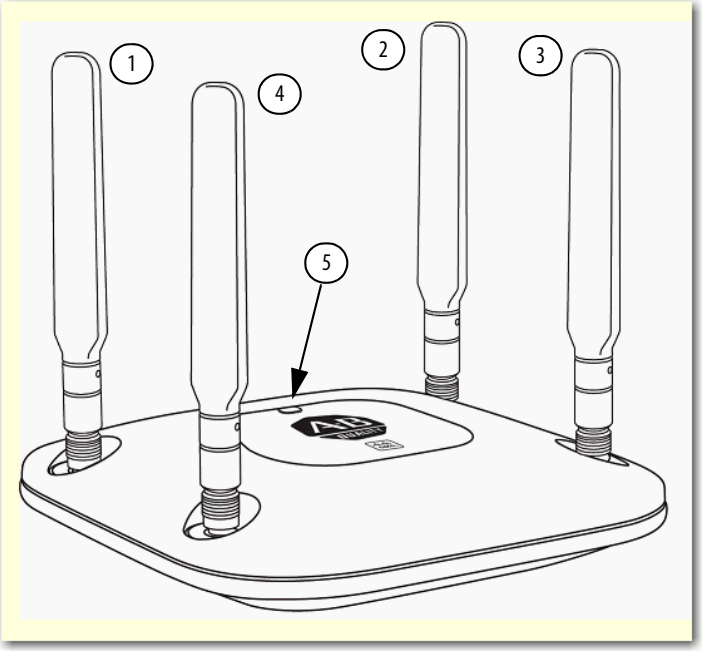
IMPORTANT **ATTENTION:** To comply with RF exposure limits, locate the antennas at a minimum of 20 cm (7.9 in) or more from the body of all persons. Antennas must be mounted indoors only.

Antenna Cable Recommendation

Keep antenna cable runs as short as possible. Cisco offers low loss (LL) and ultralow loss (ULL) cables, that have the same characteristics as Times Microwave LMR-400 and LMR-600. When drilling holes for cable, allow for the size of connector drill bit, typically15.8750 mm (5/8 in.).

Cisco cables carry the part number AIR-CAB (Aironet Cable) and then a length. For example, a 20 ft length of LL cable with RP-TNC connector is Cisco AIR-CAB-020LL-R. These heavy black cables are not plenum rated and are primarily for use in manufacturing areas.

Figure 8 - Access Point Antenna Connections



1	Antenna connector A	4	Antenna connector D
2	Antenna connector B	5	Status Indicator
3	Antenna connector C		

The Stratix 5100 WAP is configured with up to four external dual-band dipole antennas, and 2.4 GHz/5 GHz dual-band radios in a 3 x 4 MIMO configuration with three spatial streams. The radios and antennas support frequency bands 2400...2500 MHz and 5150...5850 MHz through a common dual-band RF interface. These are the features of the external dual-band dipole antennas:

- Four RP-TNC antenna connectors on the top of the access point
- Three TX and four RX antennas

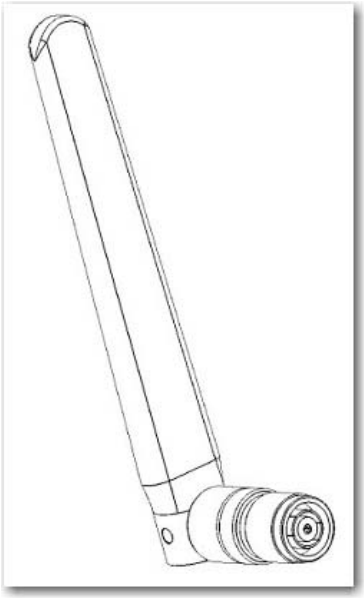
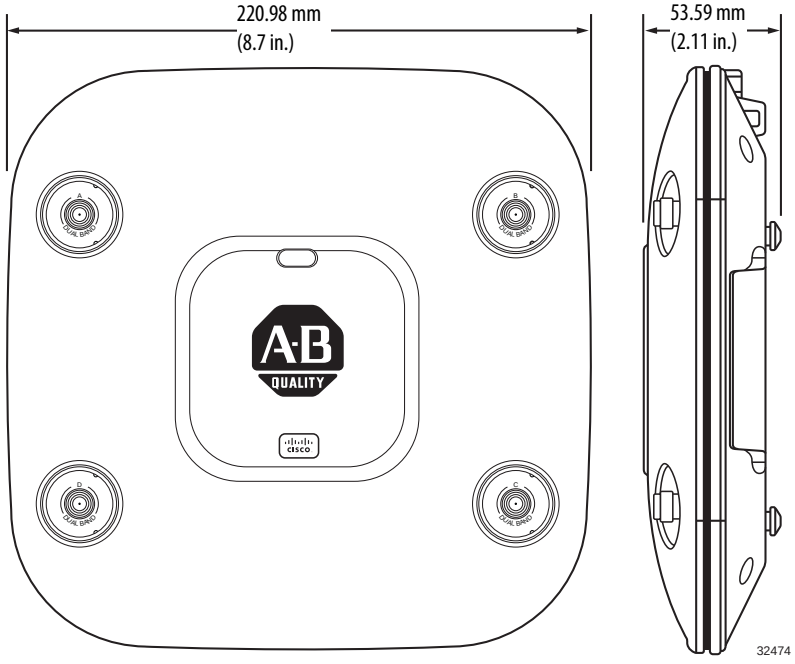


Table 4 - Dual-band Dipole Antenna (AIR-ANT2524DG-R) Specifications

Parameter	Description
Antenna type	Dual-band dipole
Operating frequency ranges	2400…2500 MHz 5150…5850 MHz
Nominal input impedance	50 Ω
VSWR	Less than 2:1
Peak Gain @ 2.4 GHz	2 dBi
Peak Gain @ 5 GHz	4 dBi
Elevation plane 3dB beam width @ 2.4 GHz	63°
Elevation plane 3dB beam width @ 5 GHz	39°
Connector type	RP-TNC plug
Antenna length	168.5 mm (6.63 in.)
Antenna width	21 mm (0.83 in.)
Radome length	124 mm (4.88 in.)
Weight	1.3 oz
Operating temperature	-20…+60 °C (-4…+140 °F)
Storage temperature	-40…+85 °C (-40…+185 °F)

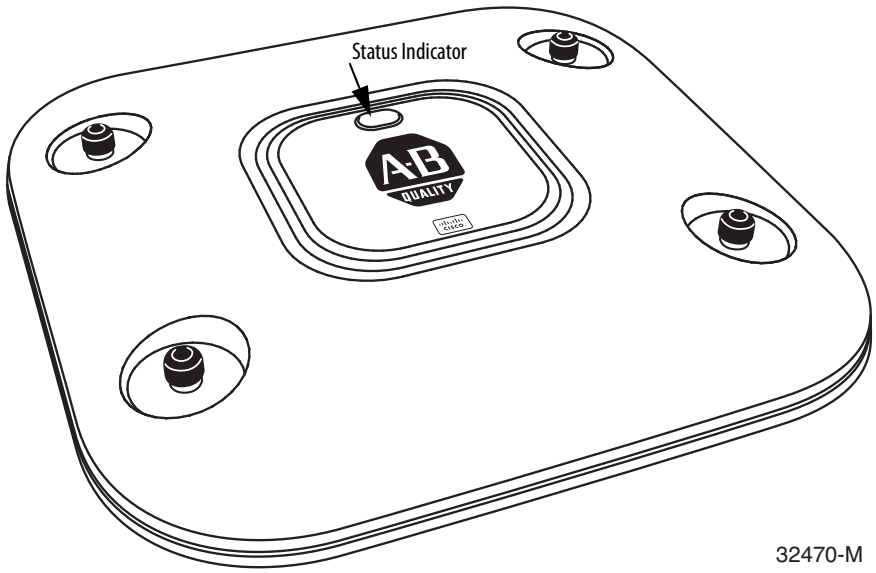
Figure 9 - Stratix 5100 WAP Dimensions



Stratix 5100 WAP Status Indicators

It is expected that there are small variations in color intensity and hue from unit to unit. This is within the normal range of the status indicators manufacturer's specifications and is not a defect.

Figure 10 - Access Point Status Indicator



The status indicators communicate various WAP conditions.

Table 5 - Status Indicator Descriptions

Message Type	Status Indicator	Description
Boot loader status sequence	Blinking green	DRAM memory test in progress
		DRAM memory test OK
		Board initialization in progress
		Initializing nonvolatile memory file system
		Nonvolatile memory test OK
		Initializing Ethernet
		Ethernet OK
		Starting Cisco IOS
		Initialization successful
Association status	Green	Normal operating condition, but no wireless client associated
	Blue	Normal operating condition, at least one wireless client association
Operating status	Blinking red	Ethernet link not operational
Boot loader warnings	Blinking blue	Configuration recovery in progress (MODE button pushed for 2…3 seconds)
	Red	Ethernet failure or image recovery. (MODE button pushed for 20…30 seconds)
	Blinking green	Image recovery in progress (MODE button released)

Table 5 - Status Indicator Descriptions (Continued)

Message Type	Status Indicator	Description
Boot loader errors	Red	DRAM memory test failure
	Blinking red and blue	Nonvolatile memory file system failure
	Blinking red and off	Environment variable failure
		Bad MAC address
		Ethernet failure during image recovery
		Start environment failure
		No Cisco image file
		Start failure
Cisco IOS errors	Red	Software failure; try disconnecting and reconnecting unit power
	Cycling through blue, green, red, and off	General warning; insufficient in-line power

Configure the Access Point

The configuration process takes place on the WAP using the Stratix 5100 Device Manager or using CLI.

For instructions on how to configure the Wireless Access Point/Workgroup Bridge by using:

- Obtain an IP address via DHCP and use Device Manager, the web browser interface.

  See Stratix 5100 Device Manager Configuration Startup on page 45 for a detailed description of the web browser interface.

- The Cisco IOS command-line interface (CLI), that you use through a console port and a Telnet session.

  See Configure the Stratix 5100 WAP Using the Command-Line Interface on page 191.

The first time you use the access point/workgroup bridge you can use these methods to configure the Stratix 5100 WAP.

Notes:

Stratix 5100 Device Manager Configuration Startup

This chapter describes the Stratix® 5100 Device Manager and start-up configurations. It is a web browser interface that can be used to configure the wireless access point/workgroup bridge.

Topic	Page
Login to the Stratix 5100 WAP	48
Obtain and Assign an IP Address	48
Default Radio Settings	48
Default Radio Settings	48
Reset the WAP to Default Settings	49
Online Help	51
Configure the Basic Settings for an Access Point	51
Online Help	51
Configure Security	58
Easy Set-up Page Security Types	59
Easy Setup Network Configuration Security Limitations	59
Create an SSID from the Security Menu	60
CLI Configuration Example	66
Delete an HTTPS Certificate	66
Disable the Web Browser Interface	66

Device Manager

Device Manager contains management pages where you can change the access point settings, update firmware, monitor the access point, and configure wireless devices on the network. The access point radio interfaces are disabled by default. As you work with the management pages, there are error messages that appear when you have missed a configuration parameter that is based on what you have already set. Once you have set the parameter correctly, you can continue.

You can do the following with Device Manager.

- Configure a VLAN.
- Assign the SSID and Broadcast SSID.
- Determine VLAN-to-SSID mappings.
- Select optimal data rates.
- Configure EAP authentication, including EAP/RADIUS server.
- Assign encryption modes.
- Use the Wireless MAC filter.
- Detect MACs for filter (capture network discovered MAC IDs and export to MAC filter list).

The Easy Setup page where you can configure an access point's basic parameters quickly.

TIP Avoid using both CLI and Stratix 5100 WAP Device manager (web browser) to concurrently configure the wireless device. If you configure the wireless device using CLI, the web browser interface can display an inaccurate interpretation of the configuration. However, the inaccuracy does not necessarily mean that the wireless device is misconfigured.

Before You Start

Before you configure the Stratix 5100 WAP, make sure you are using a computer connected to the same network as the access point, and obtain the following information from your network administrator:

- A system name for the access point
- The case-sensitive wireless service set identifier (SSID) for your radio network.
- If not connected to a DHCP server, a unique IP address for the access point, a default gateway address, and subnet mask.
- The access point MAC address. The MAC address can be found on the label on the bottom of the access point, such as, 00:16:46:25:85:4C.
- If SNMP is in use, a Simple Network Management Protocol (SNMP) community name and the SNMP file attribute.

Connect to the Stratix 5100 WAP Access Point Locally

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a computer to by using a the console cable provided, (DB-9 to (RJ-45) serial cable.

Follow these steps to open CLI by connecting to the access point console port:

1. Connect the console cable (RJ-45) to the WAP.
2. Connect the other end of the console cable (DB-9) to the serial port on the computer.

   You can also use a USB to serial adapter.
3. Set up a terminal emulator to communicate with the access point.

   Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control. If Xon/Xoff flow control does not work, use no flow control.
4. When connected, press enter to access the command prompt.
5. Configure the device via CLI.

   See Configure the Stratix 5100 WAP Using the Command-Line Interface on page 191 for detailed information.
6. When your configuration changes are completed, remove the serial cable from the access point.

Once you have completed the initial configuration using CLI and the console cable, you can login to the access point and begin using Stratix 5100 Device Manager.

Obtain and Assign an IP Address

To browse to the Stratix 5100 WAP Device Manager easy access point setup page, you must determine the access point IP address. The IP address can be already assigned if the device was previously set up, can be DHCP out of the box, or you can assign it.

Default IP Address Behavior

When you connect a Stratix 5100 WAP with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an address, continues to send requests indefinitely.

Login to the Stratix 5100 WAP

You can login to the access point by using one of the following methods.

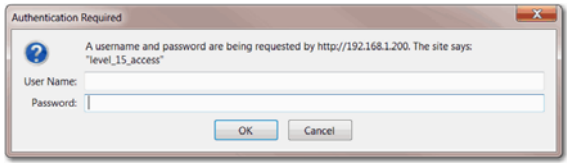
- Graphical user interface (GUI)
- Telnet, if the AP is configured with an IP address, see Access CLI on page 198.
- SSH (Secure Shell) if enabled on the AP.
- Console port, see Default Radio Settings on page 48.

Use the IP address of the WAP to go to Device Manager. If you don't know the IP address of the access point, see Obtain and Assign an IP Address on page 48.

Follow these steps to use the web browser interface:

1. Open your browser.

   Microsoft Internet Explorer or Mozilla Firefox, latest version with JavaScript enabled.
2. Enter the IP address for the Stratix 5100 WAP in the address field.
3. Enter the Username and Password and click OK.



   The Summary Status Home page appears.

Default Radio Settings

The Stratix 5100 WAP radios are disabled and no default SSID is assigned. This is to prevent unauthorized users to access a your wireless network through an access point having a default SSID and no security settings. You must create an SSID before you can enable the access point radio interfaces.

See Configure Radio Settings on page 251 for additional information about default radio settings.

Reset the WAP to Default Settings

If you need to start over during the initial setup process, you can reset the access point to factory default settings. Reset to default settings returns a device that you have configured to its default settings.

Reset to WAP Default Settings by Using the MODE Button

Follow these steps to reset the access point to factory default settings by using the access point MODE button:

1. Disconnect power (the power jack for external power or the Ethernet cable for PoE power) from the access point.
2. Press and hold MODE while you reconnect power to the access point.
3. Hold MODE until the status indicator turns amber (approximately 20...30 seconds), and release the button.

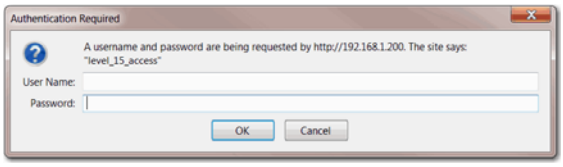
   All access point settings return to factory defaults.

Reset to Default Settings by Using the GUI

Follow these steps to return to default settings by using the access point GUI:

1. Open your Internet browser.
2. Enter the access point IP address in the browser address line and press Enter.

   The Authentication Required dialog box appears.



3. Enter your username in the User Name field.
4. Enter the access point password in the Password field and press Enter.

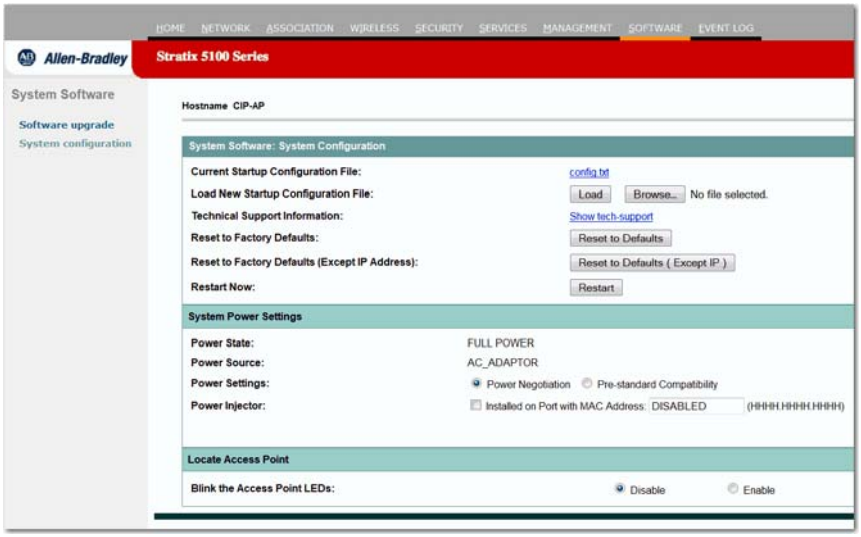
The Summary Status page appears.

5. From the top menu, click Software.

The System Software screen appears.

6. Click System Configuration.

The System Configuration screen appears.



7. Click Reset to Defaults to reset all settings, including the IP address, to factory defaults.

You can reset the defaults by using CLI, see Reset Default Settings by Using CLI on page 199.

Online Help

Click the help icon at the top of any page in the web browser interface to display online help. Click the printer icon to print the page you are on.

Use the select a topic pull-down menu to display the help index or instructions for common configuration tasks.

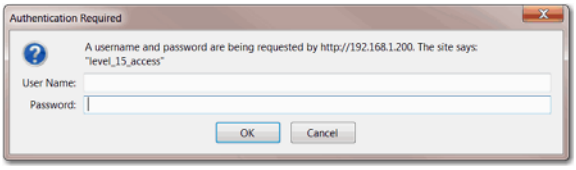
Configure the Basic Settings for an Access Point

After you determine or assign the access point IP address, you can browse to the access point Express Setup page and perform the initial configuration.

For more information on configuration parameters, see Stratix 5100 Device Manager Parameter Definitions on page 69.

1. Open your Internet browser.
2. Type the WAP address in the browser address line and press Enter.

   An Enter Network Password screen appears.



3. Press Tab to bypass the Username field and advance to the Password field.
4. Enter the case-sensitive password: wirelessap.
5. Press Enter.

   The Summary Status page appears. Your page can be different depending on the access point model you are using.

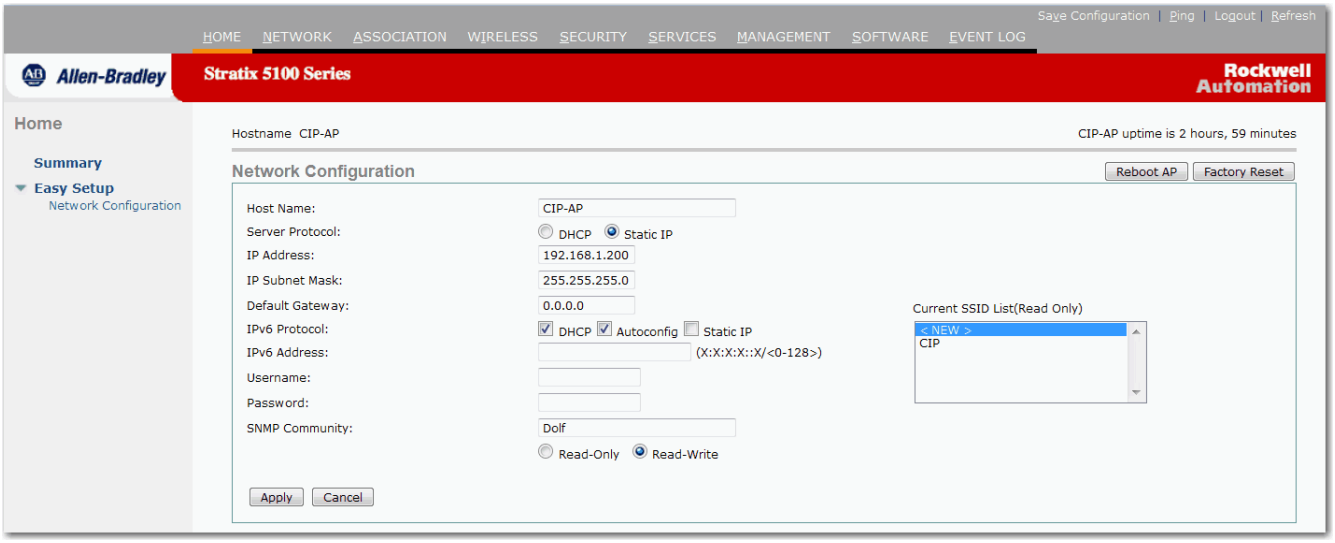
Figure 11 - Summary Status Page

6. Click Easy Setup.

7. Open Easy Setup and click Network Configuration.


Allen-Bradley
Home
Summary
Easy Setup
Network Configuration

8. Enter the network configuration settings.



This table describes the network configuration settings on the Easy Setup page. For more information about the parameters, see Easy Setup Network Configuration Page on page 72,

Table 6 - Network Configuration Settings

Parameter	Description
Host Name	The host name appears in the titles of the management system pages.
Server Protocol	Choose the item that matches the network method of IP address assignment.
IP Address	Use this setting to assign or change the WAP IP address. If you selected DHCP in Server Protocol above, leave this field blank.
IP Subnet Mask	Enter the IP subnet mask provided by your network administrator. Leave blank if DHCP enabled.
Default Gateway	Enter the default gateway IP address provided by your network administrator. If DHCP is enabled or you do not have a default gateway, leave this field blank.
IPv6 Protocol	Configure your IPv6 settings (DCHP, Autoconfig, and Static IP) with the provided checkboxes. Contact you system administrator if you need more information.
IPv6 Address	(X:X:X:X::X/<0-128>) Use this setting to assign or change the Stratix 5100 IPv6 IP address. If IPv6 DHCP is not selected above leave this field blank.
Username	The username want to use for this WAP.
Password	The password you want to use for this WAP.
SNMP Community	To use Simplified Network Management Protocol (SNMP), enter a community name. SNMP is an application-layer protocol that supports message-oriented communication between SNMP management stations and agents.
Current SSID List	List of SSIDs currently configured on the Stratix 5100 WAP.

9. Enter the radio configuration settings.

Figure 12 - Radio Configuration Settings on the Network Configuration Page

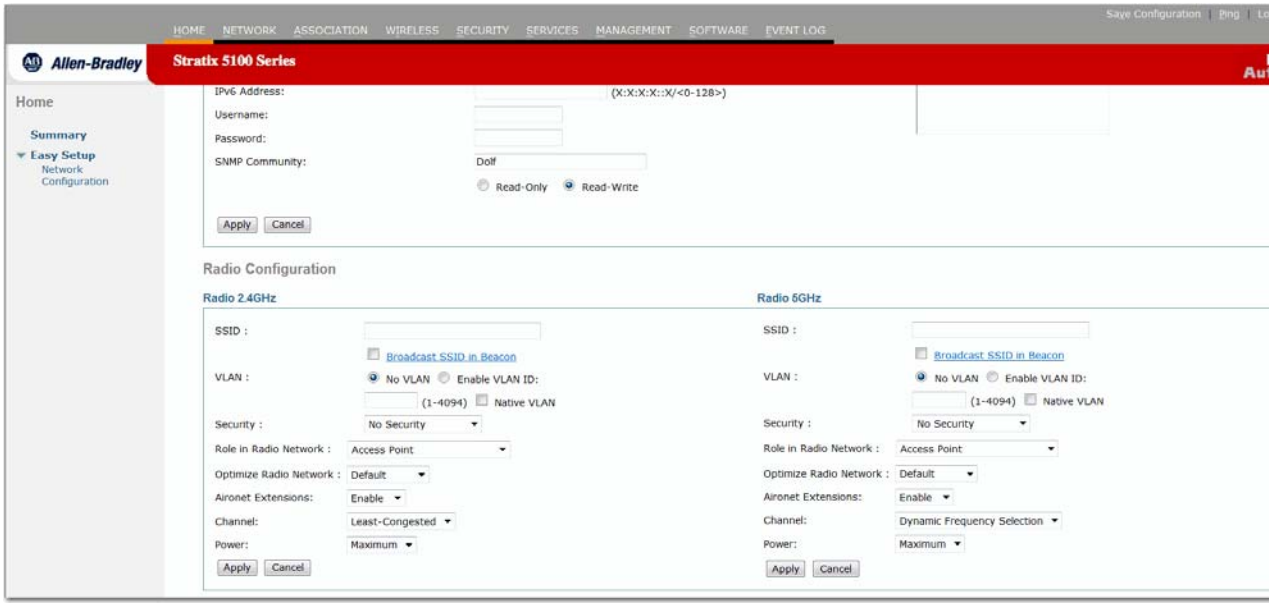


Table 7 - Radio Configuration Settings

Parameter	Description
SSID	Identifies the SSID that client devices must use to associate with a device.
Broadcast SSID in Beacon	This setting is active when the device is in the Root AP mode. When you broadcast the SSID, clients can discover the network automatically and associate to the root AP without entering the SSID manually.
Security	Lists the security types.
VLAN	Choose a VLAN setting.
Role in Radio Network	
Access Point	Choose Access Point (Root) if the access point is connected to the wired LAN.
Repeater	Choose Repeater (Non-root) if it is not connected to the wired LAN.
Root Bridge	Establishes a link with a non-root bridge.
Non-root Bridge	In this mode, the device establishes a link with a root bridge.
Workgroup Bridge	Specifies that the WAP operates as a workgroup bridge connecting one or many wired devices to the wireless network through an Ethernet switch.
Universal Workgroup Bridge	Specifies that the WAP operates as a universal workgroup bridge connecting a single wired device to a non-Cisco wireless AP.
Scanner	Specifies that the access point operates only as a radio scanner and does not accept associations from client devices.
Spectrum	Specifies that the AP operates as a dedicated RF spectrum sensor that used with the Cisco Spectrum Expert software.
Optimize Radio Network for	Use this setting to choose either preconfigured settings for the access point radio or customized settings for the access point radio. The options are default, range, and throughput.

Table 7 - Radio Configuration Settings (Continued)

Parameter	Description
Aironet Extensions	Choose Enable if there are only Rockwell Automation WAPs or Cisco Aironet devices on your wireless LAN and the unit is operating as an access point, workgroup bridge, or as a repeater.
Channel	Use this mode to specify what channel / frequency the device should use. Channel number/frequency Least Congested When you choose Least congested, the WAP makes the determination on its own which channel is best.
Power	Maximum Specific power level (dBm)

10. Click Apply to save your settings.

For additional radio configuration about the parameters, use these links:

- Easy Setup Network Configuration Page on page 72
- Network Interface Summary Page on page 80

Enable the Radio on the Network

In addition to setting the parameters on the Easy Setup page, you must go to the radio settings page to enable the radio.

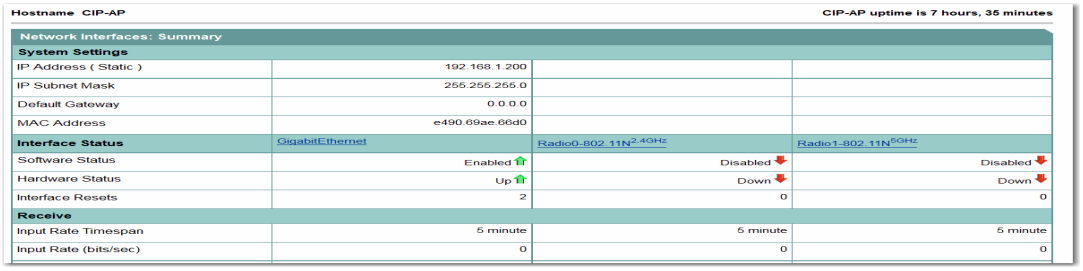
1. From the top menu, click Network.

   The Network Summary page appears.

2. Click Network Interface.

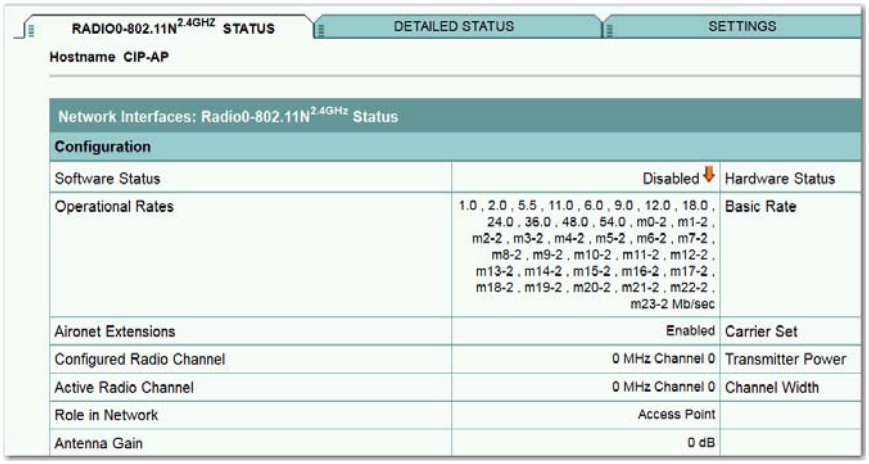
3. Click Summary.

   The Network Interfaces Summary page appears.



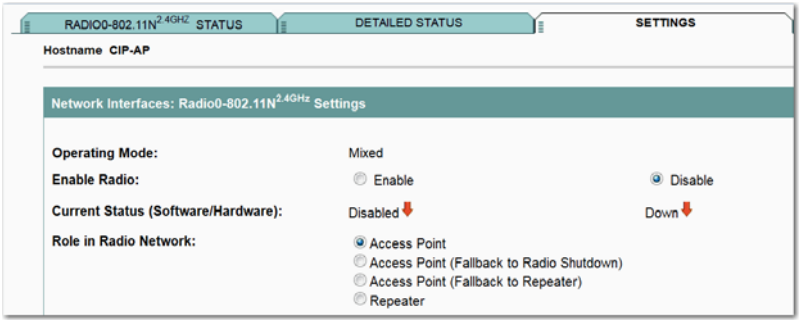
4. Click the radio you want to configure.

   The Radio Status page appears.



5. Click the Settings tab.

   The radio settings page appears.



6. Check Enable.

7. Click Apply.

TIP Your access point is now running but requires additional configuring to conform to your network operational and security requirements.

By default there are no SSIDs created so until you enable SSIDs, the access point is not able to accept wireless clients.

VLANs

If you use VLANs on your wireless LAN and assign SSIDs to VLANs, you can create multiple SSIDs by using any of the four security settings on the Express Security page. However, if you don't use VLANs on your wireless LAN, the security options that you can assign to SSIDs are limited because on the Easy Setup page encryption settings and authentication types are linked.

Without VLANs, encryption settings (ciphers) apply to an interface, such as the 2.4 GHz radio, and you cannot use more than one encryption setting on an interface.

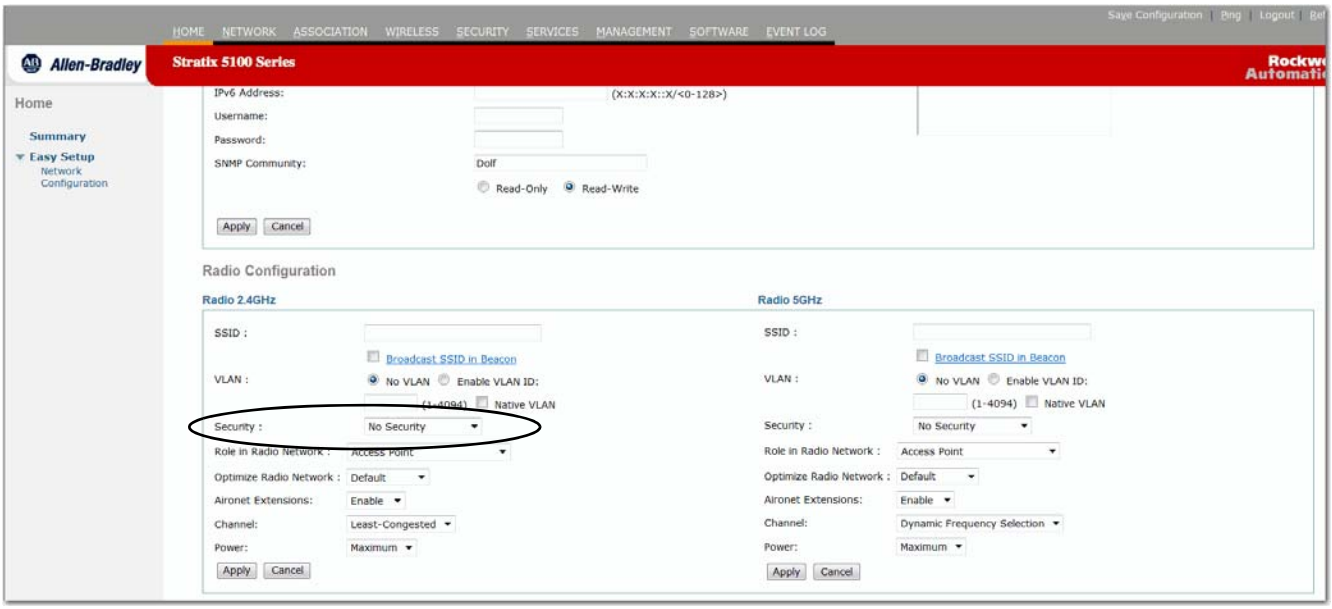
For example, when you create an SSID with static WEP with VLANs disabled, you cannot create additional SSIDs with WPA authentication because they use different encryption settings. If you find that the security setting for an SSID conflicts with another SSID, you can delete one or more SSIDs to eliminate the conflict.

Configure Security

After you assign the basic settings to the WAP, you must configure security settings to prevent unauthorized access to your network. Radio devices like the Stratix 5100 access point can communicate beyond the physical boundaries of your work site. Configuring securely settings prevents unauthorized access to your network.

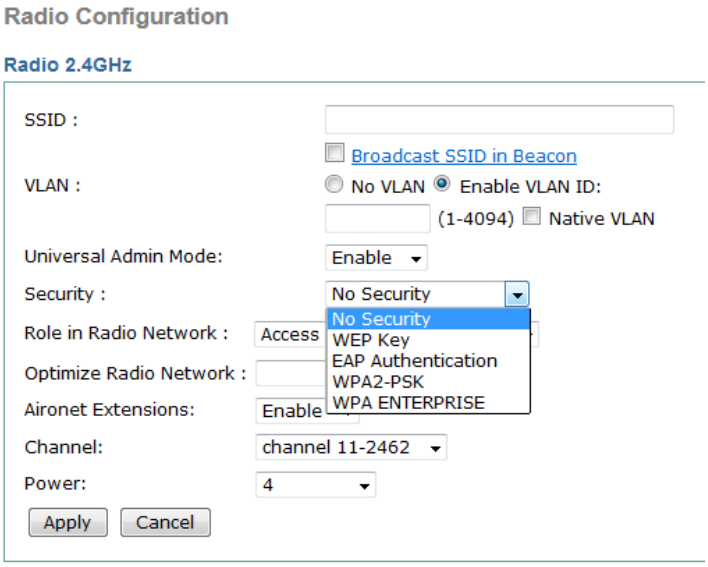
Use the Easy Setup page to create unique SSIDs and assign one of four security types to them.

Figure 13 - Easy Setup Radio Security Settings



Easy Set-up Page Security Types

There are four security types that you can assign to an SSID on the Easy Setup Network Configuration page.



For complete Security parameter descriptions see Table 12 on page 78.

Easy Setup Network Configuration Security Limitations

Because the Easy Setup page is designed for simple configuration of basic network configurations and security, the options available are a subset of the access point security capabilities.

For detailed information about configuring security, see Security Page on page 104.

Keep these limitations in mind when using the Easy Setup page:

Table 8 - Easy Setup Page Security Settings Limitations

You cannot	Notes
Edit SSIDs.	However, you can delete SSIDs and create them again.
Assign SSIDs to specific radio interfaces.	SSIDs are created and applied to each radio individually. To assign the same SSID to both radio interfaces, use the Security SSID Manager page or the Easy Setup page.
Configure multiple authentication servers.	To configure multiple authentication servers, use the Security Server Manager page.
Assign an SSID to a VLAN that is already configured on the wireless device.	To assign an SSID to an existing VLAN, use the Security SSID Manager page.
Configure combinations of authentication types on the same SSID (for example, MAC address authentication and EAP authentication).	To configure combinations of authentication types, use the Security SSID Manager page.

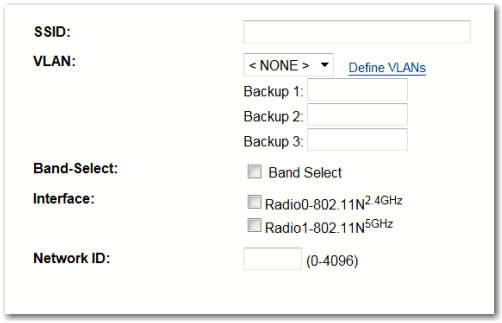
Create an SSID from the Security Menu

Follow these steps to create an SSID by using the Security menu. You can also define an SSID on the Easy Setup page.

See Security CLI Configuration Examples on page 200 for information on how to create an SSID by using CLI (Command Line Interface).

1. From the top menu, click Security.
2. From the left menu, click SSID Manager.

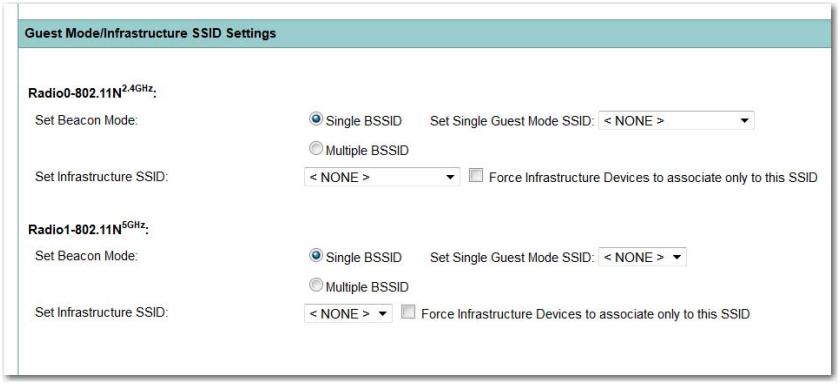
3. Click NEW and type the SSID in the SSID entry field.



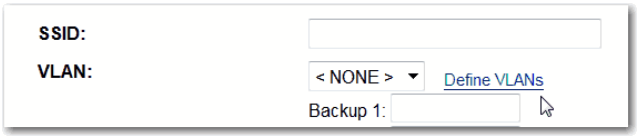
   - The SSID can contain up to 32 alphanumeric characters.
4. To broadcast the SSID in the access point beacon, select the SSID in the Set Single Guest Mode SSID dropbox.

   This setting is active only when the device is in the Root AP mode. When you broadcast the SSID, devices without pre-configured SSID can discover it and associate with the root access point.

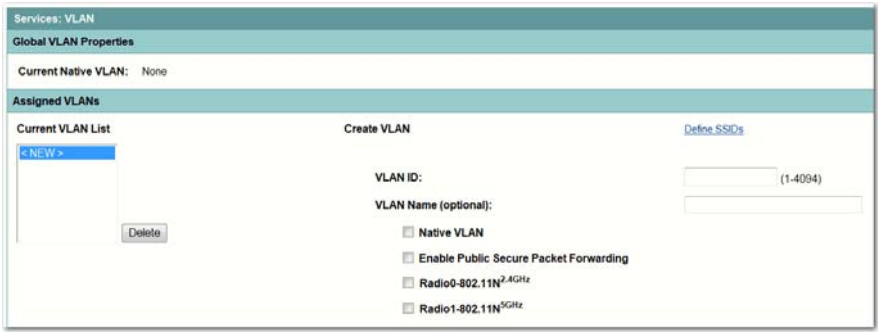
This option is useful when an SSID is used by guests or by client devices in a public space. If you do not broadcast the SSID, client devices cannot associate to the access point unless they know the SSID and have it pre-configured. Only one SSID can be in the beacon.



5. (Optional) Assign the SSID to a VLAN.
   a. Click Define VLANS.



   b. Select NEW.
   c. Enter a VLAN number (1...4094).
   d. Choose a radio and click Apply.



6. (Optional) Check the Native VLAN check box to mark the VLAN as the native VLAN.

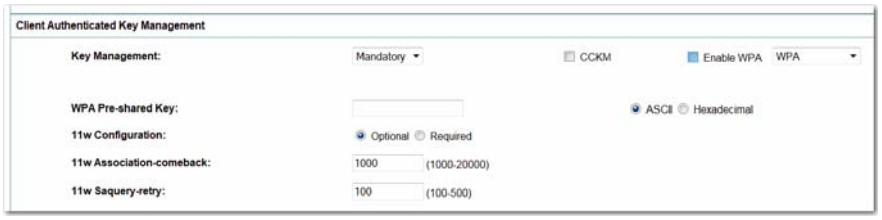
7. Choose the method of client authentication.

8. Choose the EAP authentication server priorities.

   You need to define EAP servers prior to this step.

9. If needed, choose the MAC Authentication Servers priorities.
10. Define the key management.

TIP If you don't use VLANs on your wireless LAN, the security options that you can assign to multiple SSIDs are limited. For detailed information, see Configure Virtual Local Area Networks (VLAN) on page 403.



11. Click Apply.

    The SSID appears in the SSID table at the top of the page.

Enable HTTPS for Secure Browsing

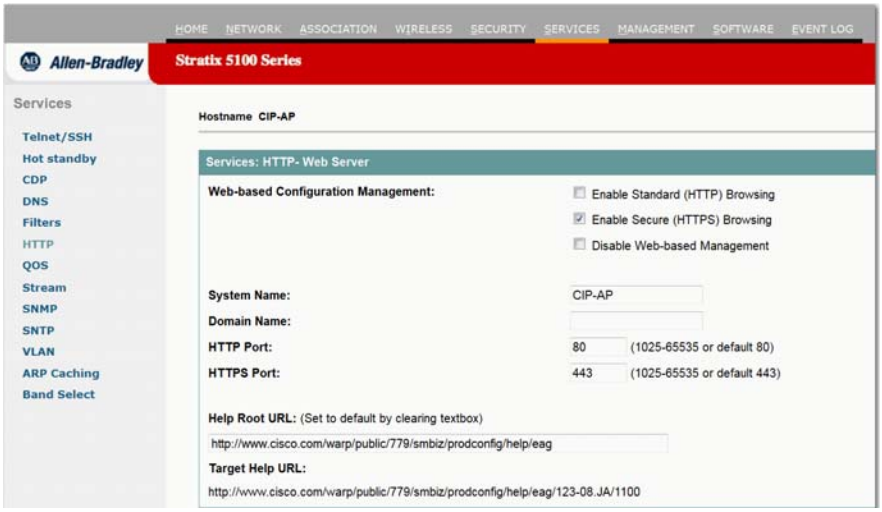
You can protect communication with the access point web browser interface by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Socket Layer (SSL) protocol.

When you enable HTTPS, your browser can lose its connection to the access point. If you lose the connection, change the URL in your browser address line from http://*ip_address* to https://*ip_address* and log into the access point again.

Follow these steps to enable HTTPS.

1. Browse to the Services: HTTP Web Server page.

Figure 14 - Services: HTTP Web Server Page

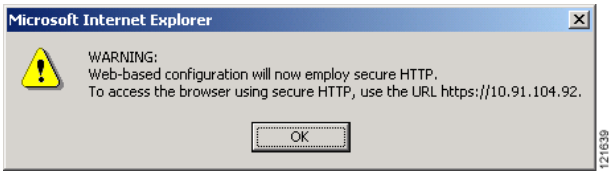


2. Click the Enable Secure (HTTPS) Browsing check box and click Apply.
3. Enter a domain name and click Apply.

TIP Although you can enable both standard HTTP and HTTPS, We recommend that you enable one or the other.

A warning page appears stating that you need to use HTTPS to browse to the access point. The page also instructs you to change the URL that you use to browse to the access point from *http* to *https*.

Figure 15 - HTTPS Warning page



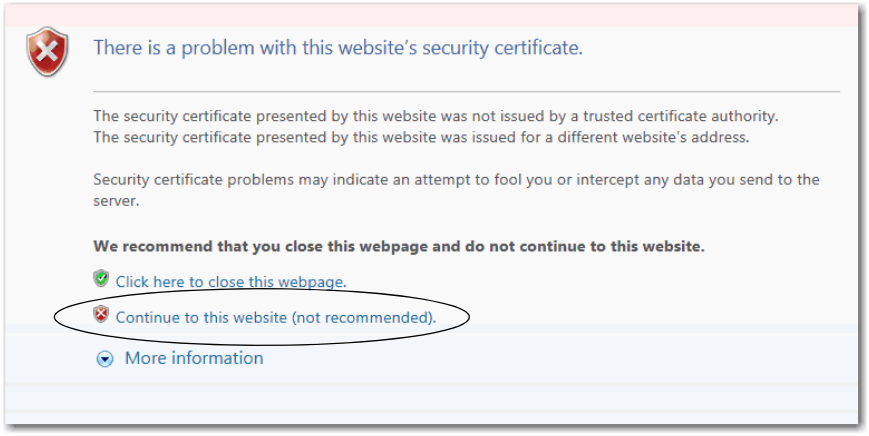
4. Click OK.

The address in your browser address line changes from:

http://*ip-address* to https://*ip-address*.

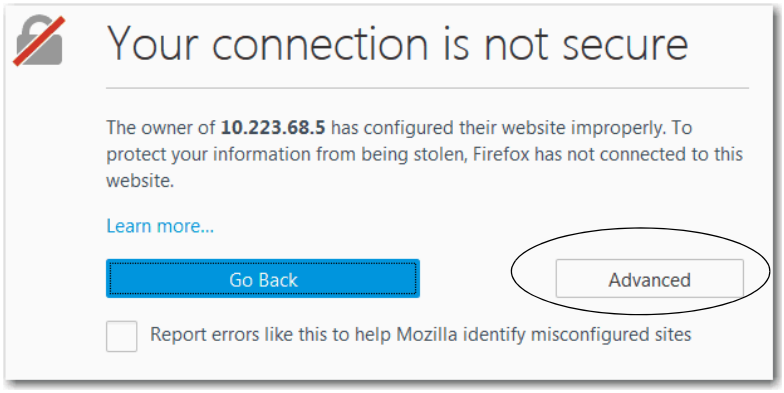
Another warning page appears stating that the access point security certificate is valid but is not from a known source. However, you can accept the certificate with confidence because the site in question is your own access point.

5. (Internet Explorer). If the following message appears, click Continue to this website.

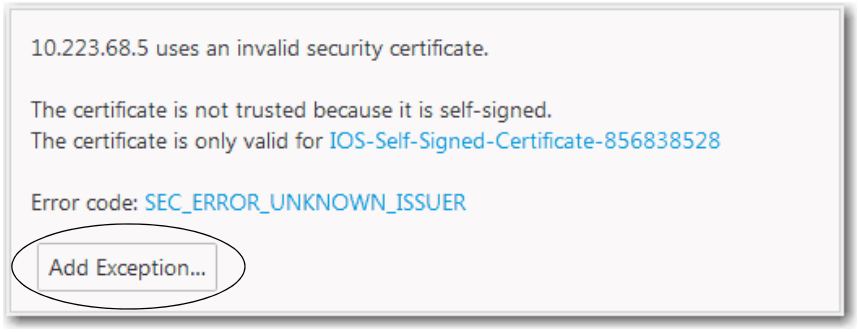


(Firefox). If the following message appears, do the following:

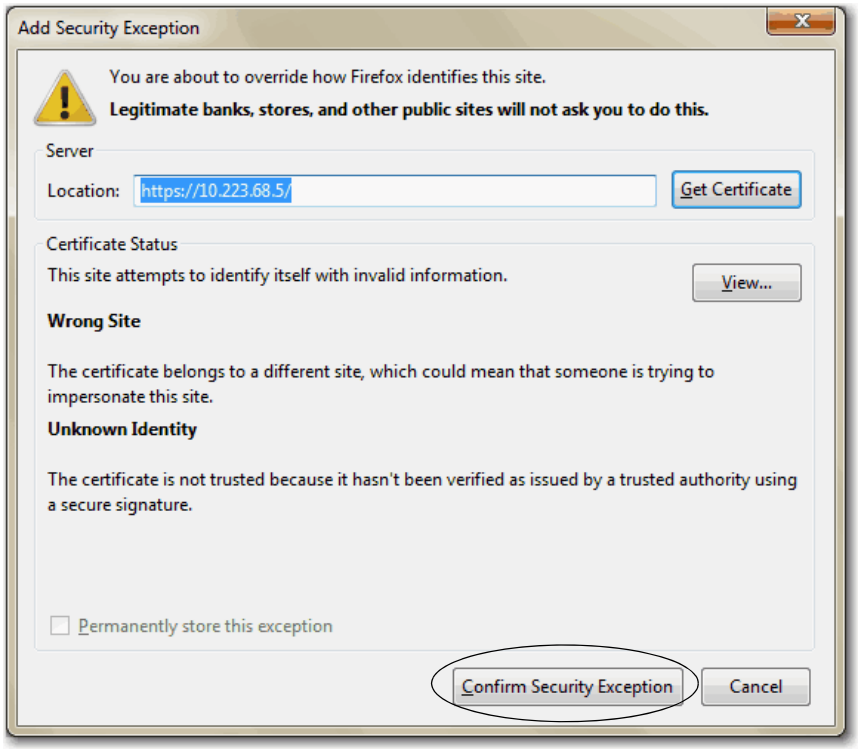
a. Click Advanced.



b. Click Add Exception.

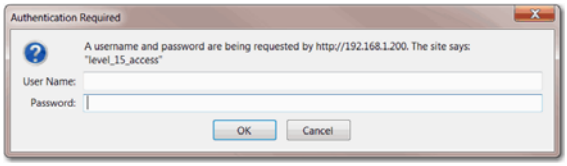


c. Click Confirm Security Exception.



The access point login dialog box appears and you must log into the access point again.

6. On the Device Manager Login window, enter the username and password.



CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in Enable HTTPS for Secure Browsing on page 62.

In this example, the access point system name is ap1100, the domain name is company.com, and the IP address of the DNS server is 10.91.107.18.

```
AP# configure terminal
AP(config)# hostname ap1100
AP(config)# ip domain name company.com
AP(config)# ip name-server 10.91.107.18
AP(config)# ip http secure-server
AP(config)# end
```

For complete descriptions of the commands used in this example, see Using the Cisco IOS Command-Line Interface Configuration Guide 15.3.

Delete an HTTPS Certificate

The access point generates a certificate automatically when you enable HTTPS. However, if you need to change the fully qualified domain name (FQDN) for an access point, or you need to add an FQDN after enabling HTTPS, you can delete the certificate. Follow these steps to delete the certificate.

1. Browse to the Services>HTTP page.
2. Uncheck the Enable Secure (HTTPS) Browsing check box to disable HTTPS.
3. Click Delete Certificate.
4. Re-enable HTTPS.

   The access point generates a new certificate by using the new FQDN.

Disable the Web Browser Interface

To prevent all use of the web browser interface, check the Disable Web-Based Management checkbox on the Services: HTTP-Web Server page and click Apply.

To re-enable the web browser interface, enter this CLI global configuration command.

```
ap(config)# ip http secure-server
```

Notes:

Stratix 5100 Device Manager Parameter Definitions

This chapter defines the parameter settings for each page in Device Manager.

Topic	Page
Device Manager System Management Tabs	71
Easy Setup Network Configuration Page	72
Network Configuration Settings on the Easy Setup Page	73
Radio Configuration Settings on the Easy Setup Page	75
Security Configuration Settings on the Easy Setup Page	78
Network Page	79
Network Interface Summary Page	80
Network Interface IP Address Page	83
Network Interface: Radio0-802.11n 2 GHz and Radio1-802.11n 5 GHz Status	88
Network Interface Radio Settings Page	92
Association Page	97
Wireless Page	99
Security Page	104
Admin Access Page	106
Encryption Manager Page	107
SSID Manager Page	109
Server Manager Page	115
Server Manager Global Properties	117
AP Authentication	119
AP Authentication Certificates	121
Intrusion Detection	123
Local RADIUS Server	125
Services Page	131
Telnet/SSH	131
Hot Standby Page	133
CDP Page	134
DNS Page	136
Filters Page	137
MAC Address Filters Page	138
HTTP Page	143

Topic (Continued)	Page
QoS Policies Page	145
Stream Page	150
SNMP Page	151
SNTP Page	154
VLAN Page	155
ARP Caching Page	157
Band Select Page	158
Management Page	160
Software Page	162
Software Upgrade HTTP Page	163
Software Upgrade TFTP Page	164
System Configuration Page	165
Event Log Page	167

Device Manager System Management Tabs

After you have initially configured the access point with an IP address and have logged on, the Home page appears. The Home page provides a summary of associated stations, system events, and port status.

The System Management tabs provide a consistent way to view and save configuration information. An expanded menu appears on the left for each System Management topic.

TIP It is important to remember that when you click back in the web browser it returns you to the previous page, the software does not save any changes you have made. Changes are applied only when you click Apply.

Figure 16 - Stratix 5100 Device Manager Home Page

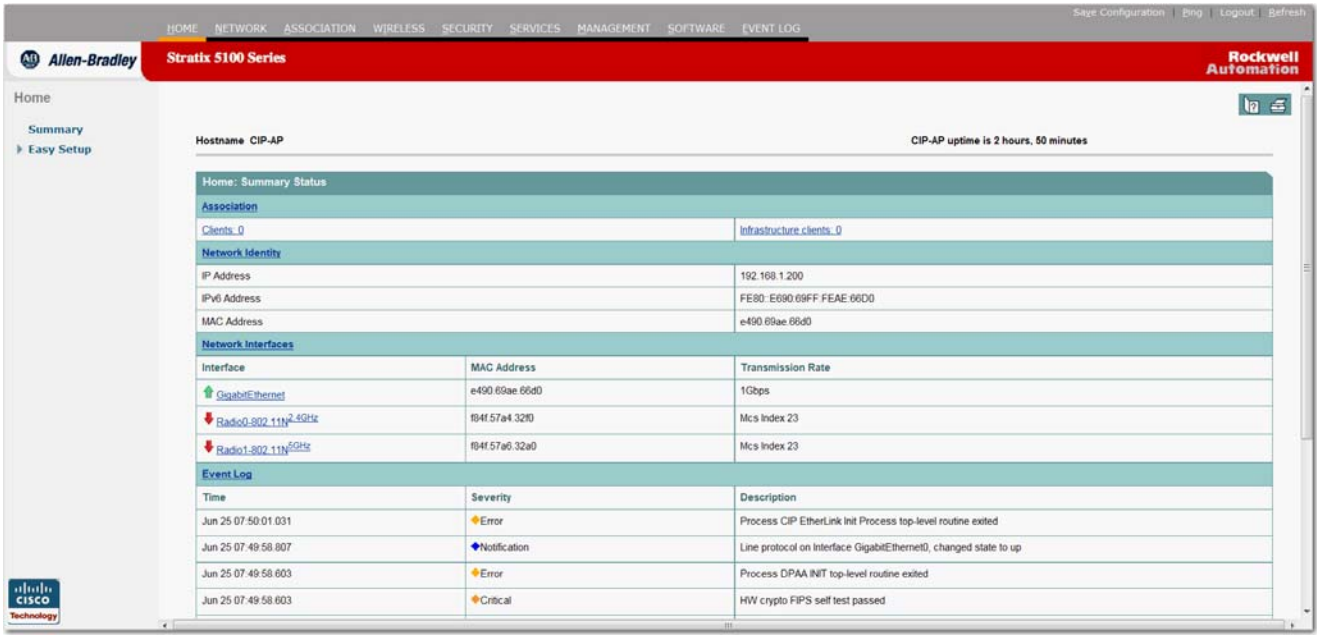


Table 9 - Stratix 5100 Device Manager System Management Tab Descriptions

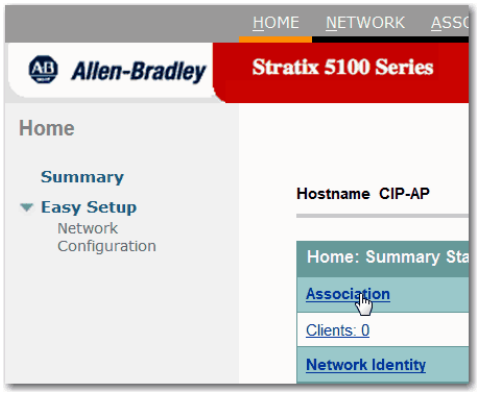
Item	Description
Home	The Home-Summary page provides the wireless device status page with information on the number of radio devices associated to the wireless device, the status of the Ethernet and radio interfaces, and a list of recent wireless device activity.
Network	The Summary page provides status and statistics for the Ethernet and radio interfaces. Network Interface has a summary of the interfaces and links to configuration pages for each interface. See Network Page on page 79 for details.
Association	Provides a list of all devices on your wireless LAN, listing their system names, network roles, and parent-client relationships. See Association Page on page 97 for details.
Wireless	Provides a summary of the Wireless Domain Services. See Wireless Page on page 99 for details.
Security	Provides access to security services, such as Administrative Access and SSID Manager. See Security Page on page 104 for details.
Services	Provides access to the other services available, for example, HTTP and QOS. See Services Page on page 131 for details.

Table 9 - Stratix 5100 Device Manager System Management Tab Descriptions (Continued)

Item	Description
Management	Location where you manage a guest user account and WebAuth. The WebAuth is where you can customize the appearance of the Login page if Web Authentication is enabled for the SSID. See Management Page on page 160 for details.
Software	Provides access to upgrading and configuring your software. See Software Page on page 162 for details.
Event Log	Creates the wireless device event log and provides links to configuration pages where you can select events to be in traps, set event severity levels, and set notification methods. See Event Log Page on page 167 for details.

Easy Setup Network Configuration Page

The Easy Setup feature on the navigation bar lists the basic settings for network configuration that includes system name, IP address, and role in radio network.



Network Configuration Settings on the Easy Setup Page

This is the Network configuration page under Easy Setup. Easy Setup contains an abbreviated version of parameters from the Network page.

Figure 17 - Network Configuration Easy Setup

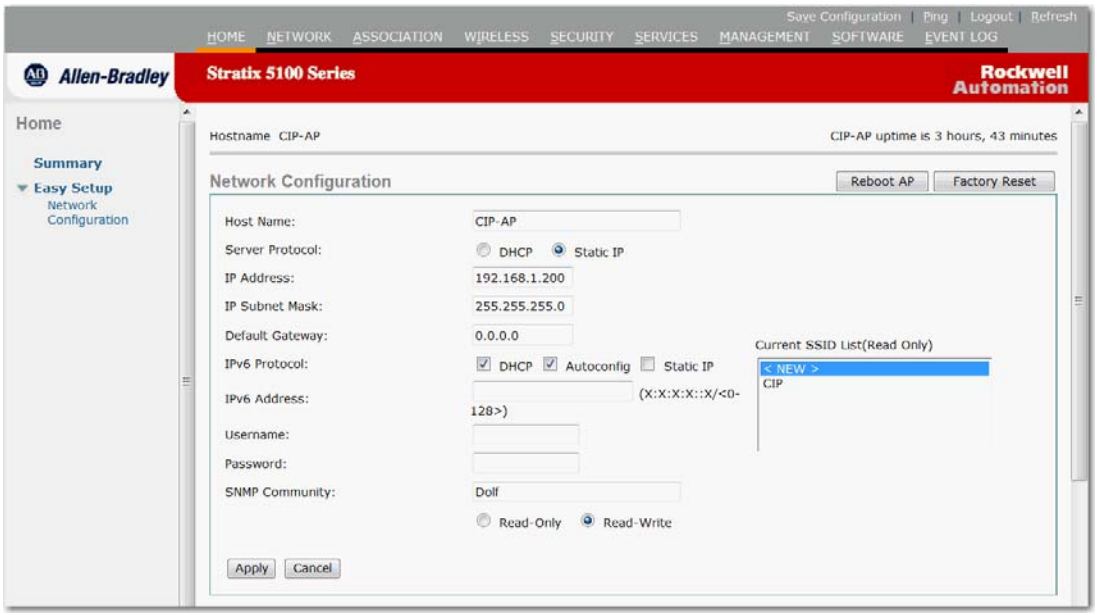


Table 10 - Network Configuration Parameter Descriptions

Parameter	Description
Host Name	The host name helps identify the wireless device on your network. The host name appears in the titles of the management system pages. You can enter up to 32 characters for the system name. However, when the wireless device identifies itself to client devices, it uses only the first 15 characters in the system name. Make sure a unique portion of the system name appears in the first 15 characters. **WARNING:** When you change the system name, the wireless device resets the radios, causing associated client devices to disassociate and disconnect.
Server Protocol	Choose the item that matches the network method of IP address assignment. • DHCP, IP addresses are automatically assigned by your network DHCP server. • Static IP, The wireless device uses a static IP address that you enter in the IP address field.
IP Address	Use this setting to assign or change the wireless device IP address. If DHCP is enabled for your network, leave this field blank. If the wireless device IP address changes while you are configuring the wireless device by using the web browser interface or a Telnet session over the wired LAN, you lose your connection to the wireless device. If you lose your connection, reconnect to the wireless device by using its new IP address. • If DHCP is not enabled, the IP address you enter in this field is the device's IP address. • If DHCP is enabled, this field provides the IP address only if a server responds with an IP address for the device.

Table 10 - Network Configuration Parameter Descriptions (Continued)

Parameter	Description
IP Subnet Mask	Enter the IP subnet mask provided by your network administrator so the IP address can be recognized on the LAN. • If DHCP is not enabled, this field is the subnet mask. • If DHCP is enabled, this field provides the subnet mask only if a server responds to the DHCP request otherwise leave it blank.
Default Gateway	Enter the default gateway IP address provided by your network administrator. If DHCP is enabled, leave this field blank.
IPv6 Protocol	Determine how the IPv6 addresses are allocated, for example DHCP, Static IP, and Auto-configuration.
IPv6 Address	Value for the address, for example, FE80::E690:69FF:FEAE:66D0 (X:X:X:X::X/<0-128>) If IPv6 DHCP is enabled leave this field blank.
Username	The username that you want to use to login to the WAP.
Password	The password that you want to use to login to the WAP. The username and password are stored locally on the WAP and provide full read-write access to the user.
SNMP Community	• To use Simplified Network Management Protocol (SNMP), enter a community name. SNMP is an application-layer protocol that supports message-oriented communication between SNMP management stations and agents. This community name automatically appears in the list of users authorized to view and make changes to the management system when SNMP is enabled. • The SNMP community string is used like a username and is for authentication, privacy, and authorization services within SNMP. Choose for this community to have read-only or read/write capabilities. – Read-only indicates that the access point lets only SNMP read access. Using this option, you cannot change access point configuration settings. – Read-write indicates that the access point lets SNMP read and write access. This setting lets you change the access point configuration.
Current SSID List	• List of SSIDs configured on the device.

If you want to setup basic configuration parameters in CLI, see Configure the Stratix 5100 WAP Using the Command-Line Interface on page 191.

Radio Configuration Settings on the Easy Setup Page

This page contains information about the status of GigabitEthernet and 802.11a/n and 802.11g/n interfaces, depending on the radio that is installed on the access point. This is an abbreviated parameters from the radio settings tab in Network>Network Interface.

Figure 18 - Radio Configuration Settings on the Network Configuration Page

Table 11 - Radio Configuration Parameter Descriptions

Parameter	Description
SSID	Identifies the SSID that client devices must use to associate with a device. You must create an SSID before you can enable the radio interface.The SSID helps client devices distinguish between multiple wireless networks in the same vicinity. In this text field, you can not use these characters: TAB, ?, $, +, !, #, and ;.
Broadcast SSID in Beacon	Includes SSID in the AP beacon to allow clients to discover the network automatically.
Security	• No Security • WEP Key WEP security is a legacy method that should not be used since WEP keys are easily compromised. • EAP Authentication • WPA
VLAN	Choose a VLAN setting. • VLAN If you use VLANs on your wireless LAN and assign SSIDs to VLANs, you can create multiple SSIDs using any of the four security settings on the Express Security page. However, if you do not use VLANs on your wireless LAN, the security options that you can assign to SSIDs are limited because, on the Express Security page, encryption settings and authentication types are linked. Without VLANs, encryption settings (ciphers) apply to an interface, such as the 2.4 GHz radio, and you cannot use more than one encryption setting on an interface. • No VLAN Select this setting if you are not using VLANs. • Enable VLAN ID Select this setting if you want to specify the VLAN ID tied to the SSID. • Native VLAN Select this setting if you want this VLAN ID to be the native VLAN. Native VLAN traffic is not tagged with the VLAN ID in the Ethernet frame.

Table 11 - Radio Configuration Parameter Descriptions (Continued)

Parameter	Description
Role in Radio Network	This is where you choose a role in the radio network. The choices are: • Access point • Repeater • Root bridge • Non-root bridge • Workgroup bridge • Universal workgroup bridge • Scanner • Spectrum – Choose Access Point (Root) if the wireless device is connected to the wired LAN. In this mode, wireless client devices are allowed to associate to the access point. – A root device accepts associations from clients and bridges wireless traffic from the clients to the wired LAN. This setting can be applied to any access point.
Repeater	Choose Repeater (Non-root) if it is not connected to the wired LAN. A non-root device accepts associations from clients and bridges wireless traffic from the clients to root access point connected to the wireless LAN. This setting can be applied to any access point. When the Ethernet port is disabled, the wireless device becomes a repeater and associates to a nearby root access point. You do not have to specify a root access point that the fallback repeater associates; the repeater automatically associates to the root access point that provides the best radio connectivity.
Root Bridge	Establishes a link with a non-root bridge. In this mode, the device also accepts associations from clients and connects directly to the main Ethernet LAN network.
Workgroup Bridge	Specifies that the WAP operates as a workgroup bridge connected to a wired Ethernet LAN network through an Ethernet hub or switch. In workgroup bridge mode, the WAP associates to another access point as a client and provides a network connection to the devices connected to its Ethernet port. The workgroup bridge must associate to a Cisco Aironet or Stratix 5100 access point on your network.
Non-root Bridge	In this mode, the device establishes a link with a root bridge. Specifies that the unit is operating as a non-root bridge, that it connects to a remote LAN network, and that it must associate with a Cisco Aironet or Stratix 5100 root bridge using the wireless interface.
Universal Workgroup Bridge	Provides the means for the Stratix 5100 WAP to be configured as a wireless bridge and to associate with non-Cisco and non-Rockwell access points.
Scanner	Specifies that the access point operates as a radio scanner only and does not accept associations from client devices. As a scanner, the access point collects radio data and sends it to the WDS access point on your network.
Spectrum	Specifies that the AP operates as a dedicated RF spectrum sensor that used with the Cisco Spectrum Expert software.
Optimize Radio Network for	Use this setting to choose either preconfigured settings for the wireless device radio or customized settings for the wireless device radio. The options are default, range, and throughput.

Table 11 - Radio Configuration Parameter Descriptions (Continued)

Parameter	Description
Aironet Extensions	Choose Enable if there are only Rockwell Automation WAPs or Cisco Aironet devices on your wireless LAN and the unit is operating as an access point or workgroup bridge or if the unit is operating as a repeater. This setting must be set to Enable for you to use features such as load balancing, message integrity check (MIC), or Temporal Key Integrity Protocol (TKIP).
Channel	• 2.4 GHz – Least Congested – Channel Number/Frequency • 5 GHz – Dynamic Frequency Selection – Channel Number/Frequency
Power	• 2.4 GHz – Maximum, Specific power level (dBm) • 5 GHz – Maximum, Specific power level (dBm)

Security Configuration Settings on the Easy Setup Page

You can configure a limited number of security parameters for the Stratix 5100 WAP on the Easy Setup page. You may need to configure additional security parameters after you completed Easy Setup. There are four choices:

- No Security
- WEP Key
- EAP Authentication
- WPA2-PSK
- WPA Enterprise

Use the Security page to review and configure the security settings for the access point.

You can configure security also by using CLI, see Security CLI Configuration Examples on page 200.

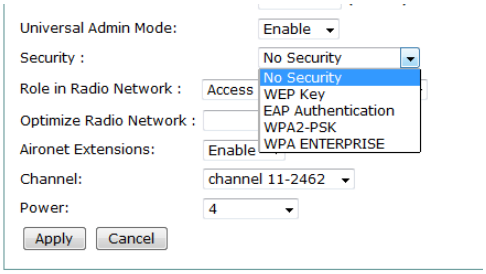


Table 12 - Security Types on Easy Set-up Security Setup Page

Security Type	Description	Security Features Enabled
No Security	This is the least secure option. Use this option only for SSIDs used in a public space and assign it to a VLAN that restricts access to your network.	None.
WEP Key	This option is more secure than no security. **WARNING:** Static WEP keys are vulnerable to attack. WEP security is a legacy method that should no longer be used.	Mandatory WEP. Client devices cannot associate by using this SSID without a WEP key that matches the wireless device key.
WPA2-PSK	This option enables Wi-Fi Protected Access (WPA) version 2 with pre-shared keys.	The key is stored in the encrypted form on the wireless device. You are required to manually enter a secret key on the access point and all clients.
EAP Authentication	This option enables 802.1X authentication, for example, LEAP, PEAP, EAP-TLS, EAP-FAST, EAP-TTLS, EAP-GTC, EAP-SIM, and other 802.1X/EAP based products. This setting uses mandatory encryption, open authentication + EAP, network EAP authentication, no key management, RADIUS server (authentication port 1645). You are required to enter the IP address and shared secret for an authentication RADIUS server on your network (server authentication port 1645). If your network does not have a RADIUS server, consider using an access point as a local authentication server, see Configure an Access Point as a Local Authenticator on page 303.	Mandatory 802.1X authentication. Client devices that associate by using this SSID must perform 802.1X authentication. If radio clients are configured to authenticate by using EAP-FAST, open authentication with EAP can also be configured. If you do not configure open authentication with EAP, the following GUI warning message appears: **ATTENTION:** Network EAP is used only for LEAP authentication. If radio clients are configured to authenticate by using EAP-FAST, Open Authentication with EAP can also be configured.
WPA Enterprise	Wi-Fi Protected Access (WPA) permits wireless access to users authenticated against a database through the services of an authentication server, then encrypts their IP traffic with stronger algorithms than those used in WEP. This setting uses encryption ciphers, TKIP, open authentication + EAP, network EAP authentication, key management WPA mandatory, and RADIUS (server authentication port 1645). As with EAP authentication, you must enter the IP address and shared secret for an authentication server on your network (server authentication port 1645).	Mandatory WPA authentication. Client devices that associate by using this SSID must be WPA-capable. If radio clients are configured to authenticate by using EAP-FAST, open authentication with EAP must be configured. If you don't configure open authentication with EAP, the following GUI warning message appears: **ATTENTION:** Network EAP is used only for LEAP authentication. If radio clients are configured to authenticate by using EAP-FAST, Open Authentication with EAP must be configured.

Network Page

The Network page contains information about the network map and adjacent nodes. The Network Interface page provides the status of GigabitEthernet and 802.11a/n and 802.11g/n interfaces.

Choose Enable or Disable for Network Map capabilities. If you select Enable, it is best to switch back to the Disable default before leaving the page because the time to discover the network can greatly increase the system load.

Figure 19 - Network Map

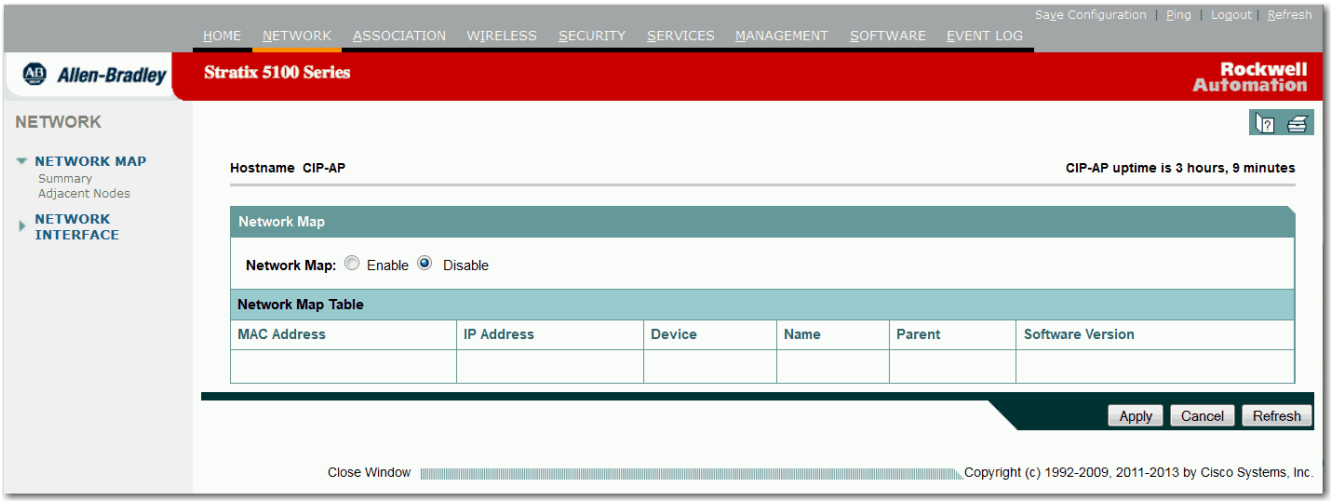


Table 13 - Stratix 5100 Network Map Parameter Descriptions

Item	Description
Network Map	
Summary	The Network Map page provides information for any device on your wireless network. The Network Map page does not list wired devices on your LAN. If you need to see what wired devices you have on a LAN behind the workgroup bridges, see Association Page on page 97. Choose Enable to view the network map. If you choose Enable, switch back to Disable before leaving the page because the time to discover the network can greatly increase the system load.
MAC Address	The unique identifier assigned to the device by the manufacturer.
IP Address	The IP address of the device.
Device	The type of device (client, access point, bridge, and so on).
Name	The name given to this device.
Software Version	The software version currently running on your device.
Radio	Specifies whether the radio is 802.11a/n or 802.11g/n.

Table 13 - Stratix 5100 Network Map Parameter Descriptions (Continued)

Item	Description
Channel	Specifies what channel the radio is using.
Age (hrs)	Specifies the amount of time the access point remains on the access point adjacent list before being removed for lack of activity.
SSID	Identifies the SSID that client devices must use to associate with a device. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity.
Adjacent Nodes	This is the amount of time the access point remains on the access point adjacent list before being removed for lack of activity. AP Age Timeout 1…1000 hours

Network Interface Summary Page

Network Interface

- Summary
- IP Address
- GigabitEthernet
- Radio0-802.11n 2.4 GHz
- Radio1-802.11n 5 GHz

The Summary page contains information about the status of GigabitEthernet and 802.11a/n or 802.11g/n interfaces, depending on the radio installed on the access point.

Figure 20 - Network Interface Summary Page

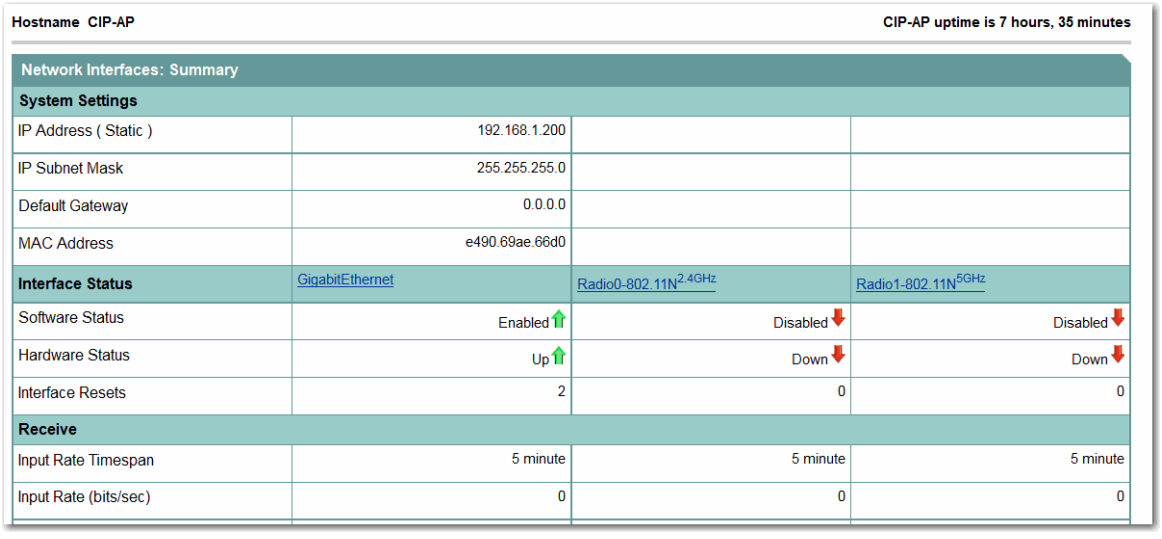


Table 14 - System Setting Parameter Descriptions

System Settings	Description
IP Address (DHCP) / IP Address (Static)	The IP address for the access point. The IP address can be assigned dynamically with DHCP or assigned statically.
IP Subnet Mask	The IP subnet mask identifies the subnetwork.
Default Gateway	The IP address of your default internet gateway is displayed here.
MAC Address	The Media Access Control address is a unique identifier assigned to the network interface by the manufacturer.
Interface Status	The status of GigabitEthernet, Radio0-802.11N$^{2.4\ GHz}$, and Radio0-802.11N$^{5\ GHz}$.
Software Status	Indicates whether the GigabitEthernet, 802.11a/n or 802.11g/n interfaces have been enabled or disabled by the operator.
Hardware Status	Indicates whether the line protocol for the GigabitEthernet, 802.11a/n or 802.11g/n interface is up or down.
Interface Resets	The number of times an interface has been reset.
Input Rate Timespan	Timespan at which interface statistics are displayed.
Input Rate (bits/sec)	The average number of bits per second transmitted in the designated input rate timespan.
Input Rate (packets/sec)	The average number of packets per second transmitted in the designated input rate timespan.
Time Since Last Input	The number of hours, minutes, and seconds since the last packet was successfully received by an interface. Knowing this time helps you determine the load on the interface and helps locate network problems.
Total Packets Input	The total number of error-free packets received by the system.
Total Bytes Input	The total number of error-free bytes received by the system.
Broadcast Packets	The total number of broadcast packets received by the interface.
Total Input Errors	The total number of input-related errors that occurred including runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
Overrun Errors	The number of times the receiver hardware was unable to send received data to a hardware buffer because the input rate exceeded the receiver's ability to process the data.
Ignored Packets	The number of received packets ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
Throttles	The number of times the receiver on the port was disabled, possibly because of a buffer or processor overload.
Output Rate Timespan	Timespan at which interface statistics are displayed.
Output Rate (bits/sec)	The average number of bits transmitted per second in the designated output rate timespan.
Output Rate (packets/sec)	The average number of packets transmitted per second in the designated output rate timespan.
Time Since Last Output	The number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Knowing this time helps you determine traffic load on the interface and helps locate network problems.
Total Packets Output	The total number of messages transmitted by the system.
Total Bytes Output	The total number of bytes, including data and MAC encapsulation, transmitted by the system.
Total Output Errors	The sum of all errors that prevented the final transmission of datagrams out of the interface being examined.

Table 14 - System Setting Parameter Descriptions (Continued)

System Settings	Description
Last Output Hang	The number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in the Time Since Last Input, Time Since Last Output, or Last Output Hang fields exceeds 24 hours, the number of days and hours is printed.
Lost Parent Counts (Repeater Mode Only)	• No beacons The number of times the repeater stopped receiving beacons from the parent. • Deauthenticated The number of times the repeater received a deauthenticate packet from the parent. • Disassociated The number of times the repeater received a disassociate packet from the parent access point. • Time lost base The number of times the time base broadcast of the repeater changed to an amount that was too large. • Host request The number of times the link between the repeater and the parent access point was restarted. The operator changed the assigned parent. • Better parent found The number of times the repeater switched to a new parent access point because the repeater detected a stronger signal.
Association Statistics (Repeater Mode Only)	If the repeater is not associating to a parent, note these statistics. • SSID mismatched The number of times the repeater received a beacon or probe response that did not match the requested SSID. • Not specified AP The number of times the repeater received a response from a parent that has not been configured in the list of parents. • Rates mismatched The number of times the repeater received a response from a parent that does not support the rates that were requested. • Privacy mismatched The number of times the repeater received a response from a parent that does not support the privacy settings that were requested. • Authentication rejects The number of times the repeater received an authentication response from a parent containing a unsuccessful status. • Association timeout The number of times the repeater did not receive an associate request response from a parent access point.

Network Interface IP Address Page

Use this page to identify the configuration server protocol and to identify the IP Address, IP Subnet Mask, and Default Gateway IP Address.

Figure 21 - Network Interfaces IP Address

Table 15 - IP Address Parameter Description

Parameter	Description
Configuration Server Protocol	Set this parameter to match the network's method of IP address assignments. Choose DHCP if your network servers are using automatic assignment of IP addresses. Choose Static IP if fixed IP addresses are being assigned. Choose Disable DHCP Address Binding if you require compatibility with older DHCP servers. Normally, you do not check this checkbox. If you check the checkbox, no client identifier is sent to the DHCP server. The client identifier is used by the DHCP server to issue consistent IP addresses.
IP Address	Use this setting to assign or change the access point's IP address. If DHCP is not enabled for your network, the IP address you enter in this field is the access point's IP address. If DHCP is enabled, you cannot modify this field.
IP Subnet Mask	Enter an IP subnet mask to identify the subnetwork. If DHCP is not enabled, this field is the subnet mask. If DHCP is enabled, you cannot modify this field.
Default Gateway IP Address	Enter the IP address of the network's default gateway. If DHCP is enabled, you cannot modify this field unless Override DHCP Default Gateway is selected.
Override DHCP Default Gateway	This setting enables you to change the default gateway negotiated by the DHCP server. Enabling this feature can stop traffic to the access point; therefore, we recommend leaving the gateway to the one assigned by the DHCP server.

Network Interface GigabitEthernet Status Page

Use this page to review the status for the GigabitEthernet interface.

Figure 22 - Network Interface GigabitEthernet Status Page

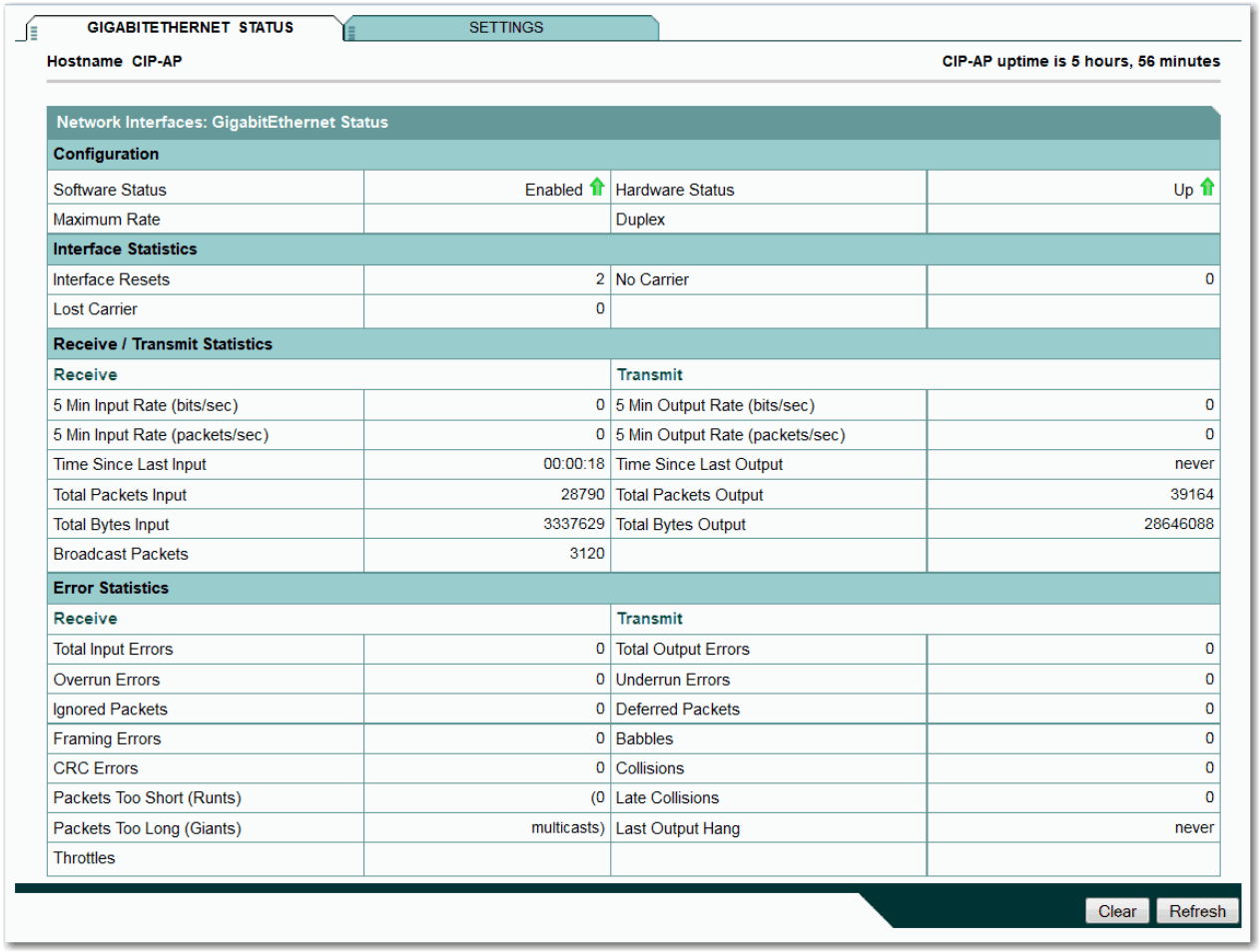


Table 16 - GigabitEthernet Status Parameter Descriptions

Parameter	Description
Configuration	
Software Status	Indicates whether the interface has been enabled or disabled by the operator.
Hardware Status	Indicates whether the line protocol for the interface is up or down.
Maximum Rate	The rate setting for the Ethernet interface, either 10 Mbps, 100 Mbps, or 1Gbps.
Duplex	The duplex setting for the Ethernet interface, either half or full.
Interface Statistics	
Interface Resets	The number of times an interface has been completely reset.
No Carrier	The number of times the carrier was not present during the transmission.
Lost Carrier	The number of times the carrier was lost during transmission.

Table 16 - GigabitEthernet Status Parameter Descriptions (Continued)

Parameter	Description
Receive Statistics	
5 min Input Rate (bits/sec)	The average number of bits per second transmitted in the last 5 minutes.
5 min Input Rate (packets/sec)	The average number of packets per second transmitted in the last 5 minutes.
Time Since Last Input	The number of hours, minutes, and seconds since the last packet was successfully received by an interface. Knowing this time helps you determine the traffic load on the interface and locate network problems.
Total Packets Input	The total number of error-free packets received by the system.
Total Bytes Input	The total number of bytes, including data and MAC encapsulation, received by the system.
Broadcast Packets	The total number of broadcast packet received by the interface.
Transmit Statistics	
5 min Output Rate (bits/sec)	The average number of bits transmitted per second in the last 5 minutes.
5 min Output Rate (packets/sec)	The average number of packets transmitted per second in the last 5 minutes.
Time Since Last Output	The number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Knowing this time helps you determine the traffic load on the interface and locate network problems.
Total Packets Output	The total number of messages transmitted by the system.
Total Bytes Output	The total number of bytes, including data and MAC encapsulation, transmitted by the system.
Error Statistics/Receive	
Total Input Errors	The total number of input-related errors that occurred, including runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
Overrun Errors	The number of times the receiver hardware was unable to send received data to a hardware buffer because the input rate exceeded the receiver's ability to process the data.
Ignored Packets	The number of received packets ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
Framing Errors	The number of packets received incorrectly having a CRC error and non-integer number of octets. These errors occur on a LAN as a result of a collision or malfunctioning Ethernet device.
CRC Errors	Cyclic redundancy checksum generated by the originating LAN station or far-end device that does not match the checksum calculated from the data received. These errors indicate noise or transmission problems on the LAN interface or LAN bus itself. A high number of CRC errors usually results in collisions or the transmission of bad data.
Packet too Short (Runts)	The number of packets that are discarded because they are smaller than the medium's minimum packet size. For example, any Ethernet packet that is less than 64 bytes is considered a runt.
Packet too Long (Giants)	The number of packets that are discarded because they exceed the medium's maximum packet size. For example, any Ethernet packet that is greater than 1,518 bytes is considered a giant.
Throttles	The number of times the receiver on the port was disabled, possibly due to buffer or processor overload.
Error Statistics/Transmit	
Total Output Errors	The sum of all errors that prevented the final transmission of datagrams from being examined.
Underrun Errors	The number of times the transmitter has run faster than the router can handle.
Deferred Packets	The number of packets deferred for an excessive period of time.

Table 16 - GigabitEthernet Status Parameter Descriptions (Continued)

Parameter	Description
Babbles	The number of times the transmit jabber time expired.
Collisions	The number of packets retransmitted because of an Ethernet collision (only applicable in half duplex).
Late Collisions	The number of late collisions. This collision usually results from an overextended LAN where the Ethernet or transceiver cable is too long, where too many cascaded multi-port transceivers are used, or where more than two repeaters are used between stations.
Last Output Hang	The number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in Time Since Last Input, Time Since Last Output, or Last Output Hang fields exceeds 24, the number of days and hours is printed.

Network Interface: GigabitEthernet Settings

You can use the settings page to define physical settings and AP authentication.

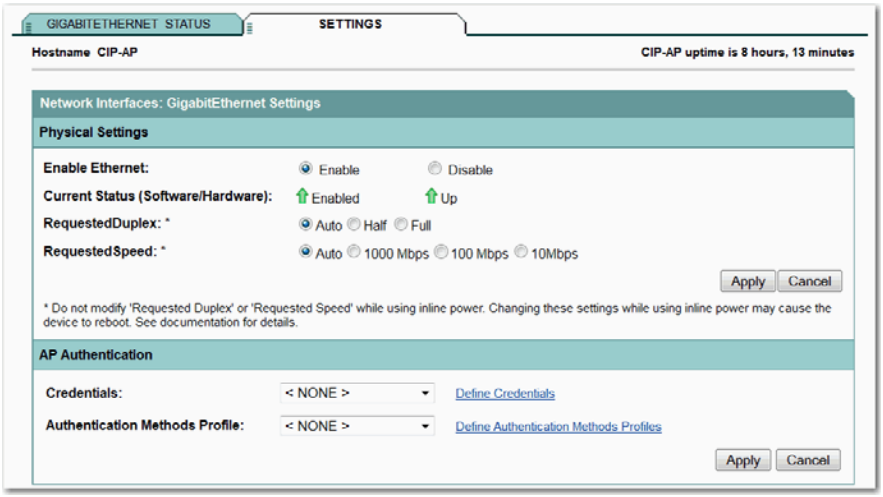
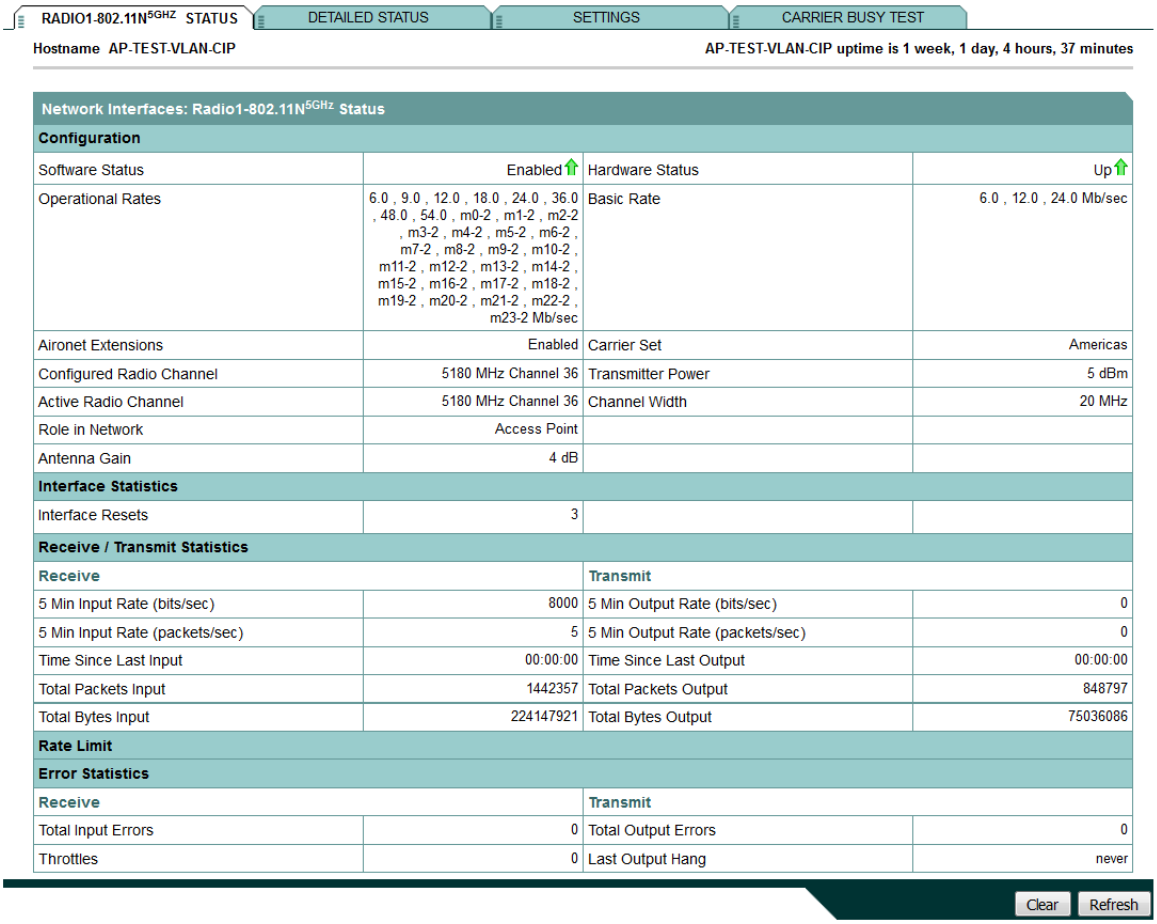


Table 17 - GigabitEthernet Parameter Descriptions

Parameter	Description
Physical Settings	
Enable Ethernet	Enable Disable
Current Status	Enabled Up
Requested Duplex	Duplex setting for the Ethernet interface; Auto, Half, and Full. **Important:** Do not modify Requested Duplex while using inline power. Changing these settings while using inline power can cause the device to reboot.
Requested Speed	Auto 1000 Mbps 100 Mbps 10 Mbps Important: Do not modify Requested Speed while using inline power. Changing these settings while using inline power can cause the device to reboot.
You must use settings for speed and duplex that match the ones on the network switch for example, if the switch use the auto setting, you have to use auto for the AP.	
AP Authentication	
Credentials	Choose a credential or click Define Credentials to go to AP Authentication where you can define the credentials you need. You only need AP credentials for the Gigabit Ethernet interface if your network switch is configured for the 802.1X authentication.
Authentication Methods Profile	Choose a profile or click Authentication Methods Profile to go to AP Authentication where you can define the profiles you need.

Network Interface: Radio0-802.11n 2 GHz and Radio1-802.11n 5 GHz Status

The Radio Status and the Detailed Status pages provide a summary of the current radio interface configuration and statistics.



RADIO1-802.11N5GHZ STATUS | DETAILED STATUS | SETTINGS | CARRIER BUSY TEST

Hostname AP-TEST-VLAN-CIP — AP-TEST-VLAN-CIP uptime is 1 week, 1 day, 4 hours, 37 minutes

Network Interfaces: Radio1-802.11N5GHz Status			
Configuration			
Software Status	Enabled	Hardware Status	Up
Operational Rates	6.0 , 9.0 , 12.0 , 18.0 , 24.0 , 36.0 , 48.0 , 54.0 , m0-2 , m1-2 , m2-2 , m3-2 , m4-2 , m5-2 , m6-2 , m7-2 , m8-2 , m9-2 , m10-2 , m11-2 , m12-2 , m13-2 , m14-2 , m15-2 , m16-2 , m17-2 , m18-2 , m19-2 , m20-2 , m21-2 , m22-2 , m23-2 Mb/sec	Basic Rate	6.0 , 12.0 , 24.0 Mb/sec
Aironet Extensions	Enabled	Carrier Set	Americas
Configured Radio Channel	5180 MHz Channel 36	Transmitter Power	5 dBm
Active Radio Channel	5180 MHz Channel 36	Channel Width	20 MHz
Role in Network	Access Point		
Antenna Gain	4 dB		
Interface Statistics			
Interface Resets	3		
Receive / Transmit Statistics			
Receive		**Transmit**	
5 Min Input Rate (bits/sec)	8000	5 Min Output Rate (bits/sec)	0
5 Min Input Rate (packets/sec)	5	5 Min Output Rate (packets/sec)	0
Time Since Last Input	00:00:00	Time Since Last Output	00:00:00
Total Packets Input	1442357	Total Packets Output	848797
Total Bytes Input	224147921	Total Bytes Output	75036086
Rate Limit			
Error Statistics			
Receive		**Transmit**	
Total Input Errors	0	Total Output Errors	0
Throttles	0	Last Output Hang	never

Clear Refresh

Table 18 - Radio Interface Configuration and Statistics Parameter Descriptions

Parameter	Description
Configuration	
Software Status	Indicates whether the interface has been enabled or disabled by the operator.
Operational Rates	The data rates (expressed in megabits per second) the device uses for data transmission. The device always attempts to transmit at the highest rate selected. if high rate of errors and retransmissions occur, the device steps down to the highest rate that enables data transmission.
Aironet Extensions	If compatibility with non-Cisco/Aironet products is required, deselect Aironet Extensions. Disabling this option limits several advanced features of the access point, such as load balancing, MIC, and TKIP.
Carrier Set	Indicates the regulatory domain that the access point is operating on. The carriers sets constrain the frequencies and power levels available.
Current Radio Channel	The current channel and frequency of the 802.11a/n or 802.11g/n radio.
Transmitter Power	The power level of the radio transmission. The default power setting is the highest transmit power allowed in your regulatory domain.

Table 18 - Radio Interface Configuration and Statistics Parameter Descriptions (Continued)

Parameter	Description
Hardware Status	Indicates whether the line protocol for the interface is up or down. Normally, if the Software Status is enabled, the Hardware Status is up. An error condition occurs if the Software Status is enabled and the Hardware Status is down.
Basic Rate	Enables transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set as a basic rate.
Role in Network	A Stratix 5100 in the Access Point (Root) mode connects wireless clients to the wired network. A Stratix 5100 in the Workgroup Bridge mode becomes a wireless client to the Root AP and is used to connect one or many wired clients via the wireless link.
Antenna Gain	The status of the antennae gain can be viewed. You can set the gain using the web interface (Radio Interface - Detailed Settings). Configuring the antenna gain does not actually change the antenna characteristics or the resulting emitted power. This parameter is only used for RF planning purposes by a network management software.
Interface Statistics	
Interface Resets	The number of times an interface has been completely reset.
Receive Statistics	
5 min Input Rate (bits/sec)	The average number of bits per second received in the last 5 minutes.
5 min Input Rate (packets/sec)	The average number of packets per second received in the last 5 minutes.
Time Since Last Input	The number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. Knowing this time helps you determine the traffic load on the interface and helps locate network problems.
Total Packets Input	The total number of error-free packets received by the system.
Total Bytes Input	The total number of bytes, including data and MAC encapsulation, received by the system.
Transmit Statistics	
5 min Output Rate (bits/sec)	The average number of bits transmitted per second in the last 5 minutes.
5 min Output Rate (packets/sec)	The average number of packets transmitted per second in the last 5 minutes.
Time Since Last Output	The number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Knowing this time helps you determine the traffic load on the interface and helps locate the network problems.
Total Packets Output	The total number of messages transmitted by the system.
Total Bytes Output	The total number of bytes, including data and MAC encapsulation, transmitted by the system.
Error Statistics	
Total Input Errors	The total number of input related errors that occurred including runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
Total Output Errors	The sum of all errors that prevented the final transmission of datagrams from being examined.
Last Output Hang	The number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in the Time Since Last Input, Time Since Last Output, or Last Output Hang fields exceeds 24, the number of days and hours is printed.
Throttles	The number of times the receiver on the port was disabled, possibly because of buffer or processor overload.

Detailed Status

This page shows status details for the interface.

Figure 23 - Interface Detailed Status

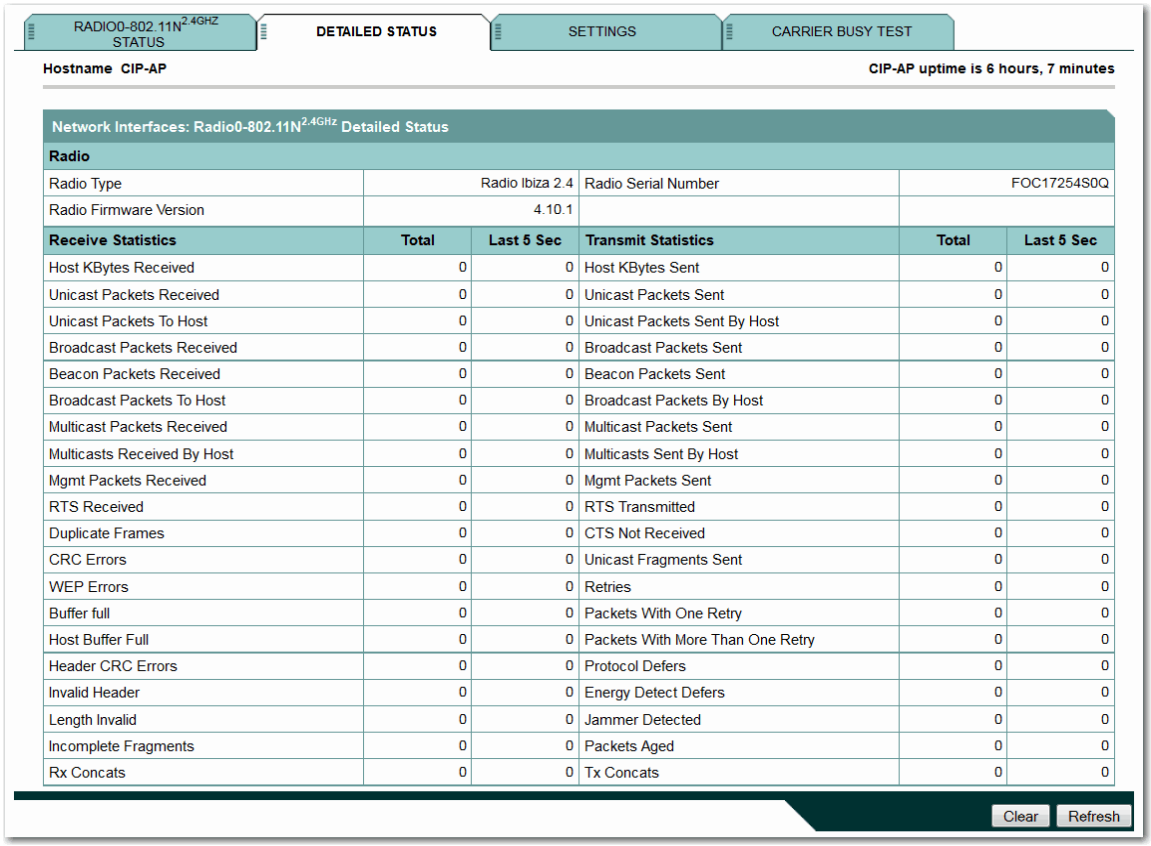


Table 19 - Network Interfaces: Radio0-802.11N2.4 GHz and 5 GHz Detailed Status

Parameter	Description
Radio	
Radio Type	List the interface and serial number.
Radio Firmware Version	Current firmware version installed on the WAP.
Receive/Transmit Statistics	
Host Kilobytes Received/Sent	Number of Kilobytes Sent and Received by the access point.
Unicast Packets Received/Sent	Number of Unicast Packets Received/Sent in point-to-point communication.
Unicast Packets Sent To Host/By Host	Number of Unicast Packets Received/Sent by the access point.
Broadcast Packets Received/Sent	Number of Broadcast Packets Received/Sent by the access point.
Beacon Packets Received/Sent	Number of Beacon Packets Received/Sent by the access point.
Broadcast Packets To Host/By Host	Number of Number of Broadcast Packets Received/Sent by the access point.
Multicast Packets Received/Sent	• The number of packets received that were sent as a transmission to a set of nodes. • The number of packets transmitted that were sent as a transmission to a set of nodes.

Table 19 - Network Interfaces: Radio0-802.11N2.4 GHz and 5 GHz Detailed Status (Continued)

Parameter	Description
Multicasts Received/Sent By Host	Number of Multicast Packets Received/Sent by the server.
Mgmt Packets Received/Sent	Number of Management Packets Received/Sent by the access point.
RTS Received/Transmitted	Number of Request-to-Send (RTS) frames received or transmitted by the access point.
Duplicate Frames	Number of times a frame with a sequence control field that indicates that a duplicate is received.
CTS Not Received	Number of CTS frames not received by the access point in response to an RTS frame.
CRC Errors	Displays the number of packets with CRC errors.
Unicast Fragments Sent	Number of fragments of frames that the access point transmitted.
WEP Errors	Number of frames that are discarded because the access point could not decrypt them or because they were not encrypted.
Retries	Number of attempts to send a packet.
Buffer full	Number of messages that are sent to the sending device to suspend transmission until the data in the buffers has been processed.
Packets With One Retry	Number of transmitted packets with one retry only.
Host Buffer Full	Number of messages that are sent to the sending device to suspend transmission until the data in the buffers has been processed.
Packets With More Than One Retry	Number of transmitted packets with more than one retry.
Header CRC Errors	Number of header CRC errors received.
Protocol Defers	Number of transmitted protocol defers.
Invalid Header	Number of invalid headers received.
Energy Detect Defers	Number of transmitted energy detect defers.
Length Invalid	Number of packets received that have invalid lengths.
Jammer Detected	Number of jamming devices detected.
Incomplete Fragments	Number of packets received that are fragmented and incomplete.
Rx/Tx concats	Number of concatenated frames.

Network Interface Radio Settings Page

The Setting page provides detailed parameters settings for the interface you need to configure. There are some overlap in these parameters with the Easy Setup page.

Figure 24 - Interface Settings Page

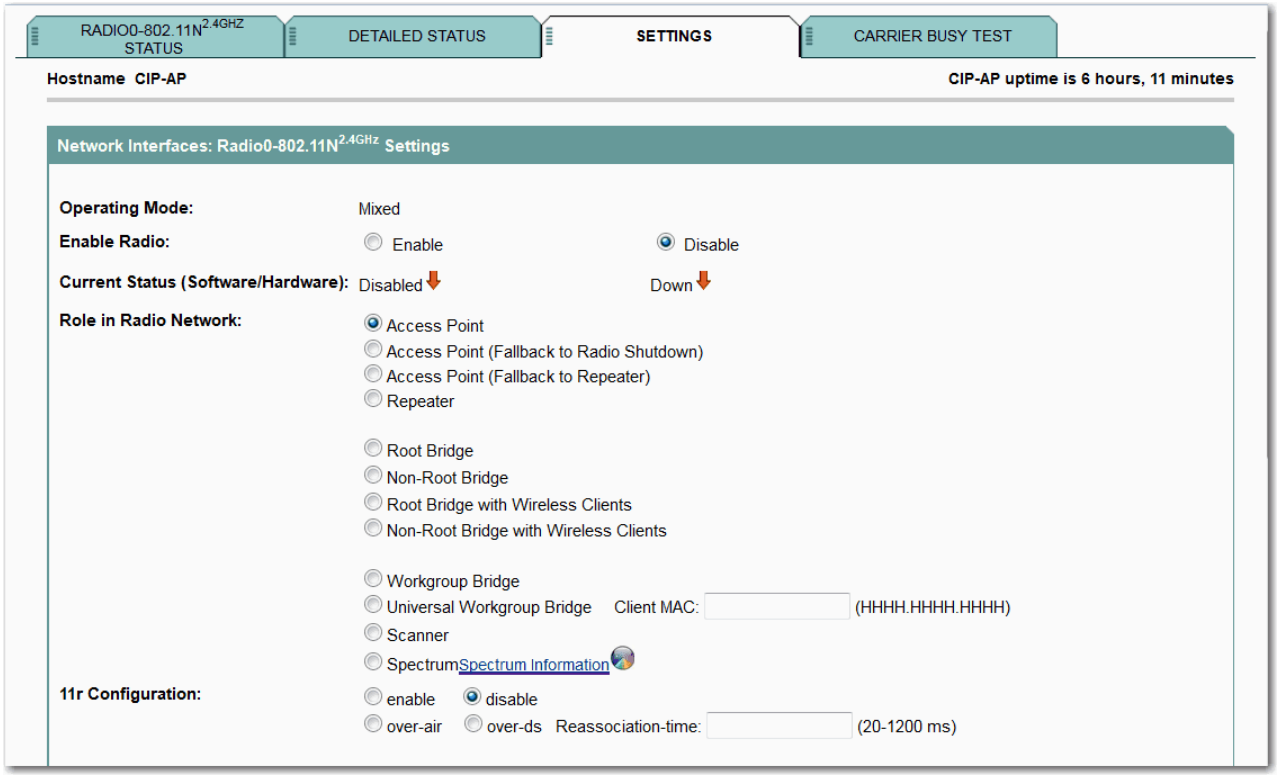


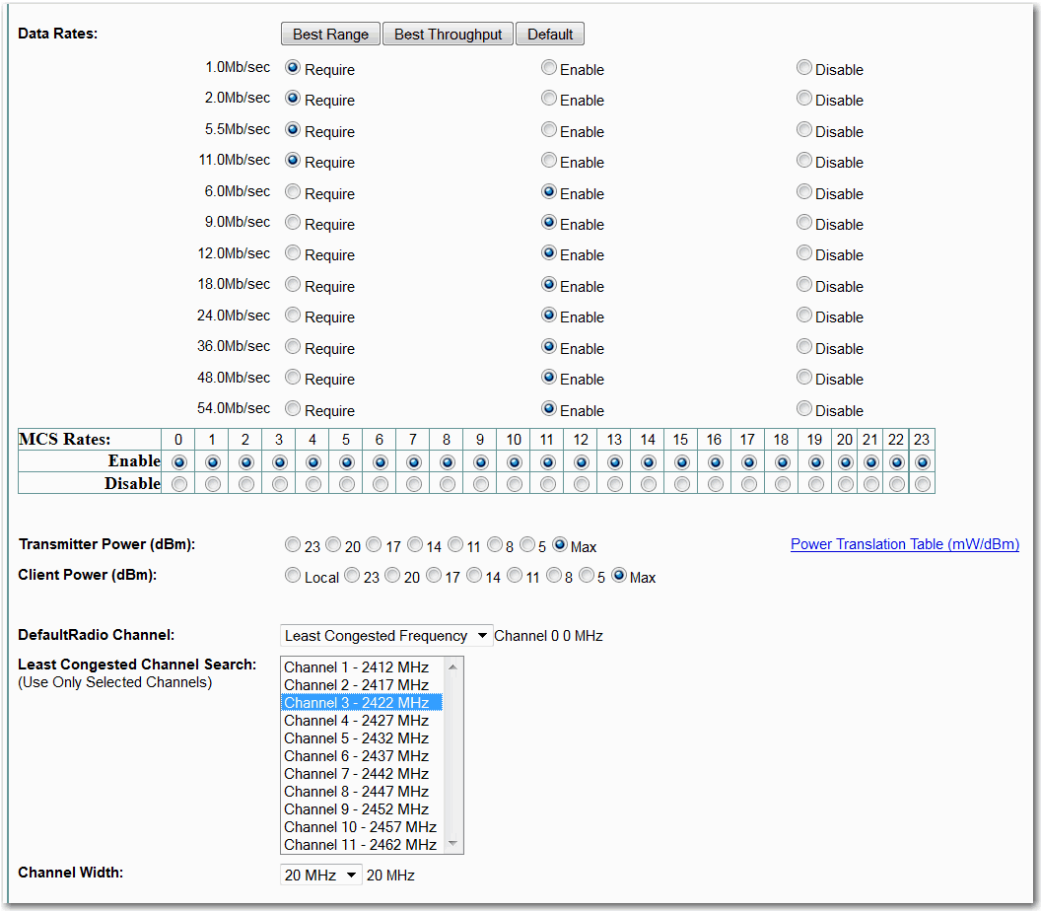
Table 20 - Radio0-802.11n 2 GHz and Radio1-802.11n 5 GHz Settings Description

Parameter	Description
Operating Mode	This value indicates whether the radio supports only 802.11a or 802.11g clients (legacy mode) or can also support 802.11n clients (mixed mode). This essentially is determined by the enabled data rates.
Enable Radio	This is where you enable the radios. In the easy Setup page, you can set some parameters, but you need to go to this page to enable the radio. Network>Network Interface>Radio0-802.11n 2 GHz (or Radio0-802.11n 5 GHz) >Settings to enable a radio.

Table 20 - Radio0-802.11n 2 GHz and Radio1-802.11n 5 GHz Settings Description (Continued)

Parameter	Description
Current Status	This value comes from the radio buttons just above it. If you set the radio to enabled this value changes. • Software Status - Up / Down / Disabled • Hardware Status - Up / Down / Reset
Role in Radio Network	This is where you choose a role in the radio network. The choices are: • access point • repeater • root bridge • non-root bridge • install • workgroup bridge • scanner • spectrum For more detailed information, see Radio Configuration Parameter Descriptions on page 75.
11r Configuration	Configures 802.11r protocol support for fast roaming. Requires WDS enabled in the network • Enable • Disable • Over-air • Over-ds • Reassociation-time: (20…1200 ms)

Figure 25 - Interface Settings Page (continued)



When a Stratix 5100 is configured in the Workgroup Bridge mode, additional radio settings appear on the page. These parameters allow to enable and optimize fast wireless roaming of a workgroup bridge between access points.

Table 21 - Radio0-802.11n 2 GHz and Radio1-802.11n 5 GHz Settings Description

Parameter	Description
Data Rates	• Default • Best Range • Best Throughput • 1.0, 2.0, 5.5, 11.0, 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, and 54.0 Mbps • Require, Enable, Disable These are legacy 802.11a/b/g data rates. 802.11n rates are configured below.
MCS (802.11n) Rates	Modulation Coding Scheme (MCS) data rates 0...23 for 802.11n support Enable Disable
Transmitter Power (dBm)	Specifies power settings for the transmitter in dBm. Power values are different for 2.4 vs. 5 GHz radios. They are also different depending on the locale and channel.
Client Power (dBm)	Specifies power settings that wireless clients should use to communicate with the AP. The client chooses the actual transmit power level based on this setting and the locally configured value. Power values are different for 2.4 vs. 5 GHz radios. They are also different depending on the locale and channel.

Table 21 - Radio0-802.11n 2 GHz and Radio1-802.11n 5 GHz Settings Description (Continued)

Parameter	Description
Default Radio Channel	• Least Congested Channel • Dynamic Frequency Selection (DFS) • Static channel number and frequency List of parameters depends on the radio band and locale.
Channel Width	20 MHz / 40 MHz
Fast Roaming parameters (WGB mode only)	These are the parameters that are available in WGB mode only. • Mobile Station Neighbors List (Ignore) Scans or ignores reported list of neighbors when limited channel scanning is enabled. • High Speed Roaming Enables WGB operation in fast roaming mode • Packet Count Minimum packet count from which average signal strength is calculated • Mobile Station Scan Period Minimum time between scans when the connection deteriorates • Threshold Power Signal strength at which scanning will start • Mobile Station Scan List of channels that will be scanned to determine the best AP to roam • Mobile Station Minimum Rate Minimum data rate at which roaming is initiated (if none, any data rate change may cause roaming)

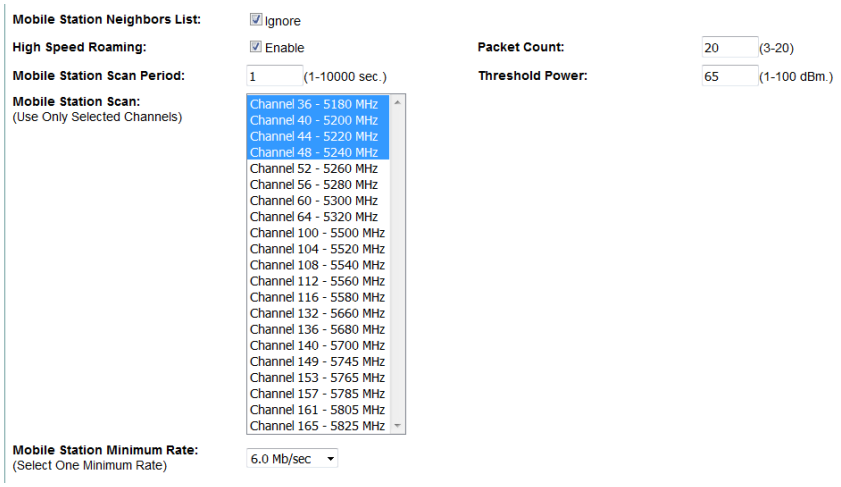


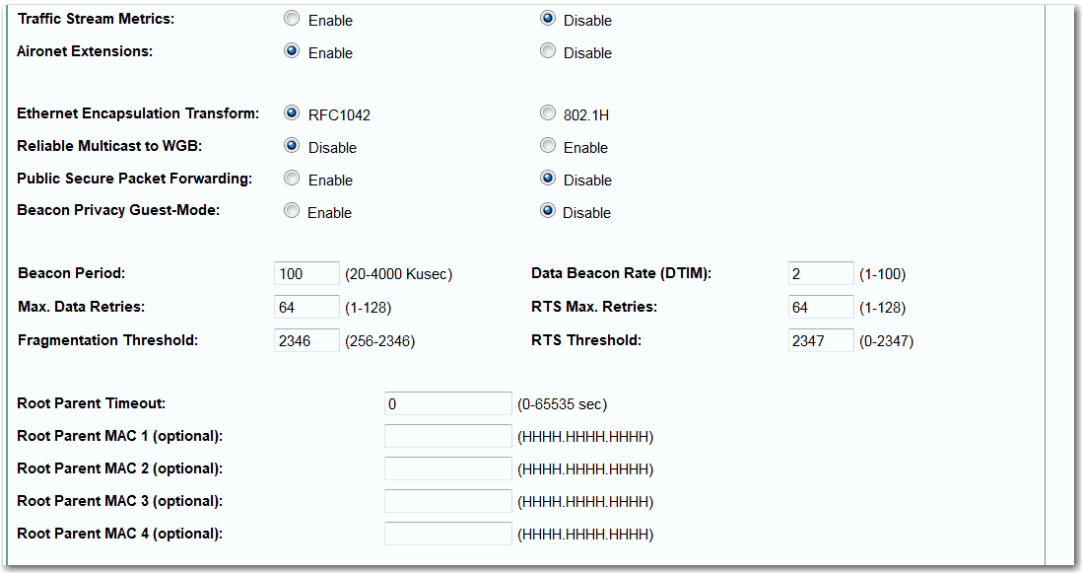
Table 22 - Radio0-802.11n 2 GHz and Radio1-802.11n 5 GHz Settings Description (Continued)

World Mode Multi-Domain Operation	Disable Legacy Dot11d
Country Code	Country Code, Indoor, Outdoor Country code selection is only available if World Mode is configured as 802.11d.

Table 22 - Radio0-802.11n 2 GHz and Radio1-802.11n 5 GHz Settings Description (Continued)

Receive Antenna	Diversity Left (B) Center (C)
Transmit Antenna	Diversity Left (B)
Internal Antenna Configuration	Enable Disable Antenna Gain (dBi): (-128…128) These parameters do not affect actual antenna operation but only used for RF planning purposes by a network management software.

Figure 26 - Interface Settings Page (Continued)



WARNING: Radio settings below are advanced and normally should not be modified.

Table 23 - Radio0-802.11n 2 GHz and Radio1-802.11n 5 GHz Settings Description (Continued)

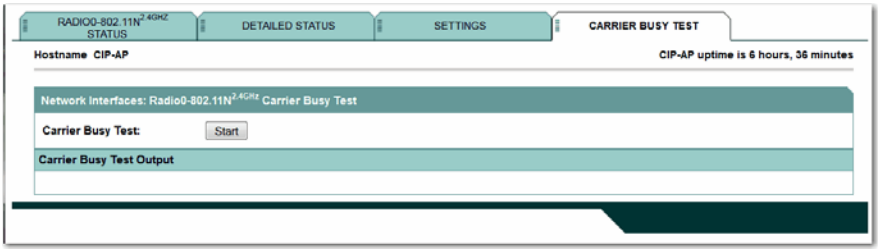
Traffic Stream Metric	Enable Disable
Aironet Extension	Enable Disable
Ethernet Encapsulation Transform	RFC1042 802.1H
Reliable Multicast to WGB	Enable Disable
Public Secure Packet Forwarding	Enable Disable

Table 23 - Radio0-802.11n 2 GHz and Radio1-802.11n 5 GHz Settings Description (Continued)

Beacon Privacy Guest-Mode	Enable Disable
Beacon Period	20…4000 Kusec
Data Beacon Rate (DTIM)	1…100
Max. Data Retries	1…128
RTS Max. Retries	1…128
Fragmentation Threshold	256…2346
RTS Threshold	0…2347
Root Parent Timeout	0…65535 s
Root Parent MAC 1…4 (optional)	HHHH.HHHH.HHHH

Carrier Busy Test

You can perform a carrier busy test to check the radio activity on wireless channels. During the carrier busy test, the wireless device drops all associations with wireless networking devices for 4 seconds while it conducts the carrier test and then displays the test results. This test disrupts the user traffic.



Association Page

The Association page is where you can view information about the clients that associated with the AP (in a root AP mode) or the parent AP (in a workgroup bridge mode).

Figure 27 - Association Page

Table 24 - Association Page Parameter Descriptions

Parameter	Description
SSID	Name
Device Type	The type of device.
Name	Displays the name of the device.
IP Address	IP address of the client.
State	The state of the client as either Associated or Association Processing.
Parent	Defines the parent wireless client device.

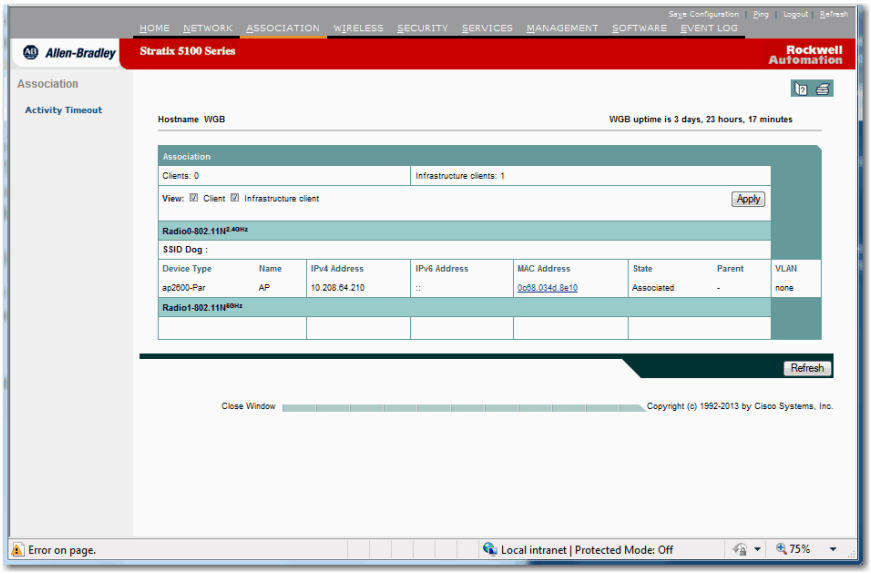
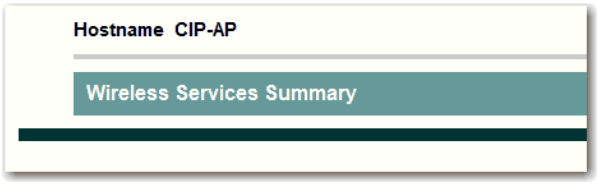


Table 24 - Association Page Parameter Descriptions (Continued)

Parameter	Description
VLAN	Identifies whether a VLAN is assigned for this client.
MAC Address	The Media Access Control (MAC) address is a unique identifier assigned to the network interface by the manufacturer. If you click the MAC Address link, it takes you to the Association: Station View - Client screen.
Activity Timeout	In this page, you specify the number of seconds that the access point tracks an inactive device. • Device Class Specifies a Cisco Aironet device class. • Default (optional) 1…100000 s Specifies the activity timeout value that the access point uses when a device associates and proposes a zero-refresh rate or does not propose a refresh rate. • Maximum (optional) Specifies the maximum activity timeout allowed for a device regardless of the refresh rate proposed by a device when it associates. • Bridge, name of a bridge. • Client Station, name of a client station. • Repeater, name of a repeater. • Workgroup Bridge, name of a workgroup bridge. • Unknown (Non-Cisco), name of unknown devices.

Wireless Page

The wireless page provides a wireless services summary. You can access the AP wireless service and WDS/WNM general setup.



AP

An access point acting as the wireless domain services (WDS) on your wireless LAN maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the WDS forwards the client's credentials to the new access point. Only two packets pass between the client and the new access point, greatly shortening the reassociation time.

Figure 28 - Wireless AP Services Summary

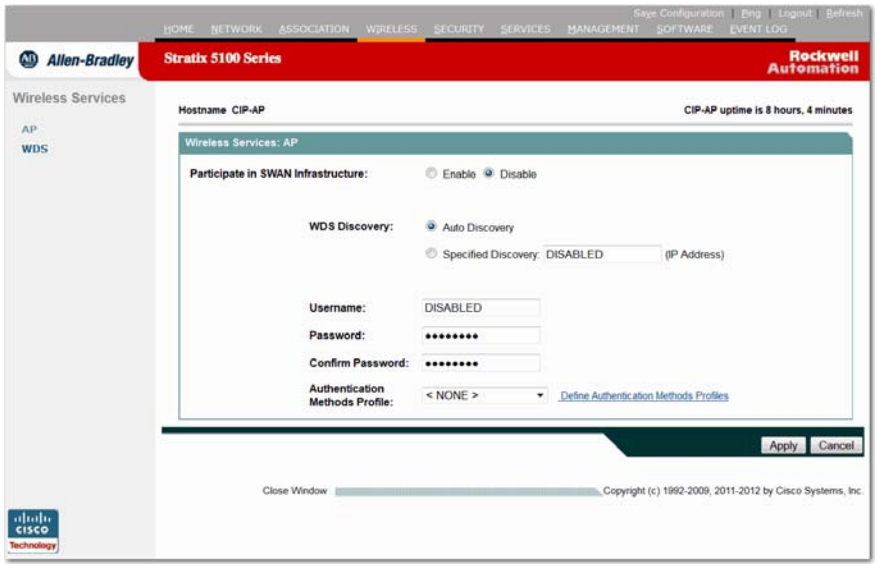
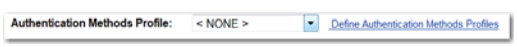


Table 25 - Wireless AP Page Parameter Descriptions

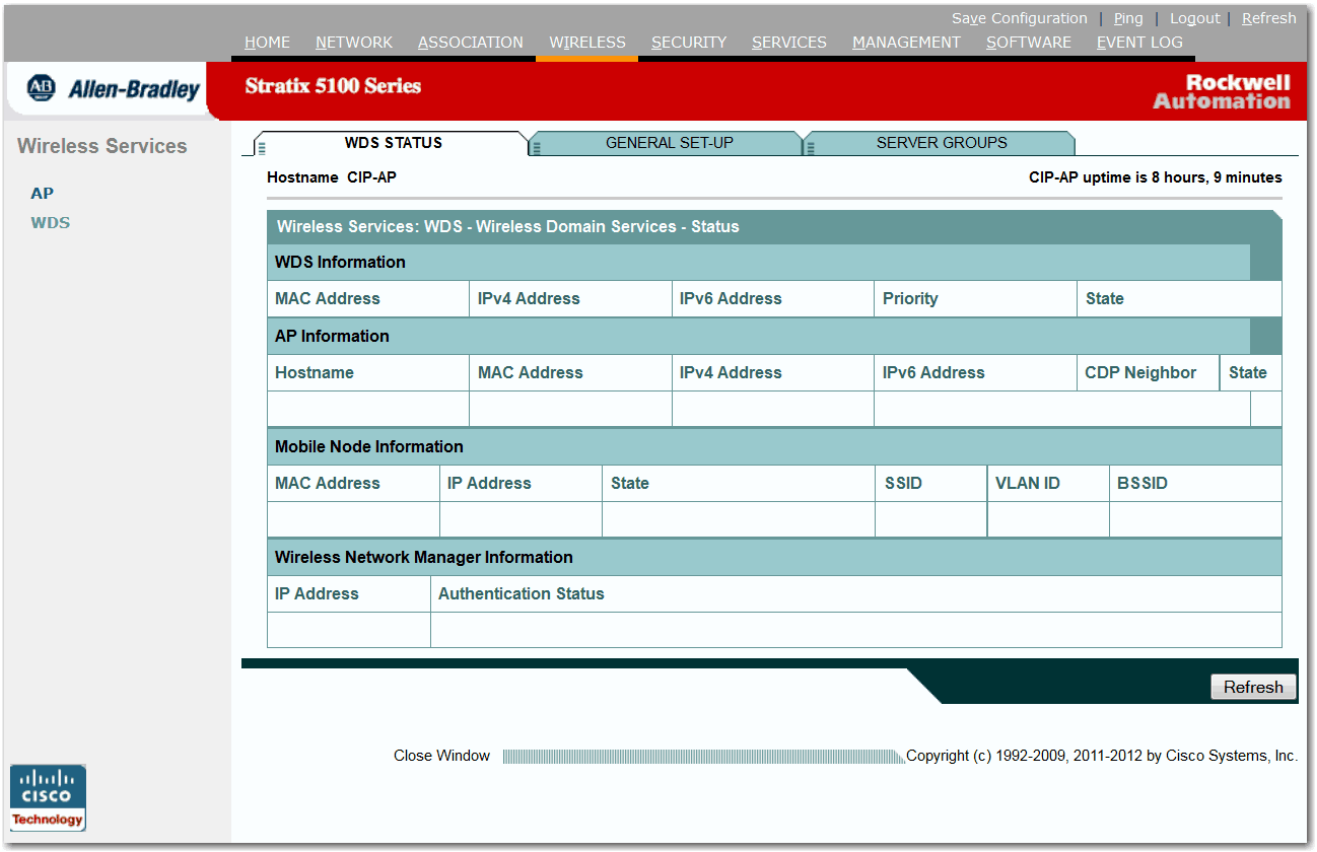
Parameter	Description
Participate in SWAN Infrastructure	Enable Disable
WDS Discovery	Auto Discovery Specified Discovery (IP Address)
Username	Participant username
Password	Participant password
Authentication Methods Profile	 The Define Authentication Methods Profile link takes you to Security>AP Authentication. See Security Page on page 104 for more information.

WDS

When you configure Wireless Domain Services on your network, access points on your wireless LAN use the WDS-enabled access point to provide fast, secure roaming for client devices and to participate in radio management. Use these parameters to identify if the interface is to be used as a Wireless Domain Services (WDS).

See Configure Wireless Domain Services and Fast Secure Roaming on page 349 for detailed configuration information.

Figure 29 - WDS (Wireless Domain Service) Status Page



This page provides an overview status of the wireless domain services you have setup.

Table 26 - Wireless WSD/WNM General Setup Page Parameter Descriptions

Parameter	Description
WDS Information	
MAC Address	The Media Access Control (MAC) address is a unique identifier assigned to the network interface by the manufacturer.
IP Address	IP address of the access points attempting to register with this wireless domain.
Priority	Displays a priority number from 1…255 of this WDS candidate. The WDS candidate with the highest priority number becomes the acting WDS.
State	Displays the state of the access point as either Registered or not.

Table 26 - Wireless WSD/WNM General Setup Page Parameter Descriptions (Continued)

Parameter	Description
AP Information	
MAC Address	The Media Access Control (MAC) address is a unique identifier assigned to the network interface by the manufacturer.
IP Address	IP address of the client/repeater.
CDP Neighbor	The IP address of the CDP neighbor with which the Ethernet port of the access point is directly connected.
State	Displays the state of the client/repeater as either Registered or not.
Mobile Node Information	
MAC Address	The Media Access Control (MAC) address is a unique identifier assigned to the network interface by the manufacturer.
IP Address	IP address of the client/repeater.
State	Displays the state of the client/repeater as either Registered or not.
SSID	Specifies the SSID tied to the VLAN.
VLAN ID	Specifies the virtual Ethernet LAN identification number tied to the SSID. You can assign a name to a VLAN in addition to its numerical ID.
BSSID	Specifies the MAC address of the Basic Server Set Identifier. The Basic Server Set is a set of stations that communicate with one another.
Wireless Network Manager Information	
IP Address	Contains the IP address of the wireless domain service that the access point to which you browsed is configured to use.
Authentication Status	The server used to authenticate infrastructure devices, such as access points, on your wireless LAN.

Figure 30 - WDS and WNM General Set-up Page

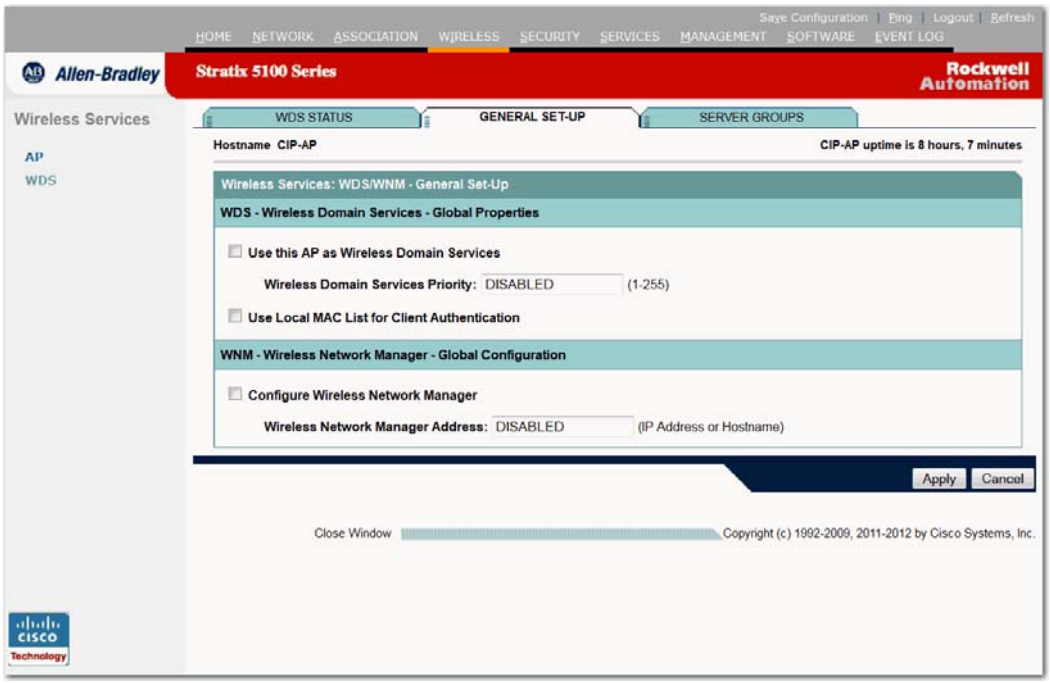
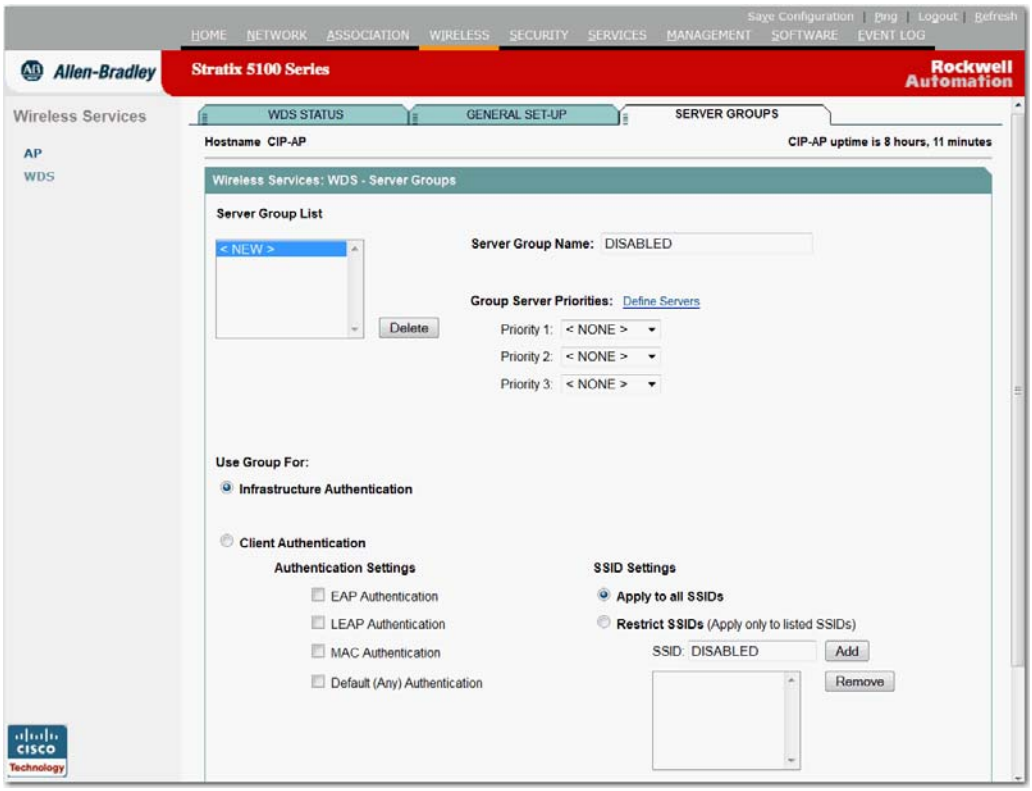


Table 27 - Wireless WSD/WNM General Setup Page Parameter Descriptions

Parameter	Description
WDS - Wireless Domain Services - Global Properties	
Use this AP as Wireless Domain Services	Check the box if you want to use the AP as Wireless Domain Services. Check the checkbox if you want this access point to become the WDS for fast secured roaming using CCKM-capable clients or if you want this access point to forward statistics to the WNM for collection by your WLSE. If you want the access point to serve as the WDS or as a WDS candidate, you should use this page to configure the access point as a WDS. For your WDS, you should choose an access point that: • Can be physically secured to prevent theft. • Serves few client devices because the access point's WDS duties can degrade performance for associated client devices.
Wireless Domain Services Priority	Set the WDS priority: 1…255 of this WDS candidate. The WDS access point candidate with the highest number becomes the acting WDS access point. If you configure access points as backup WDS, assign the highest priority to the access point that you want to act as the main WDS and lower priorities to backup WDSs. If your main WDS fails, the backup with the highest priority becomes the active WDS.
Use Local MAC List for Client Authentication	Check this to authenticate client devices using MAC addresses in the local list of addresses configured on the WDS device. If you do not select this checkbox, the WDS device uses the server specified for MAC-address authentication on the Server Groups page to authenticate clients based on MAC addresses. Selecting the Use Local MAC List for Client Authentication checkbox does not force client devices to perform MAC-based authentication. It provides a local alternative to server-based MAC-address authentication.

Figure 31 - WDS Server Groups Page



This page lets you set up authentication servers that can be used by the WDS access point. If you want an access point to serve as the WDS or as a WDS candidate, you need to configure them as such.

You must configure at least one server on the Security>Server Manager tab before setting up server groups here.

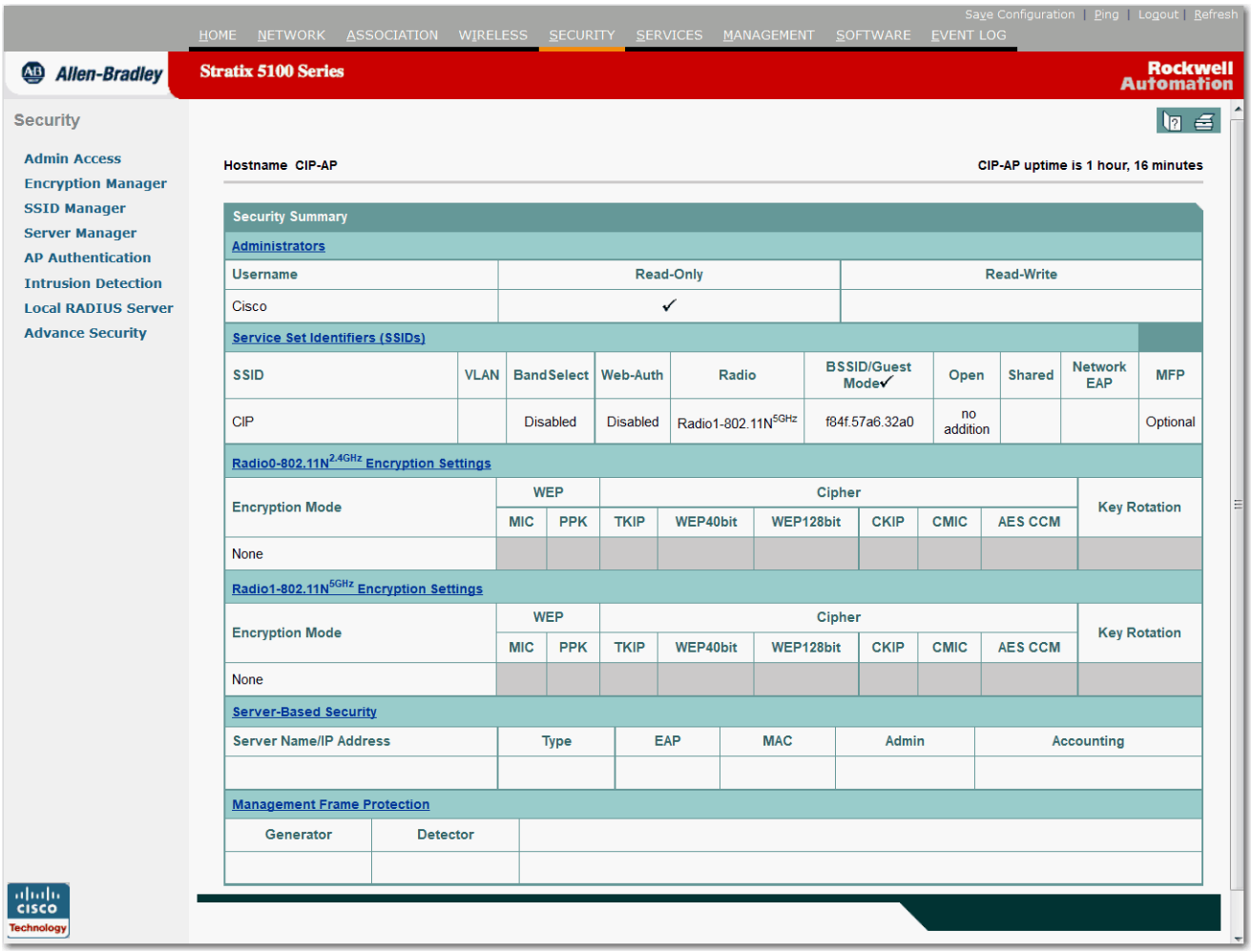
Table 28 - Wireless Server Groups Parameter Descriptions

Parameters	Description
Server Group List	Click to select which servers you want to edit.
Server Group Name	Enter a unique group name.
Group Sever Priorities	Set the priority of servers used for infrastructure and client authentications.
Define Servers	Click Define Servers to move to the Security>Server Manager page where you can configure the servers.
Infrastructure Authentication/ Client Authentication	Select the devices to which the server group authenticates. Choose among infrastructure devices such as access points, clients using EAP authentication, clients using LEAP authentication, clients using MAC-based authentication, or clients using any authentication type. If set up, Any Authentication is the default group, which is applied when none of the other Client Authentication groups (EAP, LEAP, or MAC) apply.
SSID Settings	By default, the server group applies to all SSIDs. To define it for a specified list of SSIDs, click Restrict SSIDs. Click Add to add the desired SSIDs.

Security Page

Use the Security page to configure security settings to prevent unauthorized access to your network. Because the WAP is a radio device, the wireless device can communicate beyond the physical boundaries of your work-site. The Security Summary page provides a snap shot of the security setting and links to other security pages.

Figure 32 - Security Summary Page



Links on the Security Summary Page	Description
Administrators	Link to Admin Access, see Admin Access Page on page 106.
Service Set Identifiers (SSIDs)	Link to SSID Manager, see SSID Manager Page on page 109.
Radio0-802.11N2.4 GHz Encryption Settings	Link to Encryption Manager, see Encryption Manager Page on page 107.
Radio1-802.11N 5 GHz Encryption Settings	Link to Encryption Manager, see Encryption Manager Page on page 107.
Server-Based Security	Link to Server Manager, see Server Manager Page on page 115.
Management Frame Protection	Link to Intrusion Detection, see Intrusion Detection on page 123.

Table 29 - Security Summary Parameters Descriptions

Parameters	Description
Username	The username of the active user.
Read-Only	Specifies whether the user has read-only capabilities.
Read-Write	Specifies whether the user has read/write capabilities.
SSID	Specifies the unique identifier the client devices use to associate with the access point.
VLAN	Specifies the VLANs that are currently assigned to the SSID.
Band Select	When enabled, it encourages dual-band client radios to move to less congested 5 GHz band.
Web-Auth	Specifies if web authentication is enabled for clients.
Radio	Specifies which radio is being used.
BSSID/Guest Mode	Specifies the BSSID/Guest mode attached to this SSID.
Open/Shared/Network EAP	Specifies the method of authentication being used. • Open enables any device to authenticate and then attempt to communicate with the access point. • Shared sends an unencrypted challenge string to any device attempting to communicate with the access point. Shared authentication is a legacy mode that should not be used due to security issues. • Network EAP uses EAP to interact with an EAP-compatible server on your network to provide authentication for wireless client devices.
Management Frame Protection (MFP)	Management frames can be protected to detect adversaries who are invoking denial of service attacks. These can include, flooding the network with associations and probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

Admin Access Page

The Admin Access page provides the administrator with information pertaining to security, authentication and user lists.

Figure 33 - Security Admin Access

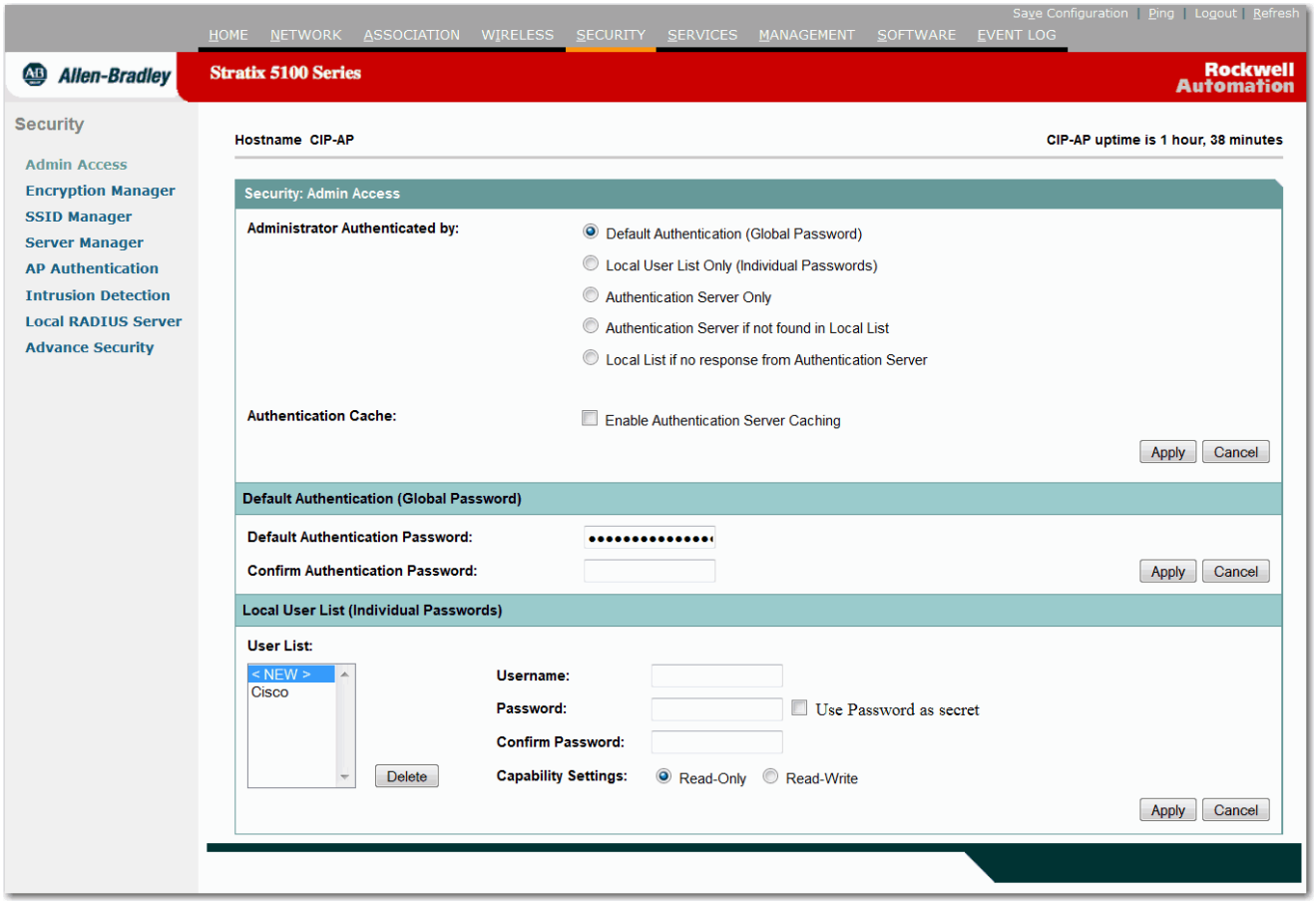


Table 30 - Security Admin Access Parameter Descriptions

Parameter	Description
Administrator Authenticated by	• Default Authentication (Global Password) • Local User List Only (Individual Passwords) • Authentication Server Only • Authentication Server if not found in Local List • Local List if no response from Authentication Server
Authentication Cache	Enable Authentication Server Caching
Default Authentication	Default Authentication Password (Global Password) Specifies password to enter the privileged exec (administrator) mode.
Local User List	• Username • Password • Use Password as secret: allows you to enter privileged exec (administrator) mode. • Capability Settings: Read only/Read-Write

Encryption Manager Page

This page enables you to select encryption mode and parameters to encrypt and decrypt radio signals.

Figure 34 - Encryption Manager Parameter Descriptions

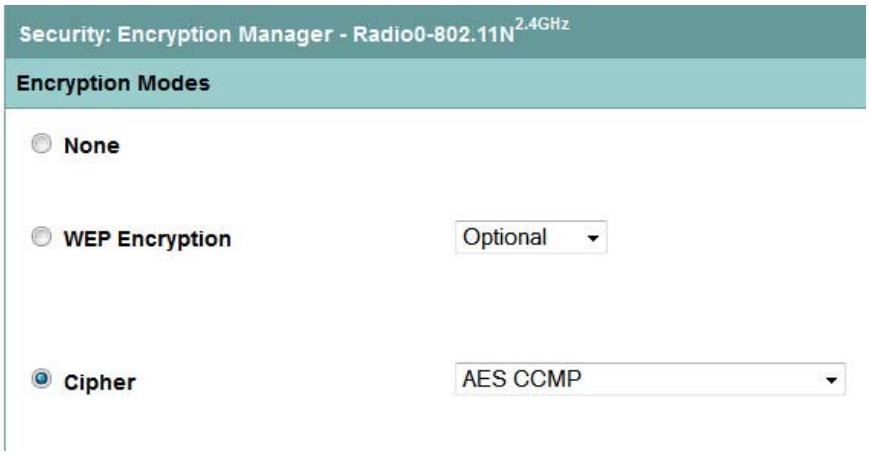


Figure 35 - Security Encryption Manager

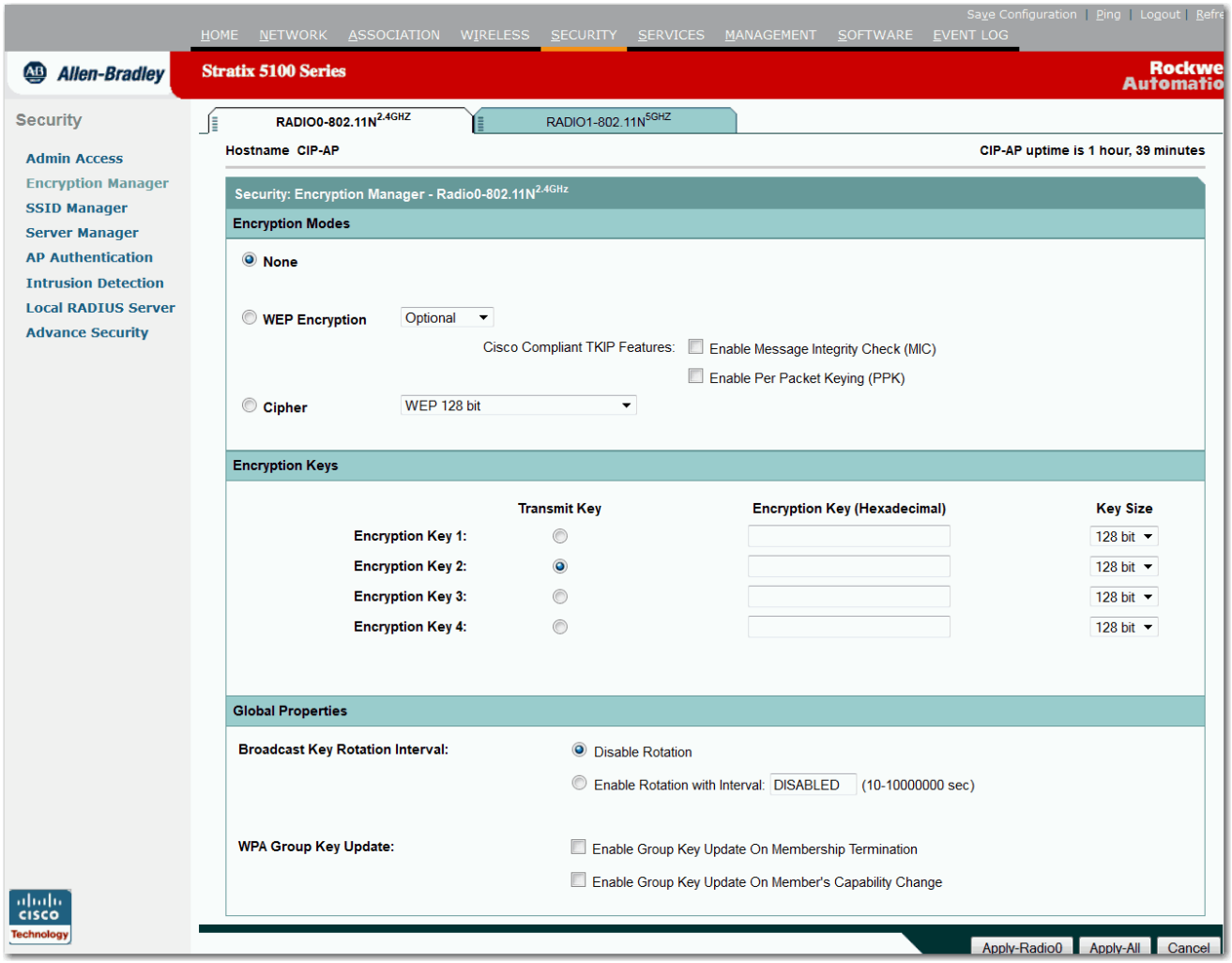
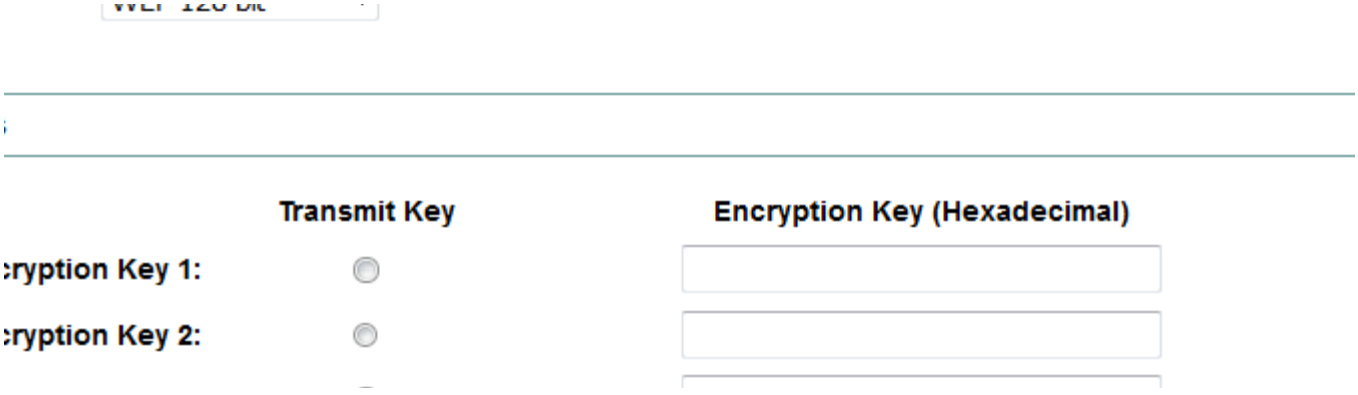


Table 31 - Security Encryption Manager Parameter Descriptions

Parameter	Description
Encryption Modes	Indicate whether clients should use data encryption when communicating with the access point.
None	Encryption is not enabled on the radio.
WEP Encryption	Choose Optional or Mandatory. If optional, client devices can communicate with this access point or bridge with or without WEP. If mandatory, client devices must use WEP when communicating with the access point. Bridges not using WEP are not allowed to communicate. WEP is an 802.11 standard encryption algorithm originally designed for a wireless LAN. However, the basic WEP construction is flawed, and an attacker can compromise the privacy with reasonable effort. WEP is **NOT recommended** for use as a WLAN security method. Cisco 802.11n radios require that either no encryption or AES-CCMP be configured for proper operation.
Cipher	Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN. You must use a cipher suite to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM). Use the drop-down menu to choose among AES, TKIP, CKIP, CMIC, and WEP. AES CCMP is the recommended and the most secure option. AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. AES-CCMP is superior to WEP encryption and is defined in the IEEE 802.11i standard. WEP is the least secure cipher suite and not recommended.
Transmit Key	This parameter is only used with WEP and **not recommended**. Click Transmit Key and select the WEP key this bridge will use. Only one key can be selected at a time. All set keys can be used to receive data. The key that you select as the transmit key must also be entered in the same key slot on client devices that associate with the access point or bridge, but it does not have to be selected as the transmit key on the client devices.
Encryption Key 1-4	This parameter is only used with WEP and not recommended. You can enter up to 4 WEP encryption keys here.
Key Size	Select 40-bit or 128-bit encryption for each WEP key.



Global Properties	Broadcast Key Rotation Interval: Disable Rotation or Enable Rotation with Interval (10…10000000 s)
Broadcast Key Rotation Interval	This is only used in legacy WPA mode and not needed for WPA2 with AES encryption. Allows the access point to generate best possible random group key and update all the key-management capable stations periodically. Broadcast key rotation does not work for static WEP clients. This feature keeps the group key private to currently active members only. However, it may generate some overhead if clients in your network roam frequently.
WPA Group Key Update	This is only used in legacy WPA mode and not needed for WPA2 with AES encryption. Check the appropriate checkbox to determine how frequently the access point changes and distributes the group key to WPA-enabled client devices. • Enable Group Key Update on Membership Termination • Enable Group Key Update on Member's Capability Change

SSID Manager Page

Use the SSID Manager page to assign SSIDs to specific radio interfaces.

Figure 36 - SSID Manager

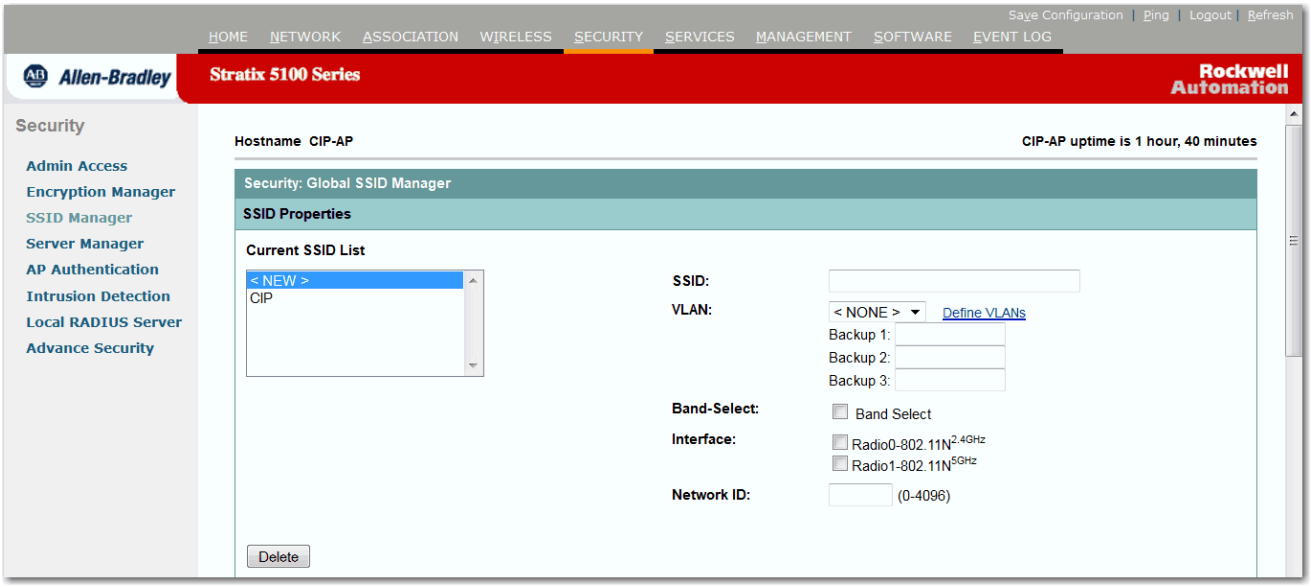


Table 32 - SSID Manager Parameter Descriptions

Parameter	Description
Current SSID List	Enter the unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity. The SSID can be any alphanumeric, case-sensitive entry from 2…32 characters.
SSID	The service set identifier (SSID) - also called the radio SSID - is a unique identifier that clients use to associate with the radio. You can add up to 16 SSIDs. The following six characters are not allowed: +,], /, ", TAB, and trailing SPACE. In addition, the following three characters cannot be the first character: !, #, and ;. The SSID parameter is case sensitive.
VLAN	Allows you to associate an SSID with a VLAN that has been configured.
Define VLANs	This takes you to the Services>VLAN page. If you do not apply configuration changes before clicking this link the changes are lost. On this page you set default VLANs and assign current VLANs and their ID and information. For instance, enterprise users can use different VLANs to segregate employee traffic from guest traffic, and further segregate those traffic groups from that of high-priority voice. Traffic to and from wireless clients with varying security capabilities can be segregated into VLANs with varying security policies.
Band-select	Band selection encourages the wireless client (capable of dual-band, 2.4 and 5 GHz operation) to move to a less congested 5 GHz radio band.
Interface	Select the radio interfaces to enable. The SSID remains inactive until you enable it for a radio interface.
Network ID	Network ID for Layer 3 mobility in a WDS-enabled network. This is a legacy feature and should not be normally configured.

Table 32 - SSID Manager Parameter Descriptions (Continued)

Parameter	Description
Client Authentication Settings and Methods Accepted	**Open Authentication** Choose Open Authentication by checking the checkbox. This enables any device to authenticate and then attempt to communicate with the access point. Additional methods such as EAP or WPA/WPA2 pre-shared key must be used to provide secure authentication. After you choose Open Authentication, you can select the additional method to use from the pull-down menu. Theses are the options in the pull-down menu. • MAC authentication • EAP • MAC authentication and EAP • MAC authentication or EAP, or with optional EAP. To enable EAP, EAP Authentication Servers must be set on this page or in the Server Manager page. To enable MAC Authentication, you must either enter the MAC address locally or select the Authentication Server Only option on the Advanced Security page. Choose Optional EAP to allow both clients and optional EAP clients to associate and become authenticated with either authentication method. Although an access point can use Open Authentication with EAP method to authenticate a wireless client device, an access point cannot use EAP to authenticate another access point. In other words, access points must authenticate each other using either open, shared, or Network EAP authentication methods. **Shared Authentication** Choose shared authentication by checking the Shared Authentication checkbox. Shared key authentication is **not recommended** because of security flaws. Use open authentication with EAP or WPA/WPA2 pre-shared key instead. The access point sends an unencrypted challenge string to any device that attempts to communicate with the access point. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point enables the requesting device to authenticate. The unencrypted challenge and the encrypted challenge can be monitored; however, this leaves the access point open to attack from an intruder who guesses the WEP key by comparing the unencrypted and encrypted text strings. Because of this weakness, shared key authentication can be less secure than open authentication. Only one SSID can use shared authentication. After you choose Shared Authentication, you can select the method to use from the pull-down menu. The choices are MAC Authentication, EAP, or MAC Authentication and EAP. **Network EAP** Choose network EAP by checking the Network EAP checkbox. The device uses the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server on your network to provide authentication for wireless client devices. Client devices use dynamic WEP keys to authenticate to the network. After you choose Network EAP, you can select MAC Authentication. Network EAP is necessary to operate with Cisco client devices that support LEAP authentication method. Normally, open authentication with EAP is used instead as more secure method.

Table 32 - SSID Manager Parameter Descriptions (Continued)

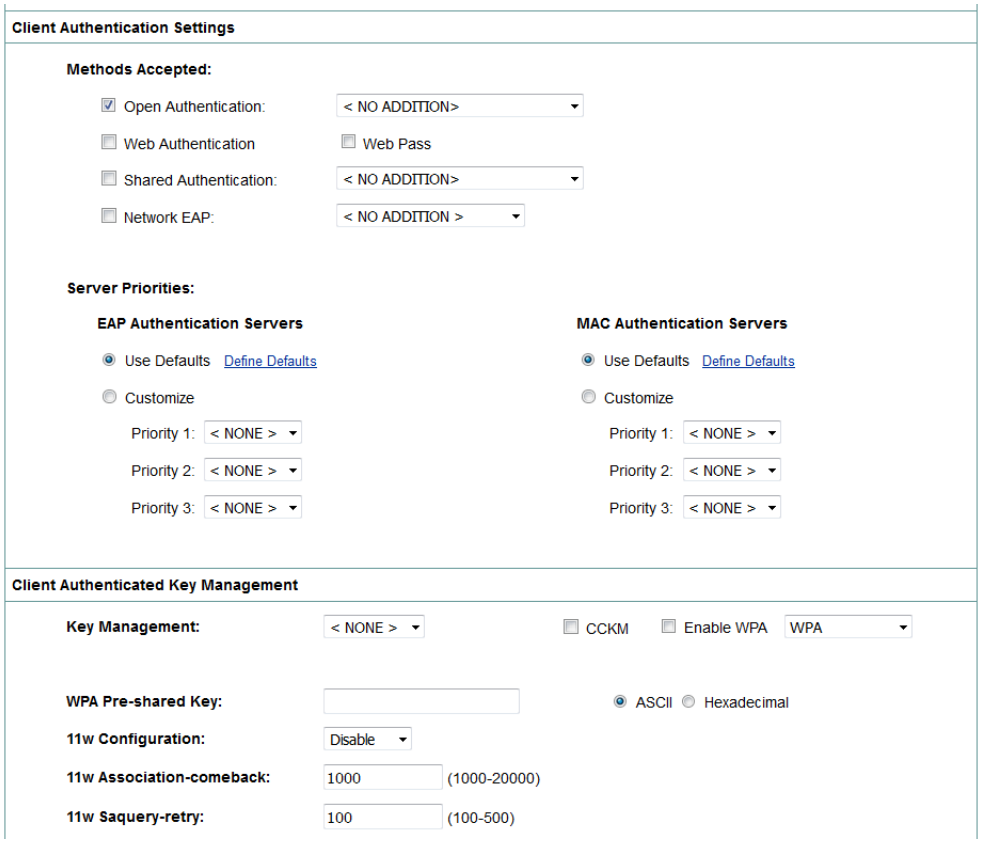
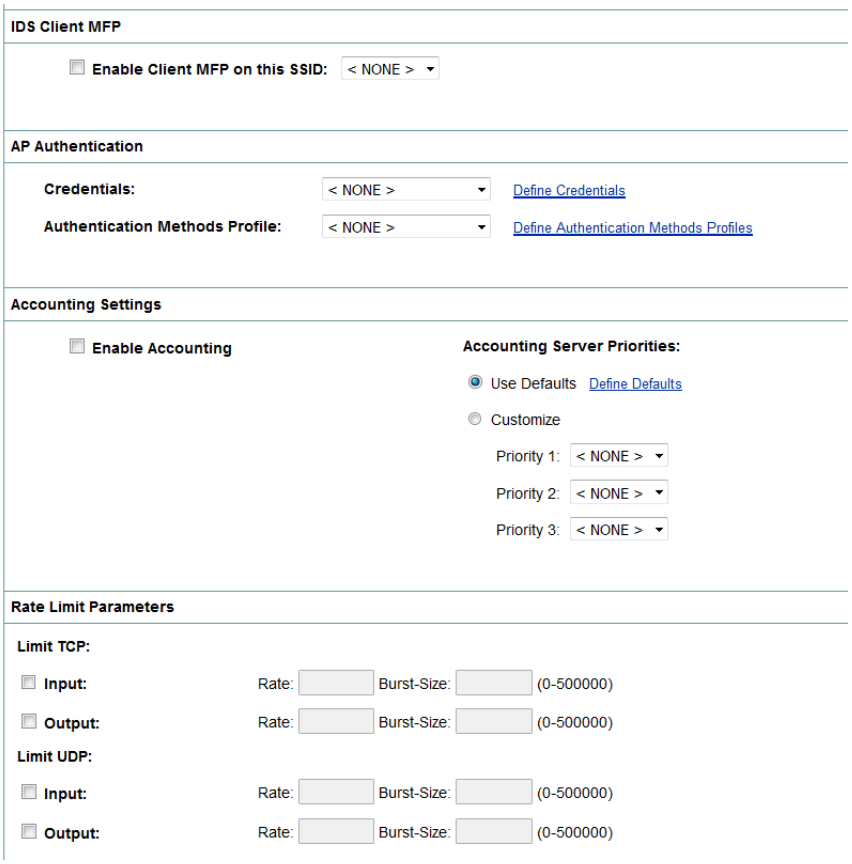
Parameter	Description
	
Server Priorities	Determine how you are going to use specific RADIUS servers on this SSID. In the EAP and MAC Authentication Server sections, you can choose to use the defaults or customize the priority by using the pull-down menu. If you click to enable the use of the defaults, click the Define Defaults link to move into the Server Manager page.
Authenticated Key Management	WPA and CCKM are the authenticated key management solutions. Wi-Fi Protected Access (WPA) relies on the version of IEEE standard 802.11i. WPA supports TKIP and WEP encryption algorithms as well as 802.1X and EAP for simple integration with existing authentication system. WPA key management uses a combination of encryption methods to protect communication between client devices and the access point. Currently, WPA key management supports two mutually exclusive authenticated key managements: WPA and WPA-PSK.If authentication key management is WPA, the client and authentication server authenticate to each other using an EAP authentication method (such as EAP-TLS) and generate a Pairwise Master Key (PMK). If authentication key management is WPA-PSK, the pre-shared key is used directly as the PMK. Using Cisco Centralized Key Management (CCKM), authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network acts as a wireless domain service (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS cache of credentials dramatically reduces the time that is required for reassociation when a CCKM-enabled client device roams to a new access point. To enable CCKM for an SSID, you must also enable network-EAP authentication. When CCKM and Network EAP are enabled for an SSID, client devices using LEAP, EAP-FAST, PEAP/GTC, MSPEAP, and EAP-TLS can authenticate using the SSID. To enable WPA for an SSID, you must also enable Open authentication or Network-EAP or both. Before you can enable CCKM or WPA, you must set the encryption mode for the SSIDs VLAN to one of the cipher suite options.
Key Management	Use the pull-down menu to indicate if you want key management to be mandatory or optional. You can select CCKM and WPA authentication key management at the same time for radio 802.11b or 802.11g. For radio 802.11a, only one key management can be selected.
WPA Pre-shared Key	To support client devices using WPA key management, you must configure a pre-shared key on the access point. Enter the key and specify if you are entering hexadecimal or ASCII character. If you use hexadecimal, you must enter 64 hexadecimal character to complete the 256-bit key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the access point expands the key for you. You can enter a maximum of 63 ASCII characters.
IDS Client MFP	Enable Client MFP on this SSID to protect wireless management traffic between the client and the AP.
AP Authentication	Credentials are used to authenticate the access point to the network. This is not the same as client authentication.

Table 32 - SSID Manager Parameter Descriptions (Continued)

Parameter	Description
Credentials	Use the pull-down menu to specify a credentials profile for an SSID. Define Credentials If you need to define credentials, click the link to go to the AP Authentication - General Setup page where you can then establish a username and password or anonymous ID and trustpoint for the credentials.
Authentication Methods Profile	When an access point connects to the network, the access point and the network authentication device negotiate to agree upon an authentication method supported by both devices to complete authentication. An authentication methods profile is used to restrict the types of authentication that the access point agrees to use. Use the pull-down menu to specify an authentication profile for an SSID.
Define Authentication Methods Profile	If you need to define an authentication method profile, click the link to go to the AP Authentication - General Setup page.
Accounting Settings Enable Accounting	Indicate whether you want this server to record usage data of clients associating with the access point. Some usage data can be used for billing or usage tracking.
Accounting Server Priorities	You can choose to use the defaults or customize the priority by using the pull-down menu. If you choose to enable the use of the defaults, click the Define Defaults link to move into the Server Manager screen.
General Settings Advertise Extended Capabilities of this SSID	Includes the SSID name and capabilities in the Wireless Provisioning Service (WPS) information element.



Advertise Wireless Provisioning Services (WPS) Support	Enables the WPS capability flag in the WPS information element.
Advertise this SSID as a Secondary Broadcast SSID	Includes the SSID name and capabilities in the WPS information element.
Enable IP Redirection on this SSID	When you configure IP redirection for an SSID, the access point redirects all packets sent from client devices associated to that SSID to a specific IP address. You can redirect all packets from client devices associated using an SSID or redirect only packets directed to specific TCP or UDP ports. When you configure the access point to redirect only packets addressed to specific ports, the access point redirects those packets from clients using the SSID and drops all other packets from clients using the SSID.
IP Address	Enter the IP address of the destination for redirected packets.

Table 32 - SSID Manager Parameter Descriptions (Continued)

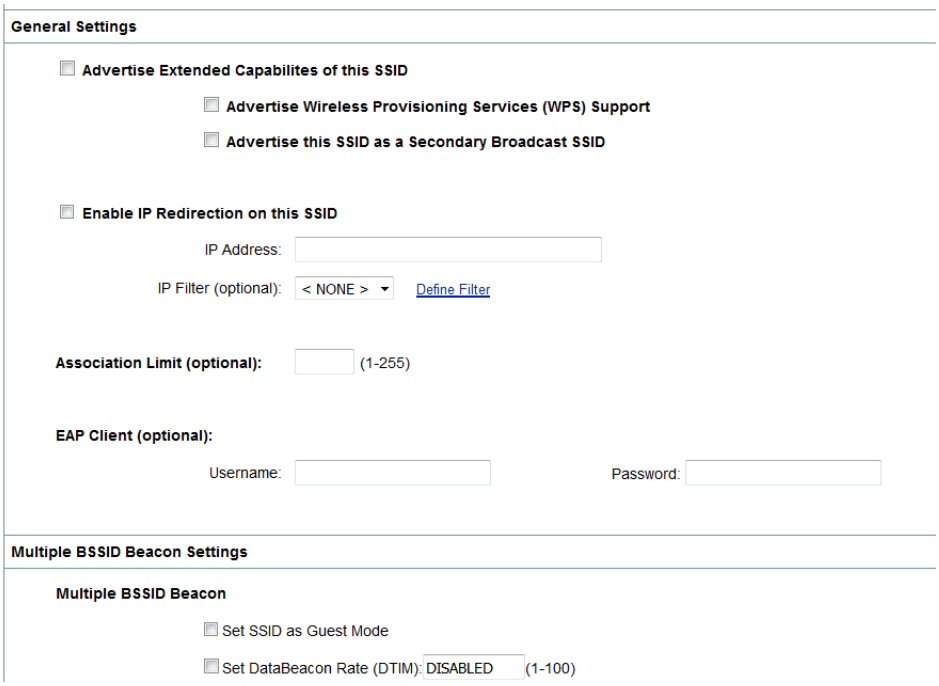
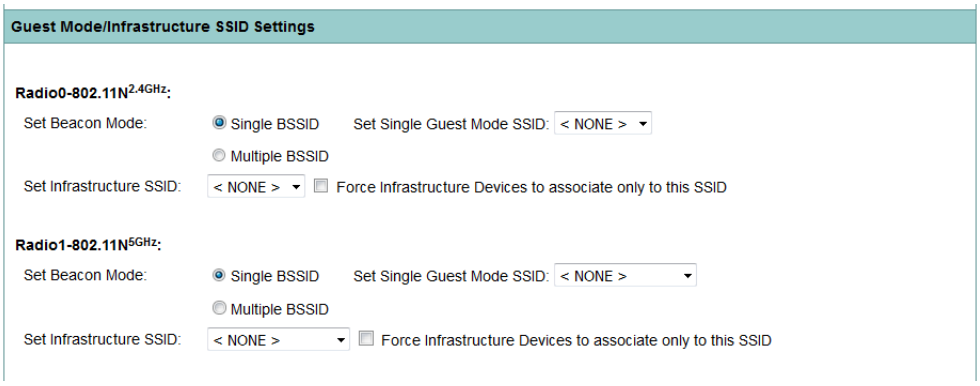
Parameter	Description
IP Filter	After you enable IP redirection and enter the IP address, click Define Filter to move to the IP Filters page where you can specify the appropriate TCP or UDP ports for redirection. If you do not specify TCP or UDP ports, the access point redirects all packets that it receives from client devices.
Association Limit (optional)	The maximum number of clients that can associate to a particular SSID. This limit prevents access points from getting overloaded and helps to provide an adequate level of service to associated clients.
EAP Client (optional)	Cisco recommends that you use AP Authentication rather than EAP Client for authenticating the access point to the network.
Username	Indicates the username used for Network EAP authentication when the repeater access point is associating with a parent access point or when a Hot Standby access point is associating with a monitored access point.
Password	Indicates the password used for Network EAP authentication when the repeater access point is associating with a parent access point or when a Hot Standby access point is associating with a monitored access point. Note: The following characters are not allowed: TAB, ?, $, +, and [.
	
Multiple BSSID Beacon Settings Multiple BSSID Beacon	Select the Set SSID as Guest Mode checkbox if you want to include the SSID in beacons. To increase the battery life for power-save clients that use this SSID, select the Set Data Beacon Rate (DTIM) checkbox and enter a beacon rate for the SSID. The beacon rate determines how often the access point sends a beacon containing a Delivery Traffic Indicator Message (DTIM).When client devices receive a beacon that contains a DTIM, they normally wake up to check for pending packets. Longer intervals between DTIMs let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often. See Configure Multiple Service Set Identifiers (SSIDs) on page 285 for further procedural information.

Table 32 - SSID Manager Parameter Descriptions (Continued)

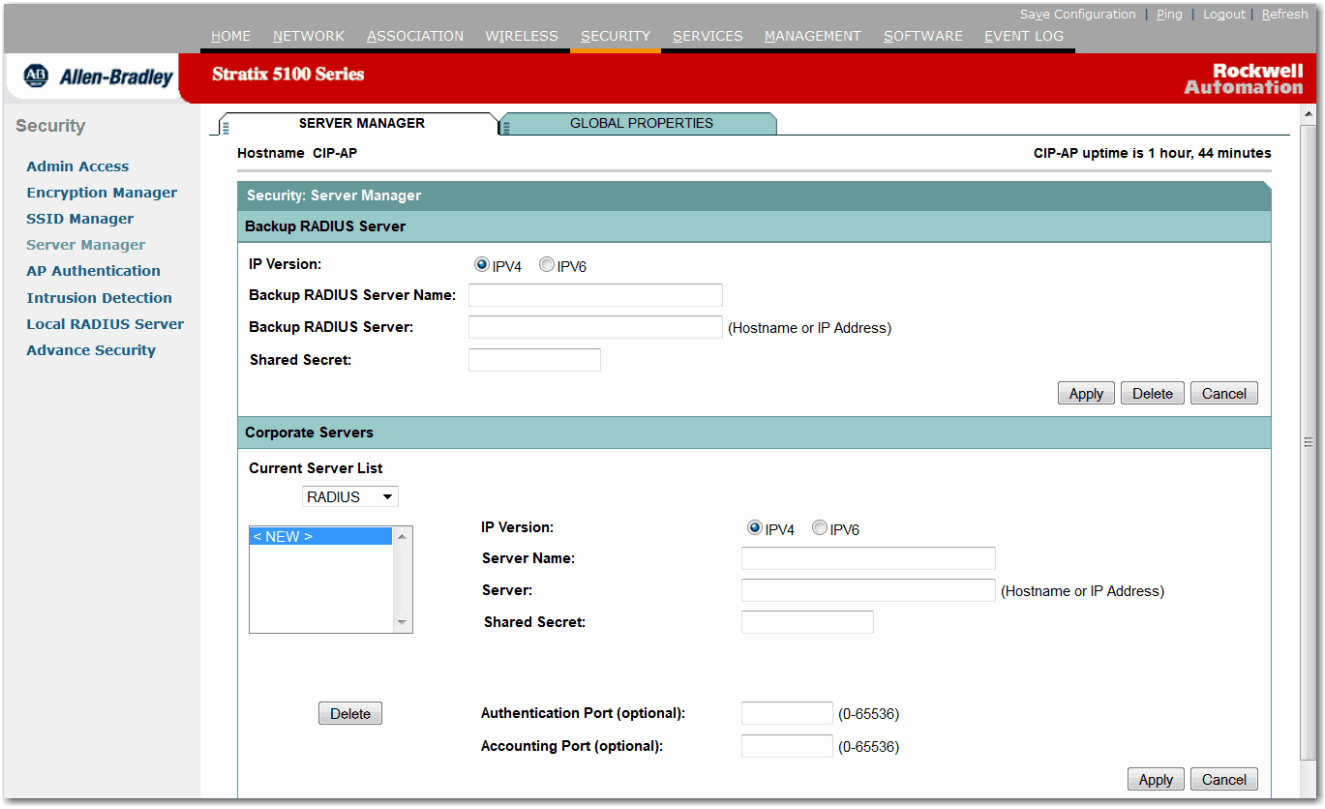
Parameter	Description
Guest Mode/Infrastructure SSID Settings Set Beacon Mode	Click to choose single or multiple access point beacon messages. From the pull-down menu, indicate the guest mode that enables clients without any SSID to associate to this access point. See Configure Multiple Service Set Identifiers (SSIDs) on page 285 for detailed procedural information.
Set Infrastructure SSID	When the access point is in repeater mode, this SSID is used to associate with a parent access point. Check the checkbox by the pull-down menu if you want to force infrastructure devices to associate only to this SSID.



Server Manager Page

The Server Manager page is where you to enter the authentication server settings. The RADIUS/TACACS+ server on the your network uses EAP to provide authentication service for wireless client devices.

Figure 37 - Server Manager



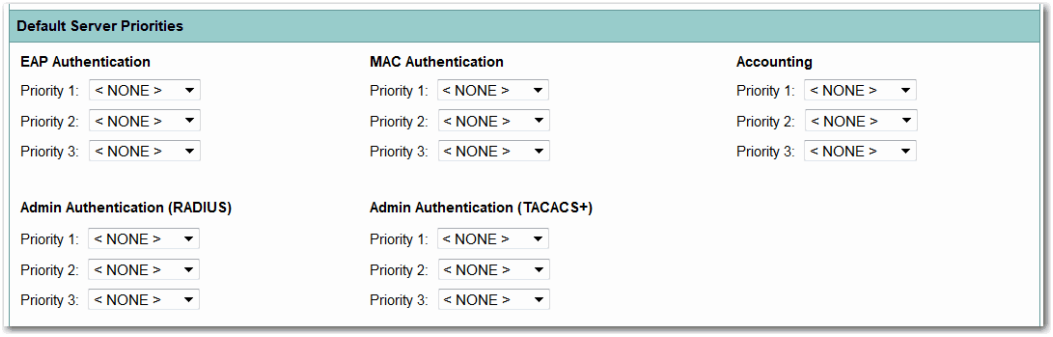


Table 33 - Security: Server Manager Parameter Descriptions

Parameter	Description
Backup RADIUS Server	Enter the host name or IP address of the access point acting as a local RADIUS server. Other access points on your wireless LAN use this backup authenticator when the main RADIUS server does not respond.
Shared Secret	Enter the shared secret used by your Local/Backup RADIUS server. The shared secret on the device must match the shared secret on the Local/ Backup server.
Corporate Servers Current Server List	Identifies the servers that are currently available.
Server	Enter the name or IP address of the server.
Shared Secret	Enter the shared secret used by your RADIUS/TACACS+ server. The shared secret on the device must match the shared secret on the RADIUS/TACACS+ server.
Authentication Port (optional)	Enter the port number your RADIUS/TACACS+ server uses for authentication. The port setting for the Cisco RADIUS server (the Access Control Server [ACS]) is 1645, and the port setting for many RADIUS servers is 1812. Check your server's product documentation to find the correct port setting.
Accounting Port (optional)	Enter the port number your RADIUS server uses for accounting. The port setting for Cisco's RADIUS server (the Access Control Server [ACS]) is 1646, and the port setting for many RADIUS servers is 1813. Check your server's product documentation to find the correct accounting port setting.
Default Server Priorities EAP Authentication	Select the servers to be used for EAP authentication in order of desired priority.
MAC Authentication	Select the servers to be used for MAC authentication in order of desired priority.
Accounting	Select the servers to be used for Accounting in order of desired priority.
Admin Authentication (RADIUS)	Select the servers to be used for RADIUS admin authentication in order of desired priority.
Admin Authentication (TACACS+)	Select the servers to be used for TACACS Admin authentication in order of desired priority.

Server Manager Global Properties

The Server Manager Global Properties page provides more information about the servers you are using and the global locations of those servers.

Figure 38 - Server Manager Global Properties

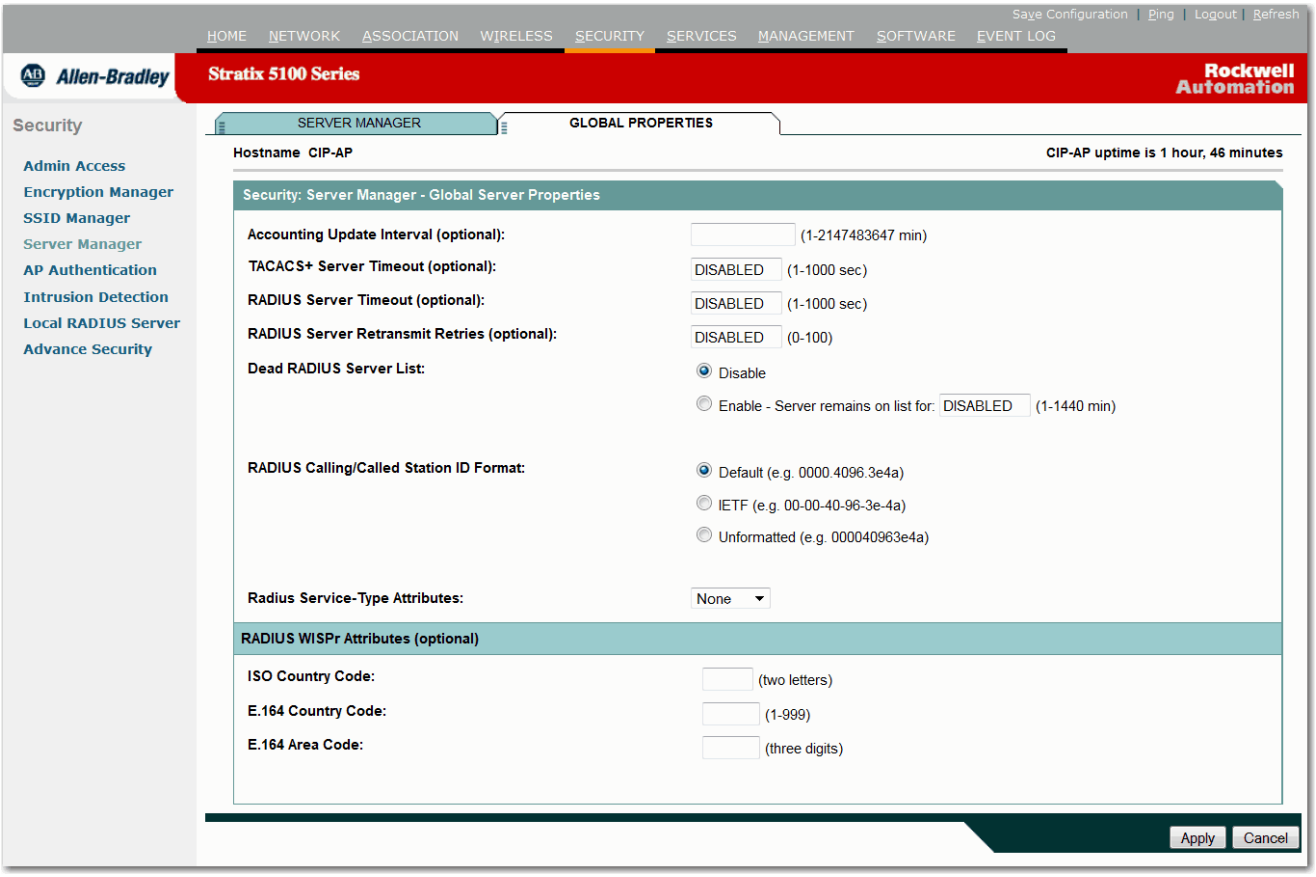


Table 34 - Server Manager Global Properties Parameter Descriptions

Parameter	Description
Accounting Update Interval (optional)	1…2147483647 min
TACACS+ Server Timeout (optional)	1…1000 sec
RADIUS Server Timeout (optional)	1…1000 sec
RADIUS Server Retransmit Retries (optional)	0…100
Dead RADIUS Server List	Enable Server remains on list for 1…1440 min Disable

Table 34 - Server Manager Global Properties Parameter Descriptions

Parameter	Description
RADIUS Calling/Called Station ID Format	Default Example: 0000.4096.3e4a IETF Example: 00-00-40-96-3e-4a Unformatted Example: 000040963e4a
RADIUS Service-Type Attributes	Login Framed
RADIUS WISPr Attributes (optional)	ISO County Code 2 letters E.164 Country Code 1…999 E.164 Area Code three digits

AP Authentication

Traditionally, the dot1x authenticator/client relationship has always been a network device and a PC client respectively, as it was the personal computer user that had to authenticate to gain access to the network. However, wireless networks introduce unique challenges to the traditional authenticator/client relationship.

First, access points can be placed in public places, inviting the possibility that they could be unplugged and their network connection used by an outsider. Second, when a a workgroup bridge or repeater access point is incorporated into a wireless network, the repeater access point must authenticate to the root access point in the same way as a client does. If EAP authentication is used instead of pre-shared keys, authentication credentials need to be configured on the WGB or the repeater.

You must first create and configure a credentials profile and apply the credentials to an interface or SSID. Credentials are used to authenticate the access point to the network.

Figure 39 - AP Authentication

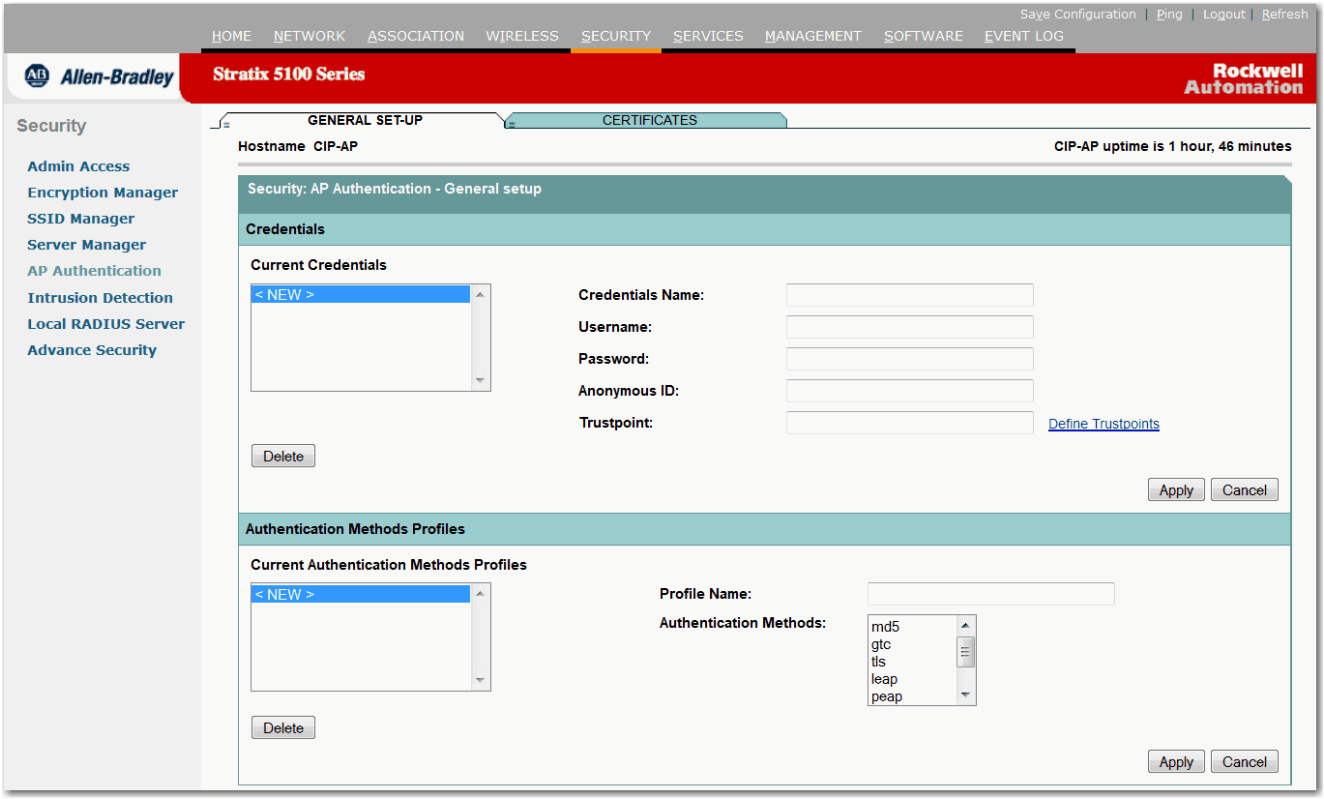


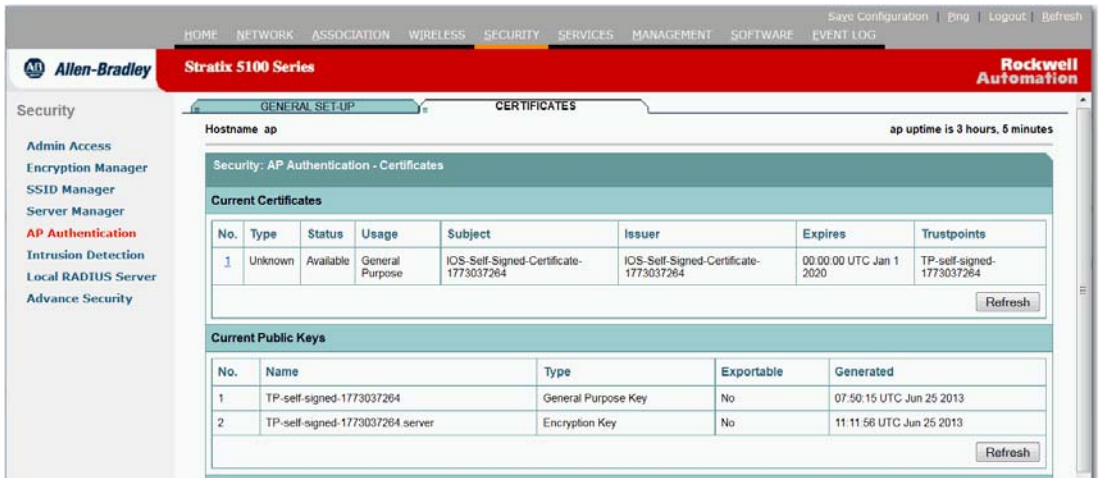
Table 35 - AP Authentication General Set-up Parameter Descriptions

Parameter	Description
Current Credentials	Choose <NEW> if you want to add a dot1x credentials profile.
Credentials Name	Enter a name for the dot1x credentials profile if you are adding a new profile. You can change the name if you have chosen an existing profile.
Username	Enter the authentication user id.
Password	Enter the authentication password.
Anonymous ID	Enter the anonymous identity to be used. Depending on your network authentication requirements, you can configure an anonymous ID instead of a username and password.
Trustpoint	Router certificates and the associated CA certificate are managed through a trustpoint. Enter the default pki-trustpoint. Enter the trustpoint if one is required for network authentication.
Define Trustpoints	If you need to define a trustpoint, click the link to go to the AP Authentication - Certificates page where you can configure the parameters for the trustpoint.
Authentication Methods Profile	Credential profiles are applied to an interface or an SSID in the same way. When an access point connects to the network, the access point and the network authentication device negotiate to agree upon an authentication method supported by both devices to complete authentication. An authentication methods profile is used to restrict the types of authentication that the access point agrees to use. If you wish to restrict the authentication types used to authenticate to the network, define an authentication methods profile and assign it to the relevant SSIDs or GigabitEthernet interface. The restriction can be required to prevent the network authentication server and the access point from negotiating an authentication method such as LEAP rather than a more secure authentication method such as EAP-FAST.
Current Authentication Methods Profile	Choose <NEW> if you want to add an authentication methods profile.
Profile Name	If you are adding a new profile, enter a name for the authentication methods profile. You can change the name if you have chosen an existing profile.
Authentication Methods	Choose the authentication methods that the access point needs to use to authenticate to the network. By choosing a strong authentication method, you can prevent the access point from allowing weaker authentication methods to be approved. For example, if a RADIUS server supports EAP-FAST and LEAP, under certain configurations, the server can initially employ LEAP instead of a more secure method. If no preferred method list is defined in this parameter, LEAP can be chosen rather than the stronger, more advantageous EAP-FAST.

AP Authentication Certificates

This page lists the current certificates and public keys available. You can also configure the parameters for the trustpoint.

Figure 40 - AP Authentication Certificates



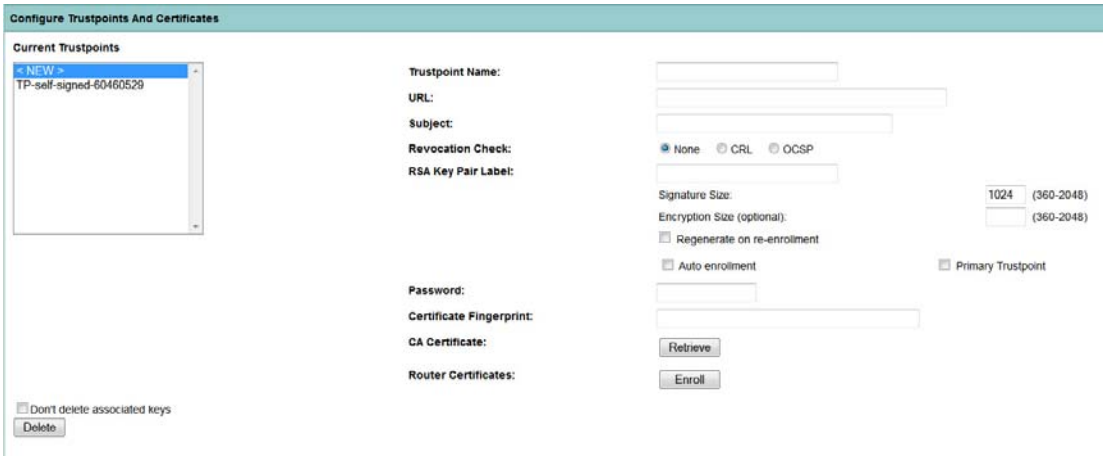


Table 36 - Certificates Page Properties Parameter Descriptions

Parameter	Description
Certificates	Lists the certificates that are currently installed on the access point.
Current Public Keys	Lists the public keys that are available.
Current Trustpoints	Which certificate authorities the access point is currently using for certificate operations. • CA Certificate After defining the trustpoint, click the Retrieve button to download the certificate authority certificate. • Router Certificates After successfully retrieving the CA certificate, click the Enroll button to enroll the access point certificate(s) with the CA. This sends a certificate enrollment request to the CA and installs the received certificate(s). This may happen immediately or might take some time depending on the settings of the CA. For example, some CAs are set to immediately issue the certificate, while some might require human intervention, delaying the issuance of the certificate for some time. • Don't delete associated keys When a trustpoint is deleted, the associated RSA keys are also deleted. If you want to keep the keys intact, this option must be chosen before deleting the trustpoint.
Trustpoint Name	The unique name assigned to define or group the details of the certificate authority together.
URL	The enrollment URL of the CA (varies from vendor to vendor).
Subject	The details of the subject field in the requested X.509 certificate.
Revocation Check	Specifies whether to perform a certificate renovation check for a received certificate. For EAP-TLS, this should be set to None.
RSA Key Pair Label	An optional name to identify the RSA keys for the certificate.
Signature/Encryption Size	The number of bits required for the RSA keys. Larger sizes are more secure.
Regenerate on Enroll	If this option is chosen, the RSA keys generate when the certificate is enrolled with the certificate authority.
Auto-enroll	Certificates are automatically enrolled when the trustpoint is configured. You do not need to explicitly download the CA certificate and then enroll the router certificate because it is done automatically.
CA Certificate	After defining the trustpoint, click the Retrieve button to download the certificate authority certificate.

Table 36 - Certificates Page Properties Parameter Descriptions

Parameter	Description
Router Certificates	After successfully retrieving the CA certificate, click the Enroll button to enroll the access point certificate(s) with the CA. This sends a certificate enrollment request to the CA and installs the received certificate(s). This may happen immediately or might take some time depending on the settings of the CA. For example, some CAs are set to immediately issue the certificate, while some might require human intervention, delaying the issuance of the certificate for some time.
Don't delete associated keys	When a trustpoint is deleted, the associated RSA keys are also deleted. If you want to keep the keys intact, this option must be chosen before deleting the trustpoint.
Current Trustpoints	• CA Certificate After defining the trustpoint, click the Retrieve button to download the certificate authority certificate. • Router Certificates After successfully retrieving the CA certificate, click the Enroll button to enroll the access point certificate(s) with the CA. This sends a certificate enrollment request to the CA and installs the received certificate(s). This may happen immediately or might take some time depending on the settings of the CA. For example, some CAs are set to immediately issue the certificate, while some might require human intervention, delaying the issuance of the certificate for some time. • Don't delete associated keys When a trustpoint is deleted, the associated RSA keys are also deleted. If you want to keep the keys intact, this option must be chosen before deleting the trustpoint.

Intrusion Detection

Management frame protection can be used to identify adversaries that are invoking denial of service attacks, flooding the network with associations and probes, interjecting as rogue access points, or affecting the network performance by attacking the QoS and radio measurement frames.

Figure 41 - Intrusion Detection: Management Frame Protection

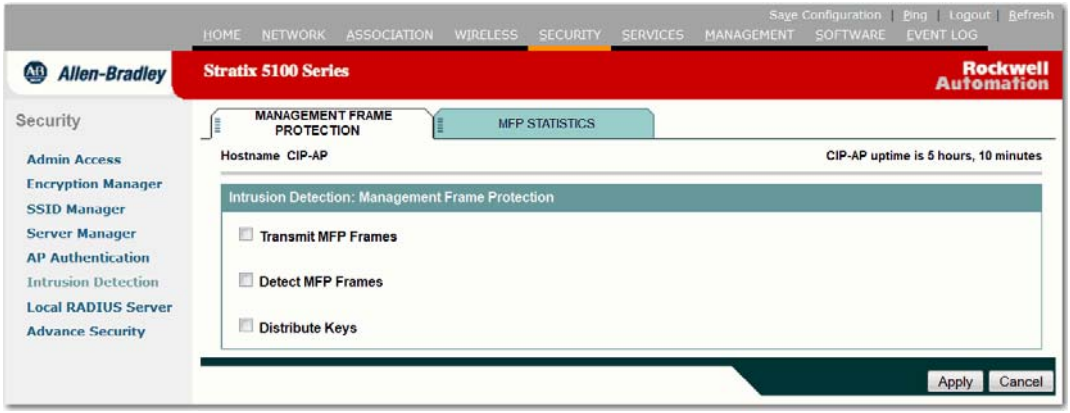


Figure 42 - Intrusion Detection: MFP Statistics

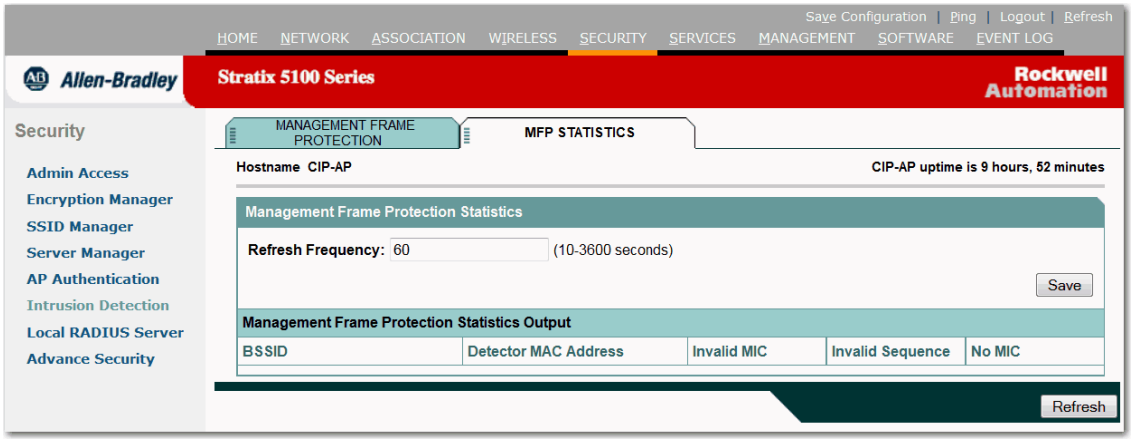


Table 37 - Intrusion Detection Page Parameter Descriptions

Parameter	Description
Transmit MFP Frames	When enabled, the access point protects the management frames it transmits by adding a message integrity check information element (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. An access point must be a member of a WDS to transmit MFP frames. If it is not, a warning message appears on this page.
Detect MFP Frames	When MFP detection is enabled, 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. The access point must be a member of a WDS to detect MFP frames. If it is not, a warning message appears on this page.
Distribute Keys	At least one WDS in the network must be configured to distribute signature keys to the MFP generators (protectors) and MFP detectors (validators) in the network. These are required by the generators to create MIC IEs and by the detectors to validate MIC IEs. This checkbox is not present if the access point cannot be a WDS.

Local RADIUS Server

Usually an external RADIUS Server is used to authenticate users. In some cases, this is not a feasible solution. In these situations, an access point can be made to act as a RADIUS Server. Here, users are authenticated against the local database configured in the access point. This is called a Local RADIUS Server feature. You can also make other access points in the network use the Local RADIUS Server feature on an access point.

Figure 43 - Local RADIUS Server Statistics Page

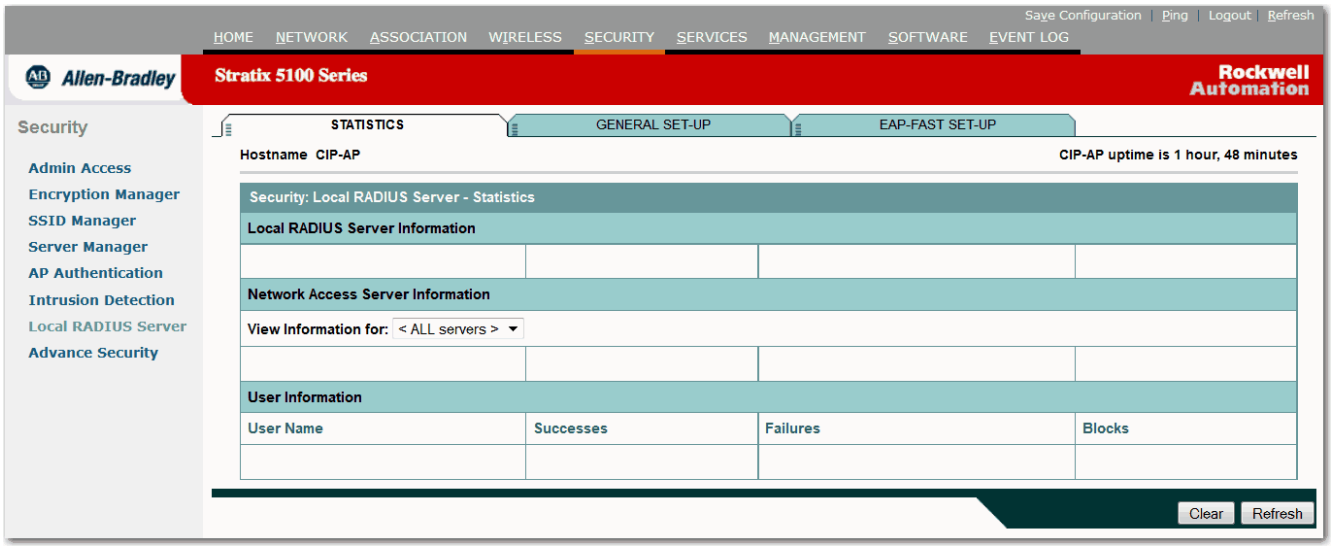


Table 38 - Local RADIUS Server Statistics Page Parameter Descriptions

Parameter	Description
Network Access Server xx.xx.xx.xx	Choose the network access server that you want to view. The network access server is the access point configured to use the local RADIUS server as a backup authenticator.
User Name	Displays the username of the active user.
Successes	The number of successful authentications.
Failures	The number of authentications that failed for this user, generally because of a bad password.
Blocks	The number of times an authentication was ignored as a result of a username being blocked because too many failed authentications had occurred.

Figure 44 - Local RADIUS Server General Set-up Page

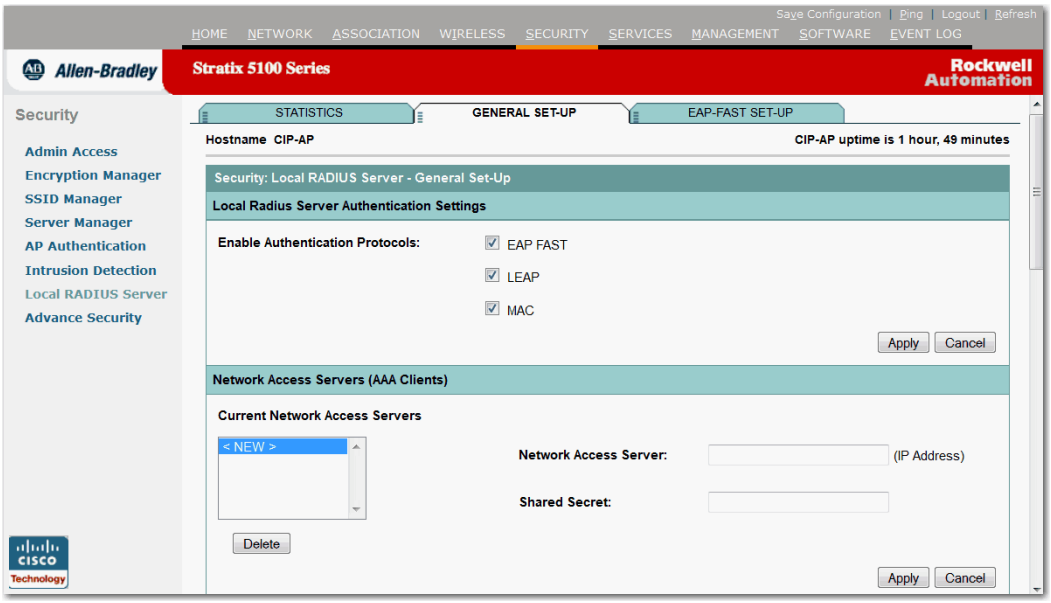
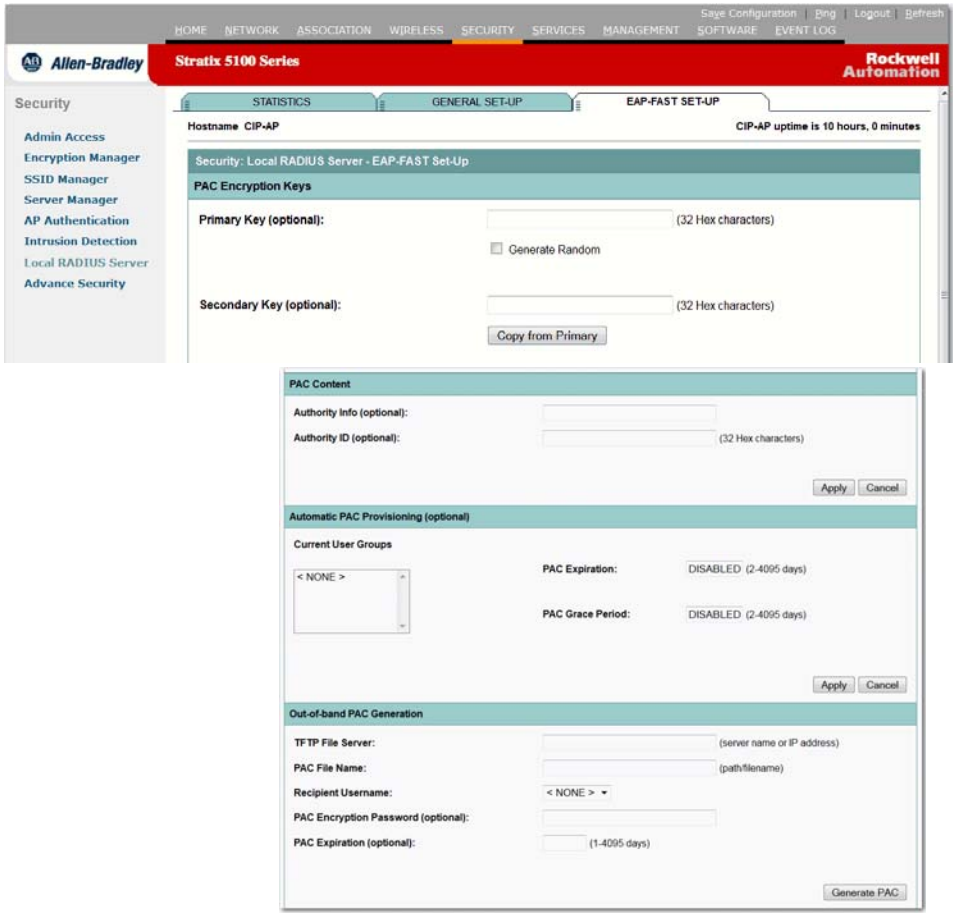


Table 39 - Local RADIUS Server General Set-up Page Parameter Descriptions

Parameter	Description
Enable Authentication Protocols	EAP FAST LEAP MAC
Network Access Server (AAA Clients)	Current Network Access Servers Network Access Server (IP Address) Shared Secret
Individual Users	Current Users Username: Text or NT Hash Password Group name MAC Authentication Only
User Groups	Current User Groups Group name Session Timeout (optional): 1…4294967295 s Failed Authentications before Lockout (optional): 1…4294967295 s Lockout (optional): Infinite or Interval 1…4294967295 s VLAN ID (optional) SSID (optional)

Figure 45 - Local RADIUS Server EAP-Fast Set-up Page



TIP The default settings for EAP-FAST authentication are suitable for most wireless LANs. However, you can customize the credential timeout values, authority ID, and server keys to match your network requirements.

Table 40 - Local RADIUS Server EAP-Fast Set-up Page Parameter Descriptions

Parameter	Description
PAC Encryption Keys	• Primary Key (optional): 32 Hex characters; Generate Random • Secondary Key (optional): 32 Hex characters; Copy from primary
PAC Content	• Authority Info (optional) • Authority ID (optional) 32 Hex characters
Automatic PAC Provisioning (optional)	Current User Groups • PAC Expiration: 2…4095 days • PAC Grace Period: 2…4095 days
Out-of- PAC Generation	• TFTP File Server: server name or IP address • PAC File Name: path/filename • Recipient Username • PAC Encryption Password (optional) • PAC Expiration (optional): 1…4095 days

Advanced Security

You can set up the access point to authenticate client devices using a combination of MAC-based and EAP authentication, see SSID Manager Page on page 109. When you enable this feature, client devices that associate to the access point using 802.11 open authentication first attempt MAC authentication.

- If MAC authentication succeeds, the client device joins the network.
- If MAC authentication fails, the access point waits for the client device to attempt EAP authentication.

Figure 46 - MAC Address Authentication Page

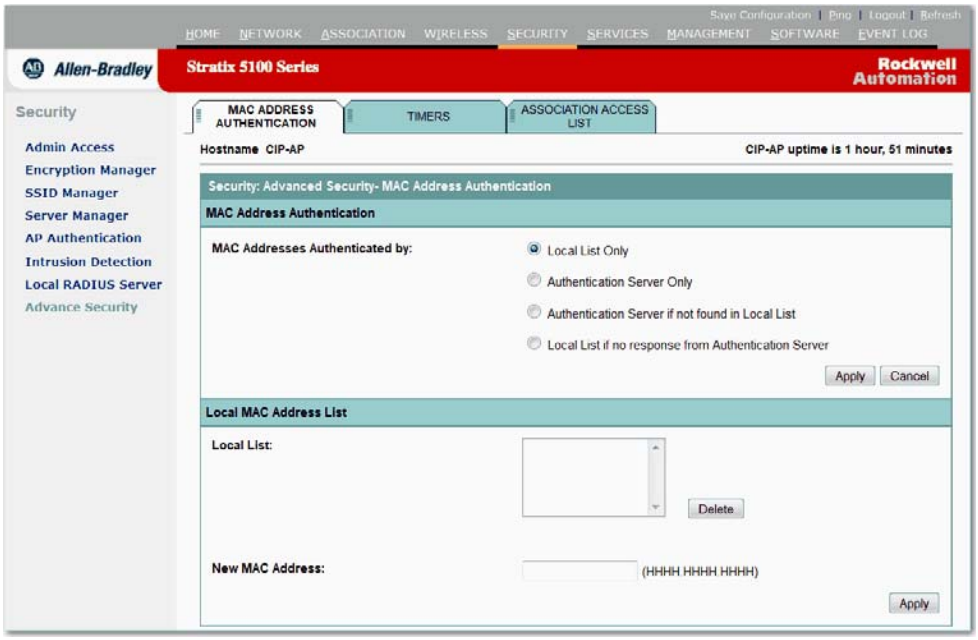


Table 41 - MAC Address Authentication Page Parameter Descriptions

Parameter	Description
MAC Addresses Authenticated by	Local list only • If you want the authentication to be stored on the access point, choose Local List Only and enter MAC addresses. Authentication Server Only • If you want the authentication to be stored on the server, choose the Authentication Server Only option. Authentication Server if not found in Local List • Choose Authentication Server if not found in Local List if you want to try MAC authentication list first and then automatically try the Authentication server list. If the authentication succeeds, the client joins the network. Local List if no response from Authentication Server • You are required to select at least one MAC Authentication on the Server Manager page if you select either Authentication Server Only or Authentication Server if not found in Local List.
Local MAC Address List	Local List • The MAC addresses appear in the Local List. The MAC addresses remain in the management system until you remove them. To remove the MAC address from the list, select it and click Delete. New MAC Address: HHHH.HHHH.HHHH • If you need to enter a new MAC address, type the address with periods separating the three groups of four characters, for example, 40.9612.3456. • To make sure the filter operates properly, use lower case for all the letters in the MAC addresses that you enter. Click Apply to put the MAC address in the management system. You must also enable MAC address authentication on the SSID Manager page. You can navigate to the Association page to verify that the preconfigured clients were associated and authenticated.

Figure 47 - Timers Page

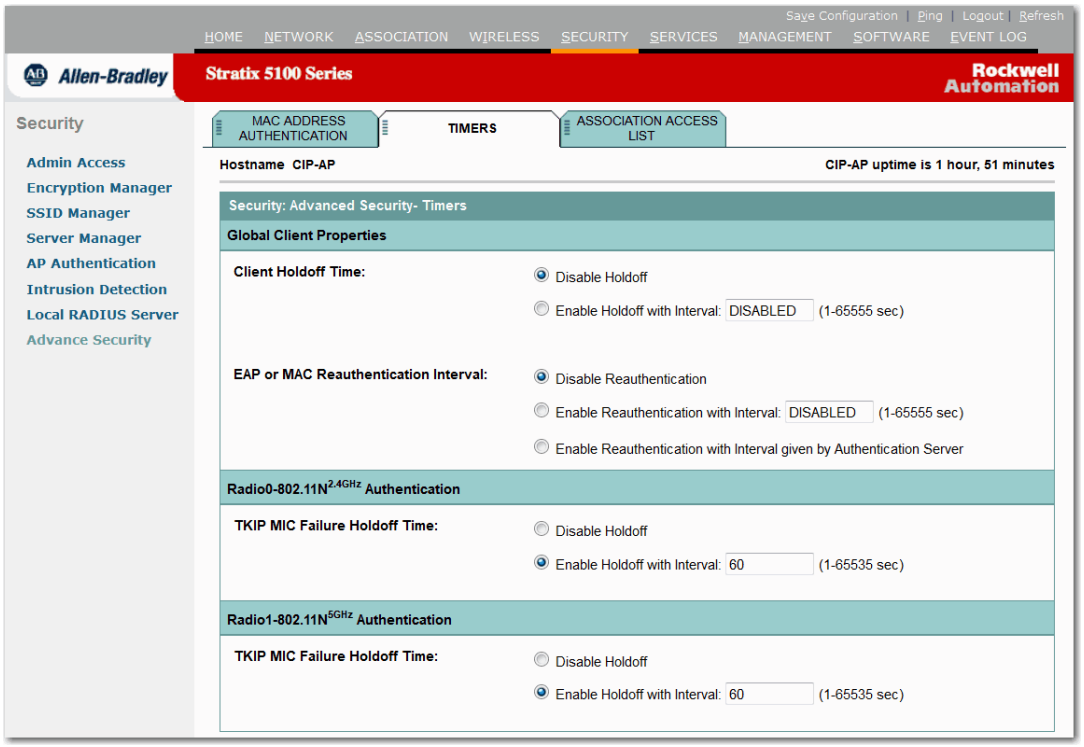


Table 42 - Timers Page Parameter Descriptions

Parameter	Description
Global Client Properties	Client Holdoff Time Disable Holdoff Enable Holdoff with Interval: 1…65555 s
EAP or MAC Reauthentication Interval	Disable Reauthentication Enable Reauthentication with Interval: 1…65555 s Enable Reauthentication with Interval given by Authentication Server
Radio0-802.11N2.4 GHz Authentication	TKIP MIC Failure Holdoff Time Disable Holdoff Enable Holdoff with Interval: (1…65535 s)
Radio1-802.11N2.4 GHz Authentication	TKIP MIC Failure Holdoff Time Disable Holdoff Enable Holdoff with Interval: (1…65535 s)
Association Access List Page Parameter Descriptions	Filter client association with MAC address access list Define Filter: Link takes you to MAC Address Filters on the Services page.

Figure 48 - Associated Access list Page

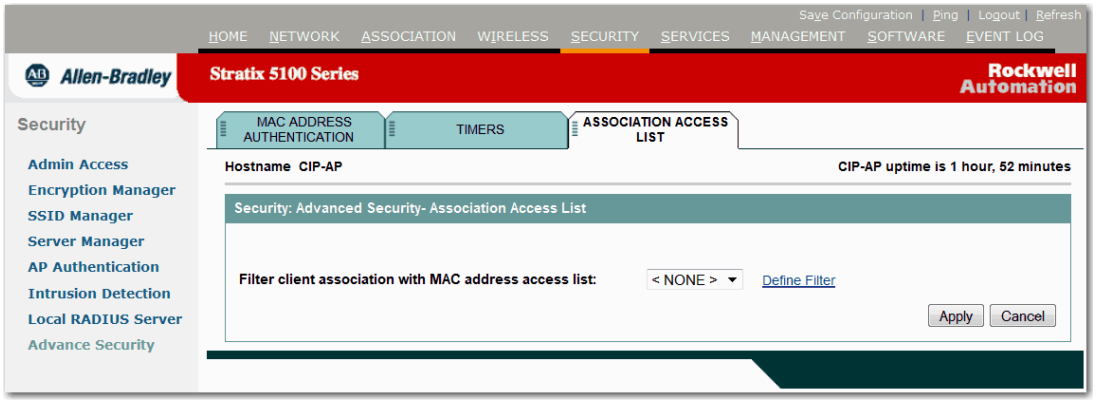


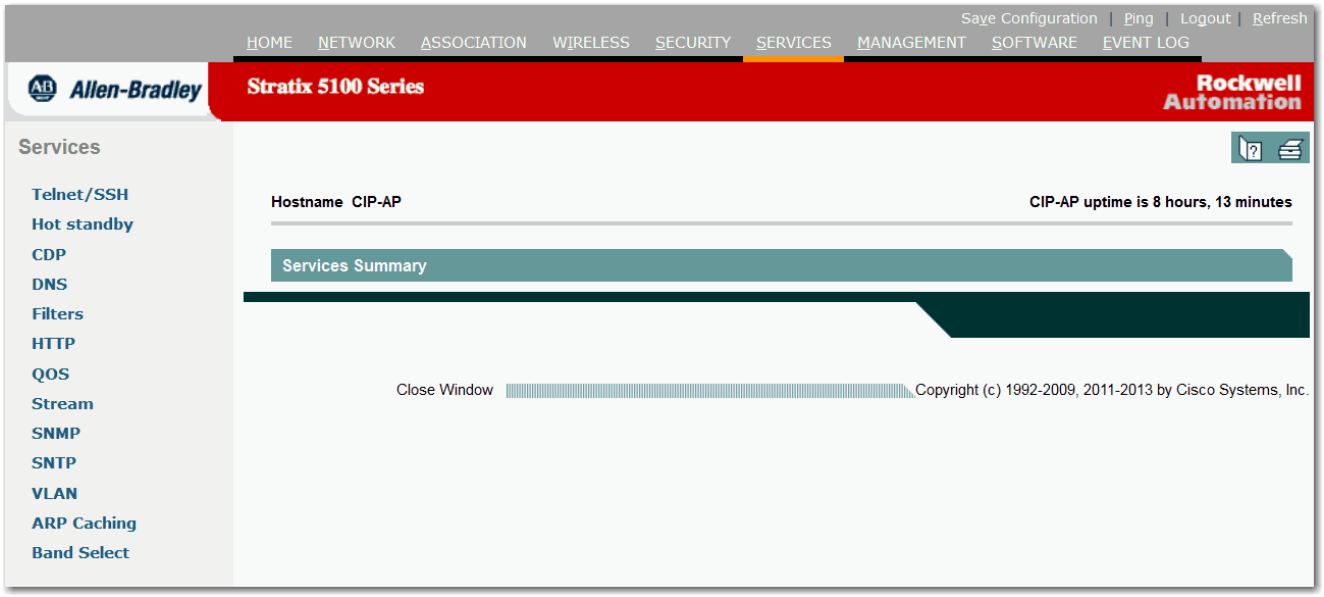
Table 43 - Association Access List Page Parameter Descriptions

Parameter	Description
Filter client association with MAC address access list	Select a filter.
Define Filter	This link takes you to Service>Filter where you can configure filters.

Services Page

The summary provides a list of the main services that are currently enabled or disabled. You can click any of the links to go to that page and change the configurations.

Figure 49 - Services Page



Telnet/SSH

Figure 50 - Telnet/SSH Page

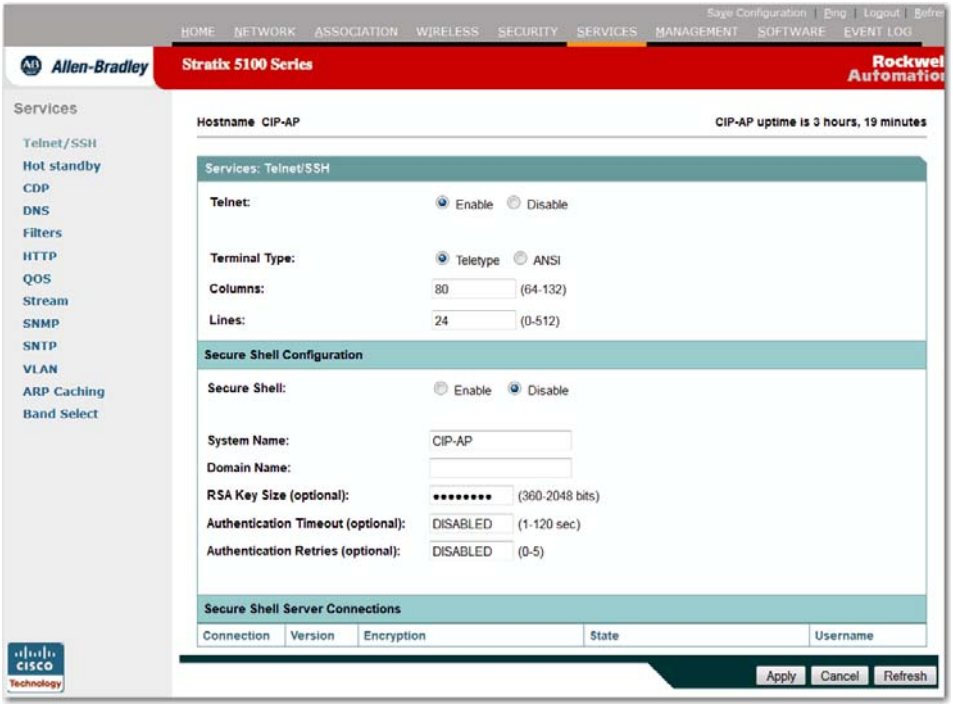


Table 44 - Telnet/SSH Page Parameter Descriptions

Parameter	Description
Telnet	• Telnet Enable or Disable. Select Enable to allow management systems to use Telnet protocol to access the WAP. • Terminal Type Teletype or ANSI. The preferred setting is ANSI, that offers graphic features such as reverse video buttons and underlined links. Not all terminal emulators support ANSI, so the default setting is Teletype. • Columns 64…132 Defines the width of the terminal emulator display, ranging from 64…132 characters. Adjust the value to get the optimum display for your terminal emulator. • Lines 0…512 Defines the height of the terminal emulator display, ranging from 16…50 characters. Adjust the value to get the optimum display for your terminal emulator.
Secure Shell Configuration	Secure shell enables a strong encryption to be used with the Cisco IOS software authentication. Secure Shell • Enable or Disable • Select Enabled if you want to enable the secure shell (SSH) feature to provide a secure, remote connection to the access point using standard cryptographic mechanisms. System Name • The host system name for your access point. Domain Name • The host domain for your access point. Required to generate keys for SSH. RSA Key Size (optional) • The size of the RSA key pair generated for the access point. Authentication Timeout (optional): 1…120 s • The time the access point waits for the client to respond during the SSH negotiation stage. Authentication Retries (optional): 0…5 • The number of SSH negotiation attempts made before the interface is reset.
Secure Shell Server Connections	This is the status of the SSH server connections. • Connection A unique number that identifies an SSH session. • Version The protocol version number that the SSH client supports. • Encryption The type of encryption the SSH client is using. • State The progress of the SSH session. • Username The login username that has been authenticated for the session.

Hot Standby Page

Figure 51 - Hot Standby Page

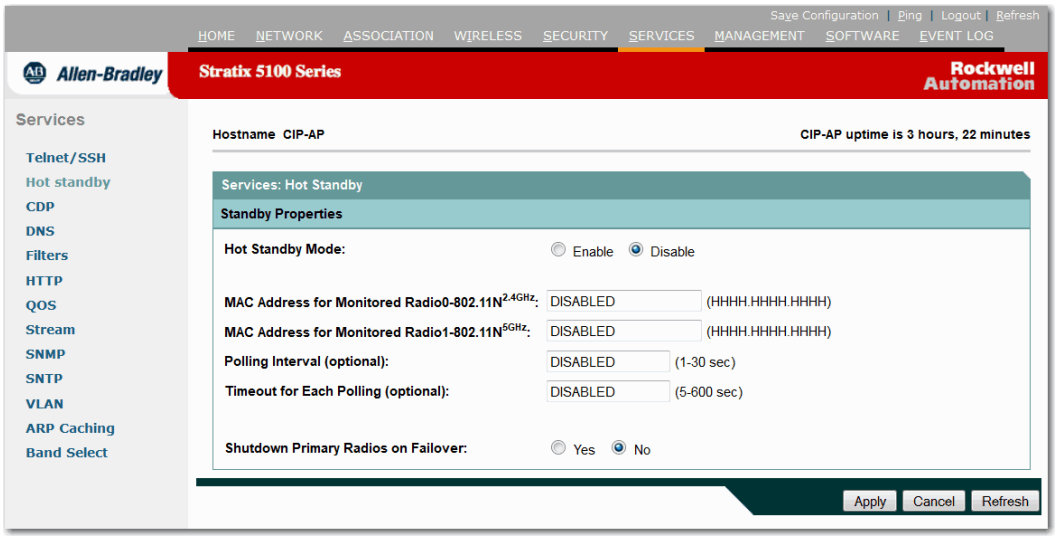


Table 45 - Hot Standby Page Parameter Descriptions

Parameter	Description
Hot Standby Mode	Enabling hot standby designates this device as a backup for another access point. The standby device is placed near the access point it monitors, configured exactly the same as the monitored device. The standby device queries the monitored access point regularly through both the Ethernet and the radio. If the monitored device fails to respond, the standby access point comes online and takes the monitored device's place in the network. When hot standby is enabled, a Standby Status field displays. This field displays the current status of the hot standby and is updated by pressing Refresh.
MAC Address for Monitored Radio0-802.11N2.4 GHz	MAC Address for Monitored 802.11 b/g/n Radio: HHHH.HHHH.HHHH The monitored device's MAC address.
MAC Address for Monitored Radio1-802.11N5 GHz	MAC Address for Monitored 802.11a/n Radio: HHHH.HHHH.HHHH The monitored device's MAC address.
Polling Interval (optional)	The number of seconds between each query that the standby device sends to the monitored access point.
Timeout for Each Polling (optional)	The number of seconds the standby device needs to wait for a response from the monitored access point before it assumes the monitored device has malfunctioned.
Shutdown Primary Radios on Failover	Select Yes if you want to configure the standby access point to send a Dumb Device Protocol (DDP) message to the monitored access point to disable the radios of the monitored access point when the standby unit becomes active. This feature prevents client devices that are associated to the monitored access point from remaining associated to the malfunctioning unit.

ATTENTION: Clients associated to the standby access point lose their connection during the hot standby setup process.

CDP Page

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices. Information in CDP packets is used in network management software. Use the CDP page to adjust the device's CDP settings.

Figure 52 - CDP Page

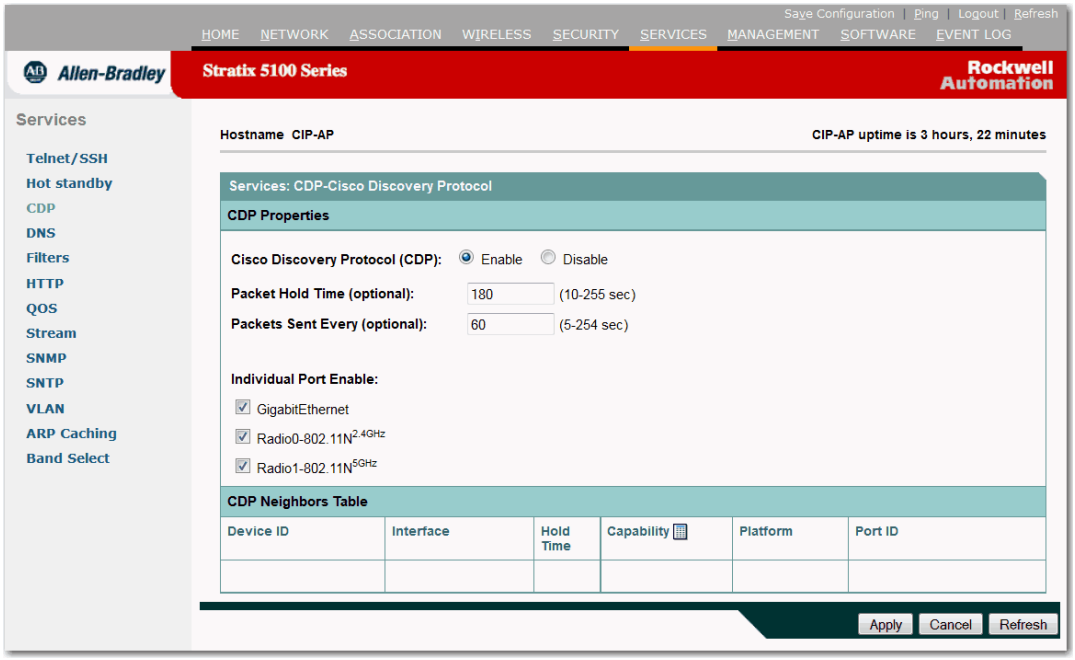


Table 46 - CDP Page Parameter Descriptions

Parameter	Description
Cisco Discovery Protocol (CDP)	Select Disabled to disable CDP on the device; select Enabled to enable CDP on the device. CDP is enabled by default.
Packet Hold Time (optional)	The number of seconds other CDP-enabled devices need to consider the CDP information valid. If other devices do not receive another CDP packet from the device before this time elapses, the device has probably gone offline. The default value is 180. The packet hold time needs to always be greater than the value in the Packets Sent Every field.

Table 46 - CDP Page Parameter Descriptions (Continued)

Parameter	Description
Packets Sent Every (optional)	The number of seconds between each CDP packet that the device sends. The default value is 60. This value needs to be less than the packet hold time.
Individual Port Enable	• Ethernet When selected, the device sends CDP packets through its Ethernet port and monitors the Ethernet for CDP packets from other devices. • Access point Radio Options When selected, the device sends CDP packets through its internal radio port and monitors the internal radio for CDP packets from other devices. Note: A MIB file is available for use with CDP. The filename is CISCO-CDP-MIB.my, and you can download the MIB at http://www.cisco.com/public/mibs/v1/CISCO-CDP-MIB-V1SMI.my.
CDP Neighbors Table	This section displays the type of device that is discovered. Specifically, it displays these values. • Device ID The configured ID, MAC address, or serial number of the device. • Interface The number and type of the local interface protocol being used. • Hold time The number of remaining seconds the current device holds the CDP advertisement from a transmitting router before discarding it. • Capability The device type as listed in the CDP Neighbors table. Possible values are R for router, T for transparent bridge, B for source-routing bridge, S for switch, H for host, I for IGMP device, or r for repeater. If you click the calculator image, you see a popup with the legend of code to capability. • Platform The device product number. • Port ID The protocol and port number of the device.

DNS Page

This page is where you decide if you want the DNS (Domain Name System) enabled or disabled. The DNS is a name resolution server that lets you connect to a device without knowing its IP address but instead by using a given name. So after you give the WAP a name and you assign the DNS server to use, you need to make sure that the DNS Server has a record of the WAP.

Figure 53 - DNS Page

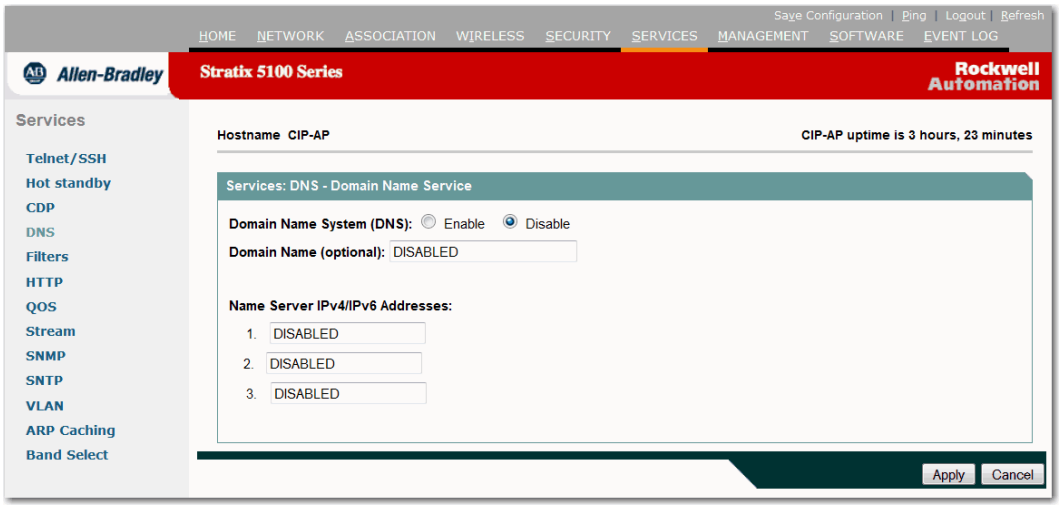


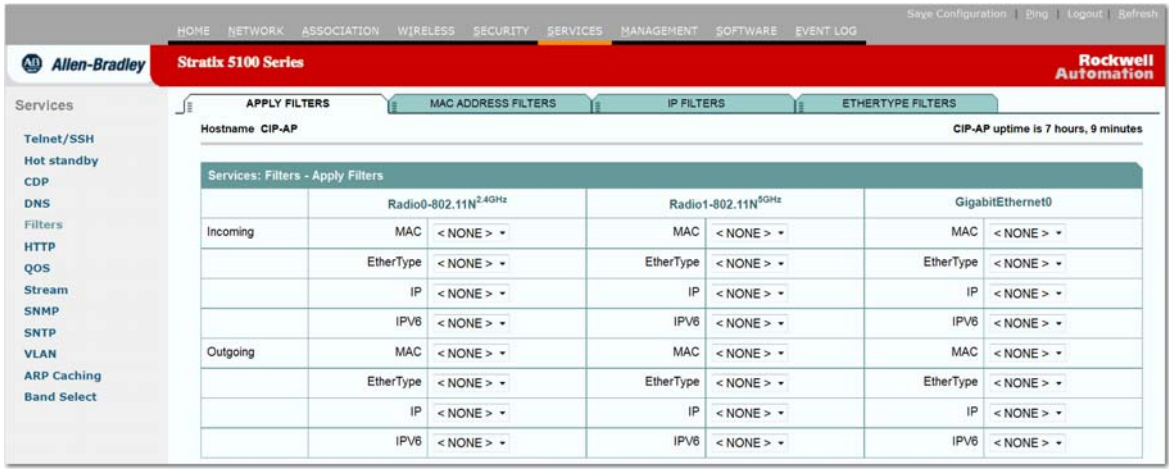
Table 47 - DNS Page Parameter Descriptions

Parameter	Description
Domain Name System (DNS)	Choose if you want DNS enabled or disabled. If you enable DNS, at least one domain name server needs to be entered.
Domain Name (optional)	If your network uses a Domain Name System (DNS), enter the name of your network's IP domain. Your entry can look like mycompany.com.
Name Server IP Addresses	Enter the IP addresses of up to three domain name servers on your network.

Filters Page

Protocol filters prevent or allow the use of specific protocols through the interface. You can set up individual protocol filters or sets of filters. This base page enables you to apply the filters for incoming and outgoing Ethernet and radio interfaces. Filters must be created before they can be applied Protocol filters are commonly called Access Control Lists (ACL).

Figure 54 - Filters Page



Any filters you set on the MAC Address, IP Filters, or Ethertype Filters pages are not applied until they are enabled on this Apply Filters page.

Apply filters with caution. Misconfigured filters can lock you out of the access point. If this happens, the recovery methods are console port accesses (if available) or resetting of the access point to the default configuration.

Table 48 - Apply Filters Page Parameter Descriptions

Parameter	Description
Incoming	From the pull-down menu, select the protocol filter set that you want to enable for MAC, Ethertype, and IP.
Outgoing	From the pull-down menu, select the protocol filter set that you want to enable for MAC, Ethertype, and IP.

MAC Address Filters Page

Use this page to allow or disallow the forwarding of unicast or multicast packets sent from or addressed to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming or outgoing packets.

Figure 55 - MAC Address Filters Page

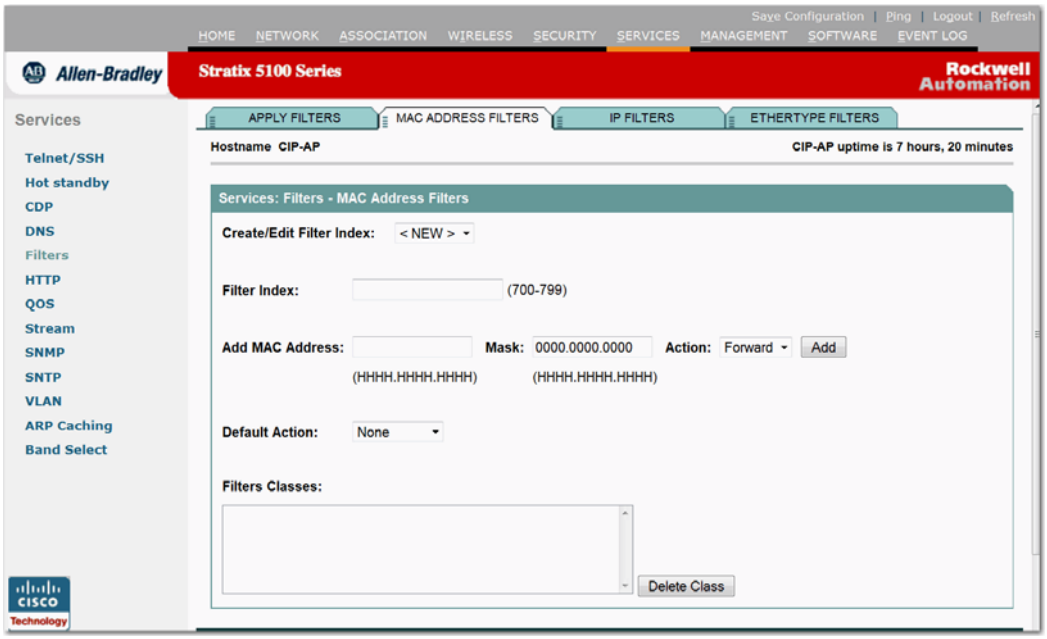


Table 49 - MAC Address Filters Page Parameter Descriptions

Parameter	Description
Create/Edit Filter Index	If you are creating a new MAC address filter, make sure to select <NEW> (the default).
Filter Index	Name the filter with a number from 700…799. The number you assign creates an access control list (ACL) for the filter.
Add MAC Address	Type a destination MAC address with the periods separating the three groups of four characters, for example, 0040.9612.3456. To make sure the filter operates properly, use lower case for all the letters in the MAC addresses that you enter. If you plan to block traffic to all MAC addresses except those you specify as allowed, put your MAC address in the list of allowed MAC addresses.
Mask	Type the mask for the MAC address. Enter the mask with periods separating the four groups of three characters, for example, 255.255.255.0. Entering 255.255.255.255 as the mask causes the access point to accept any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered in the IP Address field.

Table 49 - MAC Address Filters Page Parameter Descriptions (Continued)

Parameter	Description
Action	Select Forward or Block. Click Add. The MAC address appears in the Filters Classes field.
Default Action	Packets that do not match any of the Filters Classes are handled according to the Default Action. Select Forward All or Block All. The filter's default action must be opposite of the action for at least one of the addresses in the filter. For example, if you enter several addresses and you select Block as the action for all of them, you must choose Forward All as the filter's default action. When you click Apply, the filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.
Filters Classes	To remove the MAC address from the Filters Classes list, select it and click Delete Class.

IP Filters Page

Use this page to create or edit protocol filters. IP filters prevent or allow the use of IP address(es), IP protocols, and TCP/UDP ports through the access point's Ethernet and radio ports. You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify. You can create filters that contain elements of one, two, or all three IP filtering methods. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Figure 56 - IP Filters Page

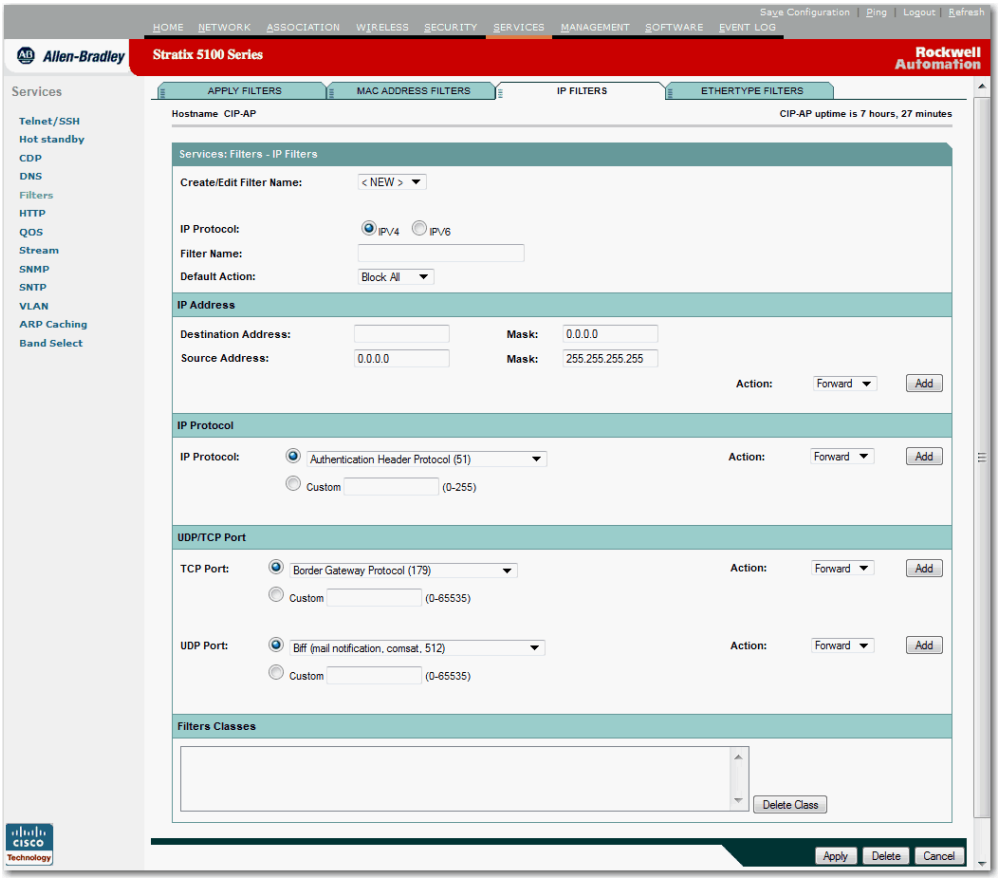


Table 50 - IP Filters Page Parameter Descriptions

Parameter	Description
Create/Edit Filter Name	If you are creating a new filter, make sure to select <NEW> (the default) from the Create/Edit Filter drop-down menu. To edit an existing filter, select the filter name from the Create/Edit Filter drop-down menu.
IP Protocol	IPV4 IPV6
Filter Name	Enter a descriptive name for the new filter.

Table 50 - IP Filters Page Parameter Descriptions (Continued)

Parameter	Description
Default Action	Packets that do match any of the Filters Classes are handled according to the Default Action. Select Forward All or Block All as the filter's default action. The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you create a filter containing an IP address, an IP protocol, and an TCP/UDP port, and you select Block as the action for all of them, you must choose Forward All as the filter's default action.
Destination Address	This is where you identify the destination IP address you want to filter. If you plan to block traffic to all IP addresses except those you specify as allowed, put the address of your own PC in the list of allowed addresses to avoid losing connectivity to the access point.
Source Address	This is where you identify the source IP address you want to filter. If you plan to block traffic to all IP addresses except those you specify as allowed, put the address of your own PC in the list of allowed addresses to avoid losing connectivity to the access point.
Mask	Type the mask for the destination IP address. Enter the mask with periods separating the three groups of four characters, for example, 255.255.255.0. • If you enter 255.255.255.255 as the mask, the access point accepts any IP address. • If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered in the IP Address field.
IP Protocol	This is where you can filter an IP protocol. Select one of the common protocols from the pull-down menu or click Custom and enter the custom IP protocol number in the Custom field. Most commonly used IP protocols are TCP (6) and UDP (17). Enter an IP protocol number from 0… 255.
TCP Port	This is where you can filter a TCP protocol. Select one of the common port protocols from the pull-down menu or select the Custom radio button and enter the TCP port number in one of the Custom fields. Enter a TCP port number from 0…65535.
UDP Port	This is where you can filter a UDP protocol. Select one of the common port protocols or check the Custom radio button and enter the UDP port number in one of the Custom fields. Enter a UDP port number from 0… 65535.
Filters Classes	The protocols appear on this portion of the page. To remove the protocol from the Filters Classes list, select it and click Delete Class.

Ethertype Filters Page

Ethertype filters prevent or allow the use of specific Layer 2 protocol on Ethernet through the access point's Ethernet and radio ports. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Figure 57 - Ethertype Filters Page

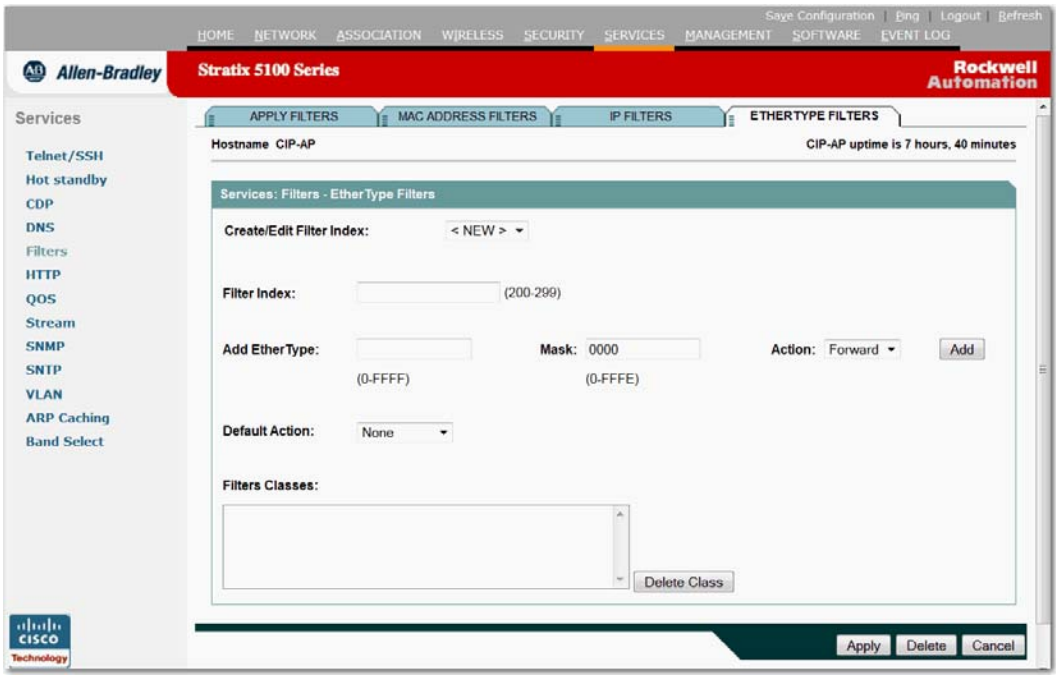


Table 51 - Ethertype Filters Page Parameter Descriptions

Parameter	Description
Create/Edit Filter Index	If you are creating a new filter, make sure <NEW> (the default) is selected in the Create/Edit Filter Index menu. To edit an existing filter, select the filter number from the Create/Edit Filter Index menu.
Filter Index	Name the filter with a number from 200…299. The number you assign creates an access control list (ACL) for the filter.
Add Ethertype	This is where you identify the Ethertype number and enter the mask for the Ethertype.
Default Action	Packets that do not match any of the Filters Classes are handled according to the Default Action. You can select Forward All or Block All. The filter's default action must be opposite of the action for at least one of the Ethertypes in the filter. For example, if you enter several Ethertypes and you select Block All as the action, you must choose Forward All as the filter's default action.
Filters Classes	Displays the current list of filters that you have configured.

HTTP Page

Use the Web Server page to enable browsing to the web-based management system files and enter settings for a custom-tailored web system for management.

Figure 58 - HTTP Page

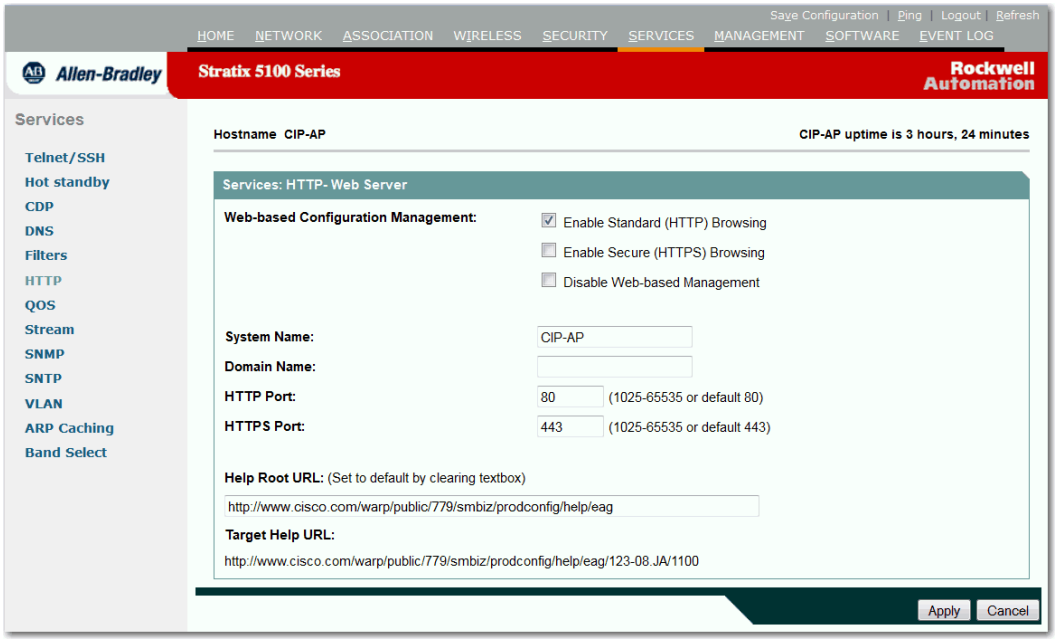


Table 52 - HTTP Page Parameter Descriptions

Parameter	Description
Web-based Configuration Management	Check Enable Standard (HTTP) Browsing to allow non-secure browsing of the management system. Check Enable Secure (HTTPS) Browsing to allow secure (SSL) browsing of the management system. It is not recommended to select both. Select Disable Web-based Management to prevent browsing of the management system. In this mode, the access point is accessible only through the console and Telnet/SSH interfaces. When HTTPS is enabled for the first time, a self-signed certificate is generated and stored in the access point. The certificate is based on your current System Name and Domain Name. The certificate is presented to the browser on each subsequent access to establish an SSL connection. The certificate can be installed in your browser or it can be approved on each access. A warning appears in browsers if the hostname and domain name in the certificate do not match those in the URL. To avoid this warning, the System Name and Domain Name must match the Fully Qualified Domain Name instead of an IP address when browsing the access point. Select Delete Existing SSL Certificate if the System Name or Domain Name has been changed. This generates a new certificate.
System Name (or Host Name)	The name of the system that appears in the titles of management system pages and in the Association page, helping to identify the device on your network. The system name is stored in the self-signed certificate that is used to establish a secure browser connection.
Domain Name	The name of your network's IP domain (such as mycompany.com). The domain name is stored in the self-signed certificate that is used to establish a secure browser connection.

Table 52 - HTTP Page Parameter Descriptions (Continued)

Parameter	Description
HTTP Port	This setting determines what port your device provides non-secure web access. Use the port setting provided by your System Administrator. The default is 80.
HTTPS Port	This setting determines what port your device provides secure (SSL) web access. Use the port setting provided by your system administrator. The default is 443.
Target Help URL	Displays the complete URL for the help files, including the appended version number and model number.

QoS Policies Page

This page lets you configure the quality of service (QoS) on your access point. With this feature, you can provide preferential treatment to certain traffic. Without QoS, the access point offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.

Figure 59 - QoS Policy Page

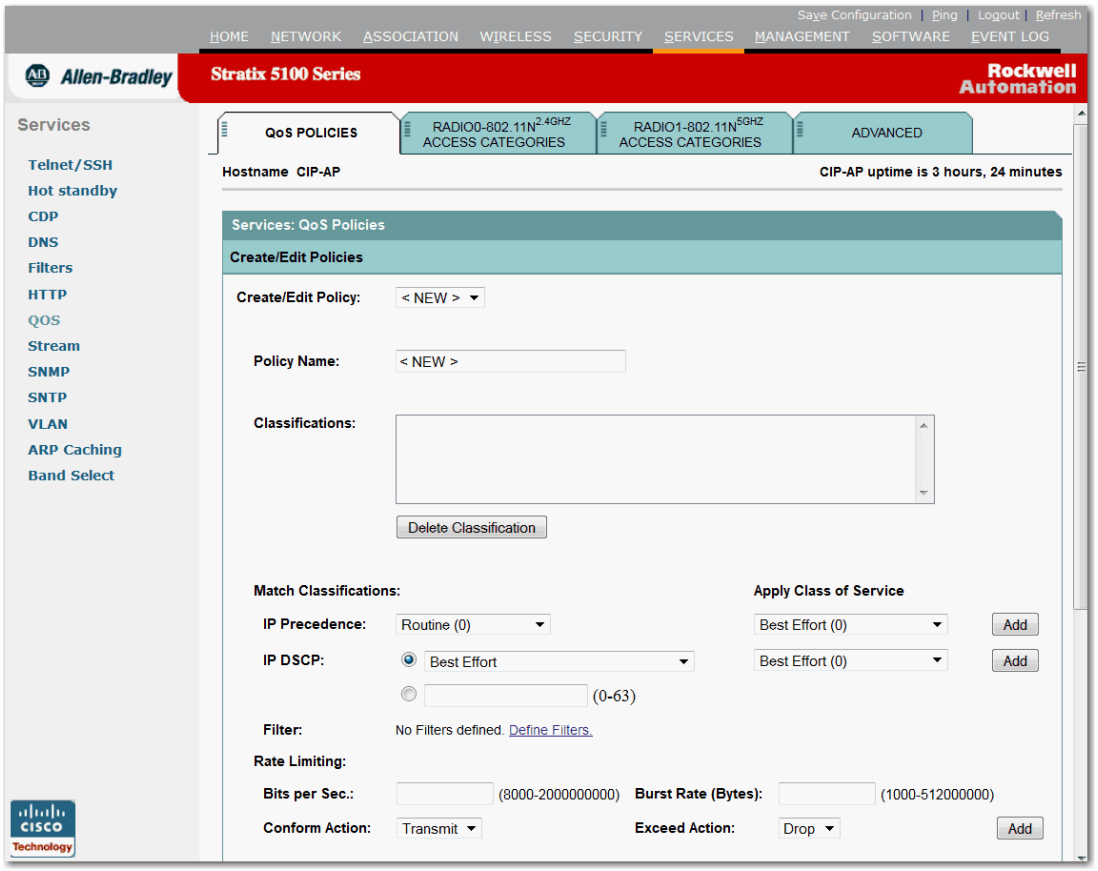


Table 53 - QoS Policies Page Parameter Descriptions

Parameter	Description
Create/Edit Policies	If you are entering a new policy, make sure <NEW> (the default) is selected in the Create/Edit Policy menu. To edit an existing policy, select the policy name from the Create/Edit Policy menu. The current choices are WMM or Spectralink, and one of these need to be filled in the Policy Name field.
Policy Name	Enter a policy name to attach to an input or output interface. If you chose an existing policy in the Create/Edit Policy field, the policy name is filled in automatically.
Classifications	Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet. The eligible classifications for the specified policy name are supplied. Specify the fields in the frame or packet you want to use to classify incoming traffic.
Match Classifications	Specify criteria for traffic classification such as IP Precedence, DSCP, and filters.

Table 53 - QoS Policies Page Parameter Descriptions (Continued)

Parameter	Description
IP Precedence	Eight IP precedence values are defined in RFC791. Select any of them as matching criteria.
IP DSCP	IP DSCP (Differentiated Service Code Point) is defined in RFC2474. Select IP DSCP values as matching criteria.
IP Protocol 119	This protocol is for matching the SpectraLink Voice Protocol.
Apply Class of Services	Determine the class of service that the access point applies to packets that match the filter that you selected from the Filter menu. Click Add beside the Class of Service pull-down.
Filter	If you have filters set up, you can assign a priority to packets that match the selected filter. From the Filter pull-down menu, select the filter you want to include in the policy. For example, you could assign a high priority to a MAC address filter that includes the MAC addresses of IP phones. The Define Filters link take you to Services>Filters where you can configure filters. Note: The access list you use in QoS does not affect the access point's packet forwarding decisions. In other words, the access point does not allow or reject packets based on this ACL but only assign QoS policies.
Rate Limiting	Bits per Sec: 8000…2000000000 Burst Rate (Bytes): 1000…512000000 Confirm Action: Transmit Exceed Action: Drop
Apply Policies to Interface/VLANs	After QoS policies are created and applied, you can assign the policies to in-going or out-going traffic of any of the two interfaces.
Incoming	Use the pull-down menu to choose the policy you want to assign for incoming traffic to the GigabitEthernet and 802.11 radio interfaces.
Outgoing	Use the pull-down menu to choose the policy you want to assign for outgoing traffic from the GigabitEthernet and 802.11 radio interfaces.

QoS: Radio Page

This page enables you to define the parameters of Carrier Sense Multiple Access (CSMA) for each traffic access category. These parameters affect how packets are delivered for the different classes of service.

See QoS Policies Page on page 145 to determine the level of service you want.

These parameters must be modified with caution because radio behavior is affected. To revert to the default values, see Reset the WAP to Default Settings on page 49.

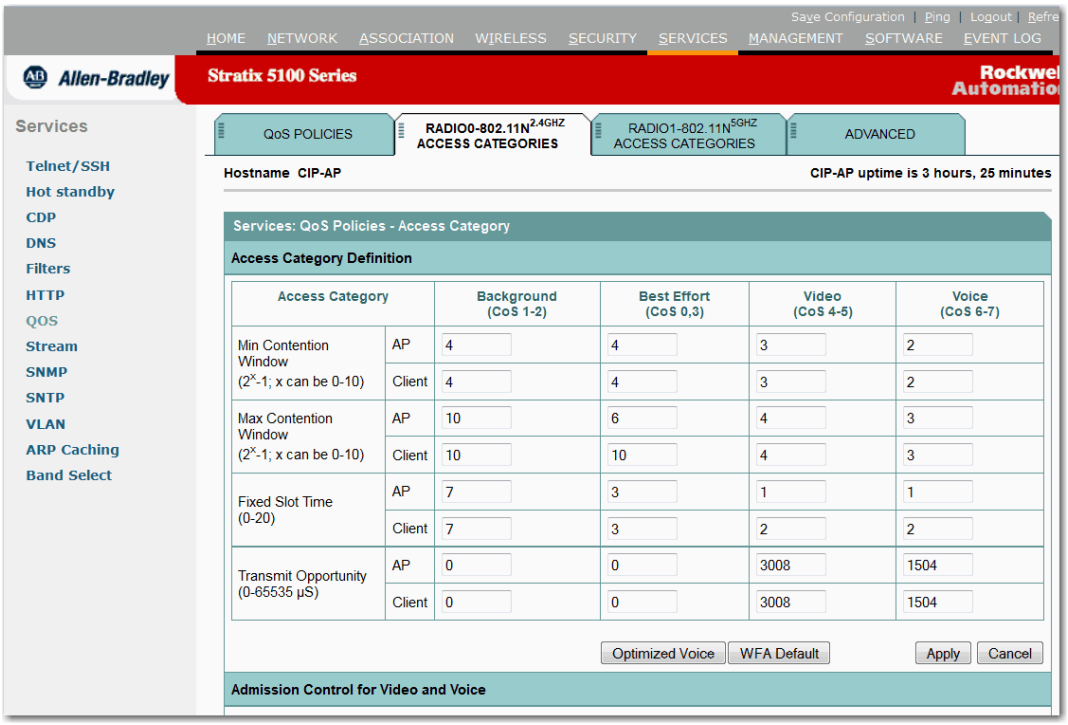


Table 54 - Access Category Definition Page Parameter Description

Parameter	Description
Min Contention	For each access category, enter the minimum contention window value. Channel access is prioritized by assigning smaller contention window values to a higher priority traffic class. If a channel is busy or a transmission collides, a node chooses a random number between 0 and the current contention window minimum.
Max Contention	For each access category, enter the maximum contention window value. The minimum contention window value is doubled each time a collision occurs until the maximum is reached. A small contention window value decreases the access delay but increases the probability of a collision.
Fixed Slot Time	For each access category, enter the fixed slot time. Channel access can be strictly prioritized by assigning smaller fixed slot values to a higher priority traffic class. Traffic in the access category must wait this fixed number of slots after each packet received before resuming its random back-off.

Table 54 - Access Category Definition Page Parameter Description (Continued)

Parameter	Description
Transmit Opportunity	Enter the number of microseconds that qualified transmitters can transmit through the normal back-off procedure with a set of pending packets. Larger values allow a client to control the channel for longer periods of time, allowing it to achieve higher throughput in this access category at the expense of longer access times for all access categories.
Admission Control	The Admission Control checkboxes control client use of the access categories. When you enable admission control for an access category, video and voice clients associated to the access point must complete the WMM admission control procedure before they can use that access category.
Optimized Voice	If you click this button, the following changes are made. • The values of Access Category Definition are changed for optimized voice. • The packet handling for user priority 5 and 6 are changed to low latency. See Services>Stream>Packet Handlings per User Priority • The Gratuitous Probe Response (GPR) is enabled on this radio. See Network Interfaces>Radio1-802.11A>Setting.
WFA Default	Click this button to return to the default values for the above fields.
Admission Control for Video and Voice	Video (CoS 4-5): Enables Admission Control Voice (CoS 6-7): Enables Admission Control
Max Channel Capacity (%)	The default max channel capacity is 75%, and the range is from 0…100%. If the channel has no calls, set this parameter to 0%. Otherwise, determine what percentage of voice calls can occupy the channel.
Roam Channel Capacity (%)	The default roam channel capacity is 6%, and the range is from 0…100%. Determine the percentage of calls that can roam into the cell or into the channel on another cell.

EDCA and QoS Enhancements

Enhanced distributed channel access (EDCA) parameters in the Stratix® 5100 access point provide preferential wireless channel access for latency and jitter sensitive traffic such as EtherNet/IP, voice and video. These parameters can be configured on the root access point and communicated to all WGBs and other wireless clients that support wireless QoS.

If a Stratix 5100 is used as a workgroup bridge in a Cisco Unified wireless network, a Wireless LAN Controller (WLC) can apply EDCA parameters to the WGB based on the defined traffic types. Starting from WLC release 8.2.110, EDCA parameters can be fully customized to match the capabilities in the Stratix 5100 access point.

Figure 60 - QOS Advanced Page

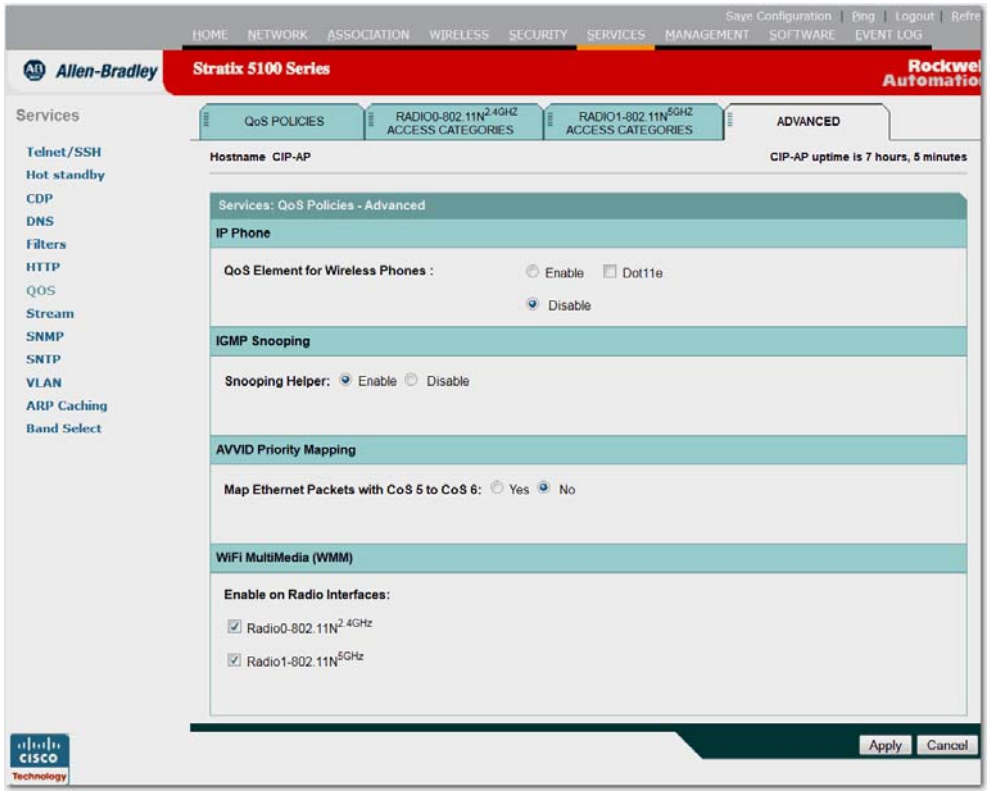


Table 55 - QoS Policies Advanced Page Parameter Description

Parameter	Description
IP Phone QoS Element for Wireless Phones	If you enable this feature, dynamic voice classifiers are created for some of the wireless phone vendor clients, that gives top priority to all voice packets. Additionally, the QoS Basic Service Set (QBSS) is enabled to advertise channel load information in the beacon and probe response frames. Some IP phones use the QBSS elements to determine the access point to associate to, based on the traffic load.
Dot11e	Click Dot11e to use the latest version of QBSS Load IE. If you do not click Dot11e, the previous QBSS Load IE version is used.
IGMP Snooping Snooping Helper	When Internet Group Membership Protocol (IGMP) snooping is enabled on a switch and a client roams from one access point to another, the client's multicast session is dropped. When the access point's IGMP snooping helper is enabled, the access point sends a general IGMP query to the network infrastructure on behalf of the client every time the client associates or reassociates to the access point. By doing so, the multicast stream is maintained for the client as it roams. The Snooping Helper is enabled by default. To disable, click the Disable selection and click Apply.
AVVID Priority Mapping	Map Ethernet Packets with CoS 5 to CoS 6 If your network is based upon Cisco AVVID specification, click Yes. This mapping prioritizes voice packets that include priority 5 (video).
WiFi MultiMedia (WMM)	Enable on Radio Interfaces Wi-Fi Multimedia (WMM) is a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS). It specifically supports priority tagging and queuing. When you enable QoS, the access point uses WMM mode by default. Uncheck the Enable on Radio Interfaces checkbox to disable WMM for a particular radio interface.

Stream Page

The Stream page sets the user priority for stream services and where you can increase or decrease data rates.

Figure 61 - Stream Page

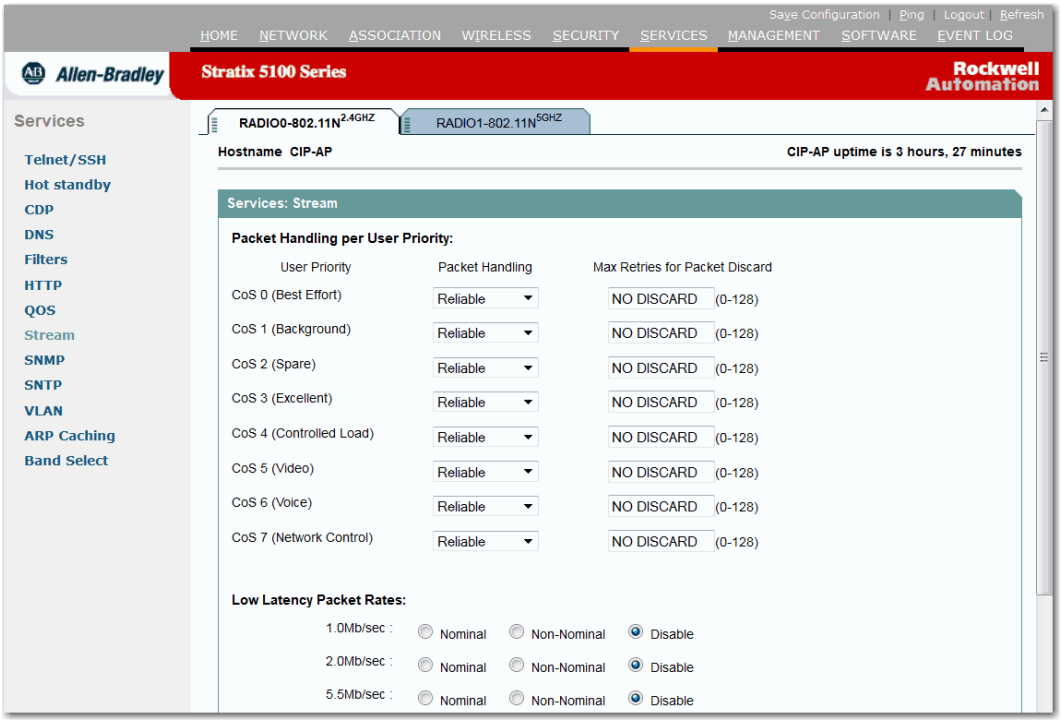


Table 56 - Stream Page Parameter Descriptions

Parameter	Description
Packet Handling per User Priority	Select the user priority to use for stream services. For each user priority listed, use the pull-down menu to choose either Reliable or Low Latency for the packet handling descriptor. Then determine the first maximum number of retries for a packet discard.
Low Latency Packet Rates	Low latency packet rates increase coverage area by decreasing data rates and increase call capacity by increasing data rates for the specified User Priorities designated.

SNMP Page

SNMP is an application-layer protocol that supports message-oriented communication between SNMP management stations and agents. This page configures the access point to work with your network administrator's Simple Network Management Protocol (SNMP) station.

In addition to enabling SNMP, you must enter an SNMP community. The SNMP community string is used like a username and is for authentication, privacy, and authorization services within SNMP. When you enter an SNMP Community name on the Express Setup page, the community associates using read-only or read/write capabilities.

Figure 62 - SNMP Page

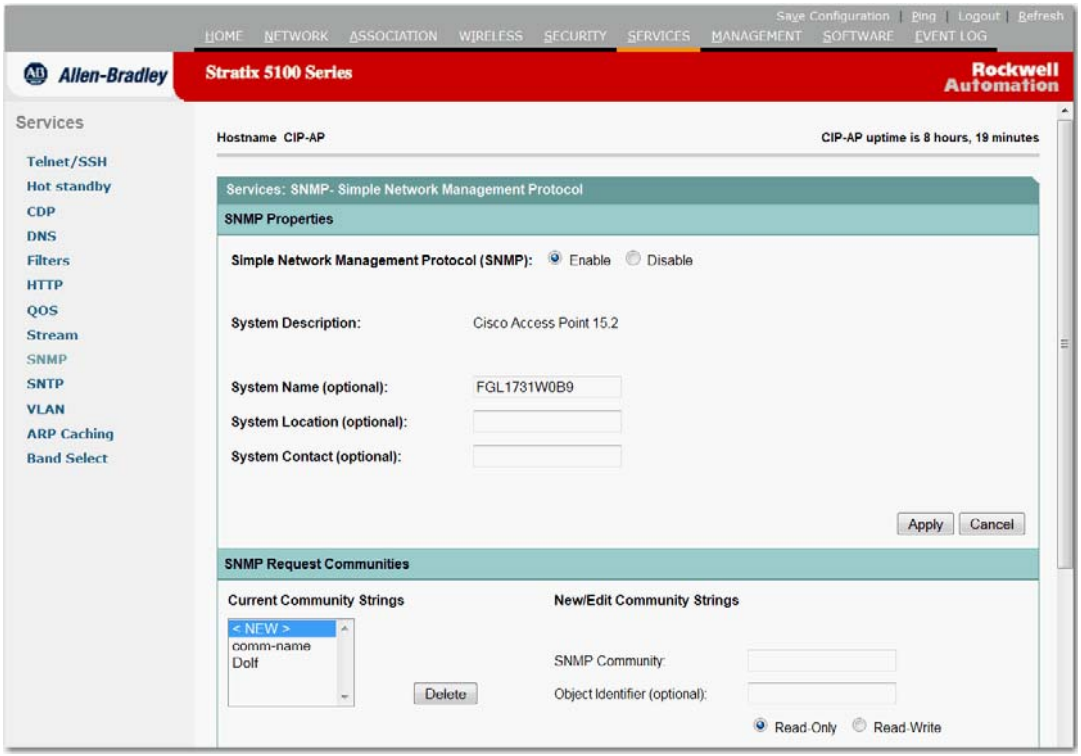


Table 57 - SNMP Page Parameter Description

Parameter	Description
Simple Network Management Protocol (SNMP)	This setting must be enabled to use SNMP with the device. In addition to enabling SNMP, you must enter an SNMP community string.
System Description	The system's device type and current version of firmware as listed at the bottom of the page.
System Name (optional)	The name of the device. The name in this field is reported to your SNMP's management station as the name of the device when you use SNMP to communicate with the device.
System Location (optional)	The physical location of the device, such as a building name or room.
System Contact (optional)	The name of the system administrator responsible for the device.

Table 57 - SNMP Page Parameter Description (Continued)

Parameter	Description
SNMP Request Communities	This section is not enabled until you select Enabled in the Simple Network Management Protocol (SNMP) field at the top of the page and click Apply.
Current Community String	If you want to add a new community string, make sure <NEW> (the default) is highlighted in the list. SNMP community strings authenticate access to MIB objects and function as embedded passwords. The currently defined community strings are displayed. You can highlight any string you want removed and click Delete.
New/Edit Community Strings	• SNMP Community After you choose a community string to edit in the Current Community Strings list, the SNMP Community value for that particular community string is displayed. SNMP community strings authenticate access to MIB objects and function as embedded passwords. • Object Identifier After you choose a community string to edit in the Current Community Strings list, the Object Identifier value for that particular community string is displayed, or you can enter a new object identifier for the community string. The object identifier is optional and limits the scope of the SNMP MIB object that the user can access through the community string.
Read-only/Read-Write	The Read-only option gives read access to authorized management stations to all objects except the community strings but does not allow write access. The Read/Write option gives read and write access to authorized management stations to all objects but does not allow access to the community string.

Figure 63 - SNMP Trap Community

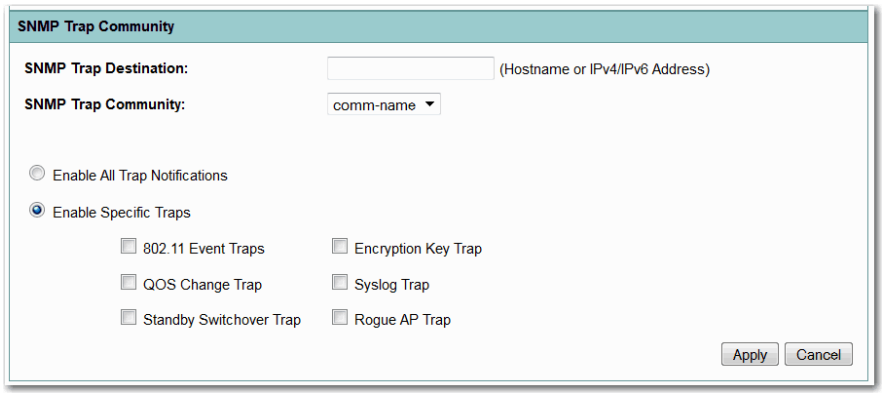


Table 58 - SNMP Trap Community Parameter Descriptions

Parameter	Description
SNMP Trap Community	This section is not enabled until you select Enabled in the Simple Network Management Protocol (SNMP) field at the top of the page and click Apply.
SNMP Trap Destination	The IP address of the SNMP management station. If your network uses DNS, enter a host name that resolves into an IP address.

Table 58 - SNMP Trap Community Parameter Descriptions (Continued)

Parameter	Description
SNMP Trap Community	The SNMP community string identifiers the sender to the trap destination. This string is required by the trap destination before it records traps sent by the device.
Enable All Trap Notifications	Select this option to enable all the notifications available on the access point.
Enable Specific Traps	Select this option to specify the notifications to be sent. • 802.11 Event Traps Enables traps for client authentication failure, client deauthentication, and client disassociation. • Encryption Key Trap Enables traps on any change in the WEP encryption key settings. • QoS Change Trap Enables traps on any change made to the 8 traffic class definitions. • Syslog Trap Enables sending of traps when event logs of a certain severity level (established by the Event Log Configuration page) occur. • Standby Switchover Trap Enables sending of traps when an access point in standby mode switches over to active mode. • Rogue AP Trap Enables sending of traps when a radio client reports a rogue access point.

SNTP Page

Simple Network Time Protocol is an adaptation of the Network Time Protocol (NTP) used to synchronize computers clocks on the Internet. In this page, you can configure NTP parameters.

Figure 64 - SNTP Page

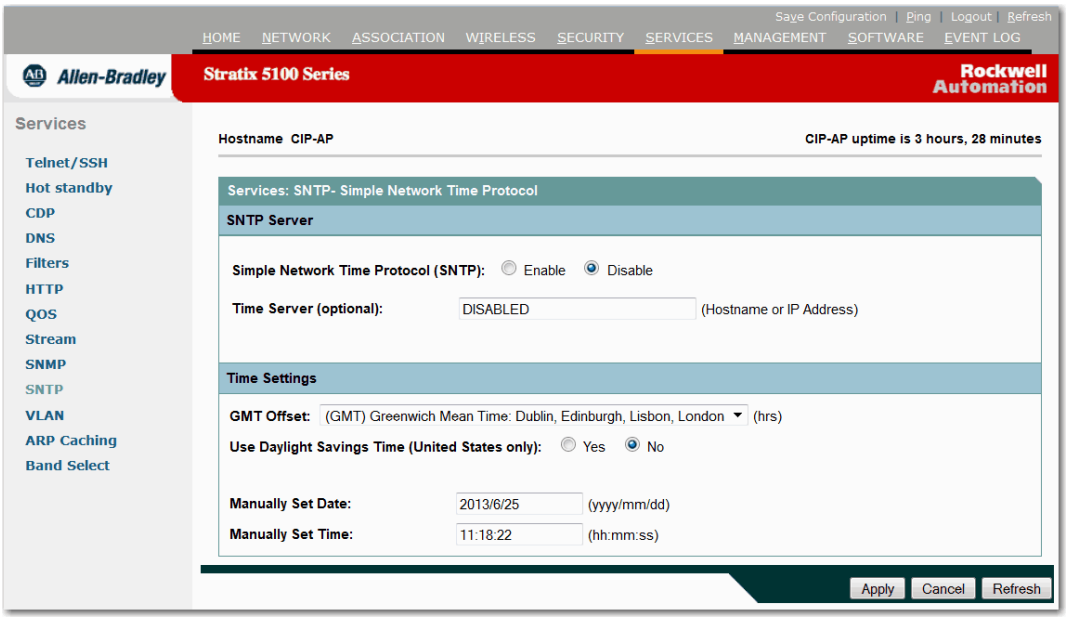


Table 59 - SNTP Page Parameter Descriptions

Parameter	Description
Simple Network Time Protocol (SNTP)	Select Enable if your network uses SNTP. If you want to turn SNTP off, select Disable. When SNTP is enabled, an SNTP Status field appears. This field indicates whether SNTP is synchronized or unsynchronized. Click Refresh to update this status.
Time Server (optional)	If your network has a default time server, enter the server's IP address or host name.
Time Settings	• GMT Offset The GMT Offset pull-down menu lists the world's time zones relative to Greenwich Mean Time (GMT). Select the time zone where the access point operates. • Use Daylight Savings Time (United States Only) Select yes to have the access point automatically adjust to Daylight Savings Time. • Manually Set Date Enter the current date to override the time server or to set the date if no server is available. When entering the date, use forward-slashes to separate the year, month, and day. For example, you can enter 2001/02/17 for February 17, 2001. • Manually Set Time Enter the current time to override the time server or to set the time if no server is available. When entering the time, use colons to separate the hours, minutes, and seconds. For example, you can enter 18:25:00 for 6:25 pm.

VLAN Page

A VLAN is a switched network that is logically segmented, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they can be intermingled with other teams. You can use software to reconfiguration the network rather than physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment; for example, LAN switches that operate bridging protocols between them with a separate group for each VLAN.

The basic wireless components of a VLAN consist of an access point and a client associated to it using wireless technology. In fundamental terms, the key to configuring an access point to connect to a specific VLAN is by configuring its SSID to recognize that VLAN. Because VLANs are identified by a VLAN ID, it follows that if the SSID on an access point is configured to recognize a specific VLAN ID, a connection to the VLAN is established. After this connection is made, associated wireless client devices having the same SSID can access the VLAN through the access point. The VLAN processes data to and from the clients the same way that it processes data to and from wired connections.

Figure 65 - VLAN Page

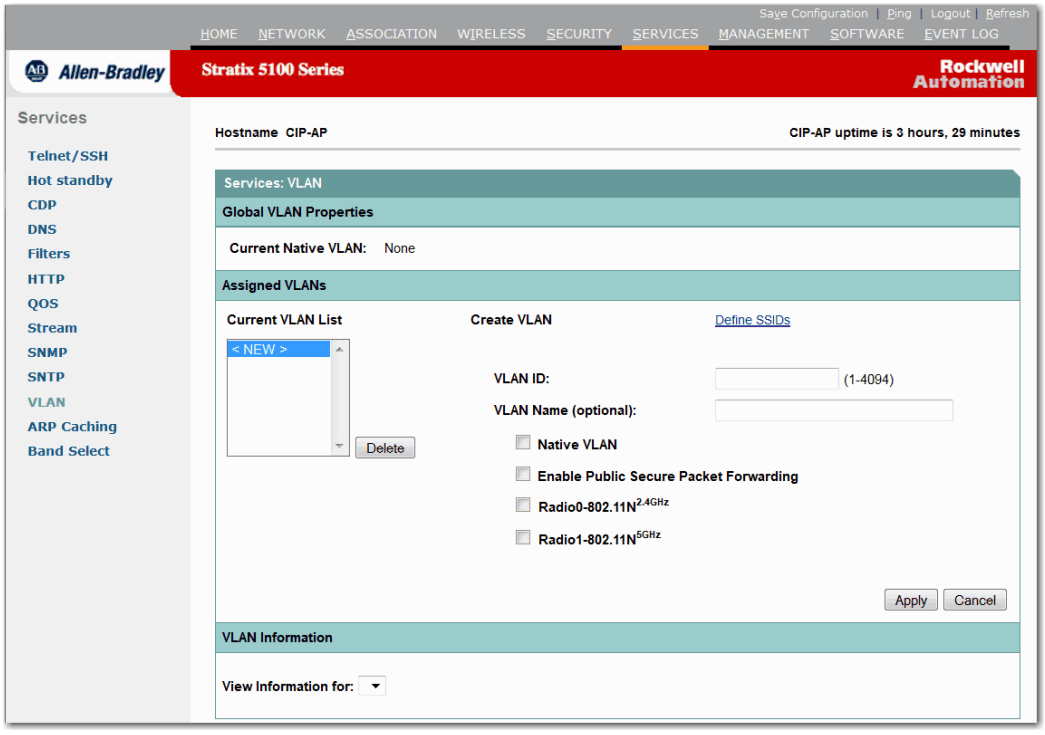


Table 60 - VLAN Page Parameter Descriptions

Parameter	Description
Global VLAN Properties	Current Native VLAN specifies the VLAN that is designated as the native VLAN. Insert here: Traffic in Native VLAN is NOT tagged with a VLAN ID in the Ethernet frame. Check the box under the VLAN ID field that denotes Native VLAN.
Assigned VLANs	Current VLAN List By choosing a VLAN from this list, the VLAN ID and SSID for this VLAN is displayed. You can then click Delete to remove the VLAN or click Define SSIDs to move to the SSID Manager page.
Create VLAN	If you are adding a VLAN, use this section to create the VLAN and assign the SSID to it.
VLAN ID	Specifies the VLAN identification number tied to the SSID. You can assign a name to a VLAN in addition to its numerical ID.
VLAN Name (optional)	You can assign a name to a VLAN in addition to its numerical ID. VLAN names can contain up to 32 ASCII characters. The access point stores each VLAN name and ID pair in a table.
Native VLAN	Untagged VLAN on an 802.1q trunked switchport.
Public Secure Packet Forwarding	Public secure packet forwarding prevents communication between clients associated to the same AP.
Radio0-802.11N 2.4 GHz	Enables VLAN on the 2.4 GHz radio interface.
Radio1-802.11N 5 GHz	Enables VLAN on the 5 GHz radio interface.
VLAN Information	Use the pull-down menu to display the list of created VLANs. After you highlight a VLAN from the list, you see the values for Ethernet packets received, Ethernet packets transmitted, radio packets received, and radio packets transmitted.

ARP Caching Page

ARP caching on the access point reduces the traffic on your wireless LAN by stopping ARP requests for client devices at the access point. Instead of forwarding ARP requests to client devices, the access point responds to requests on behalf of associated client devices.

When ARP caching is disabled, the access point forwards all ARP requests through the radio port to associated clients, and the client that the ARP request is directed responds. When ARP caching is enabled, the access point responds to ARP requests for associated clients and does not forward requests to clients. When the access point receives an ARP request for an IP address not in the cache, the access point drops the request and does not forward it.

Figure 66 - ARP Caching Page

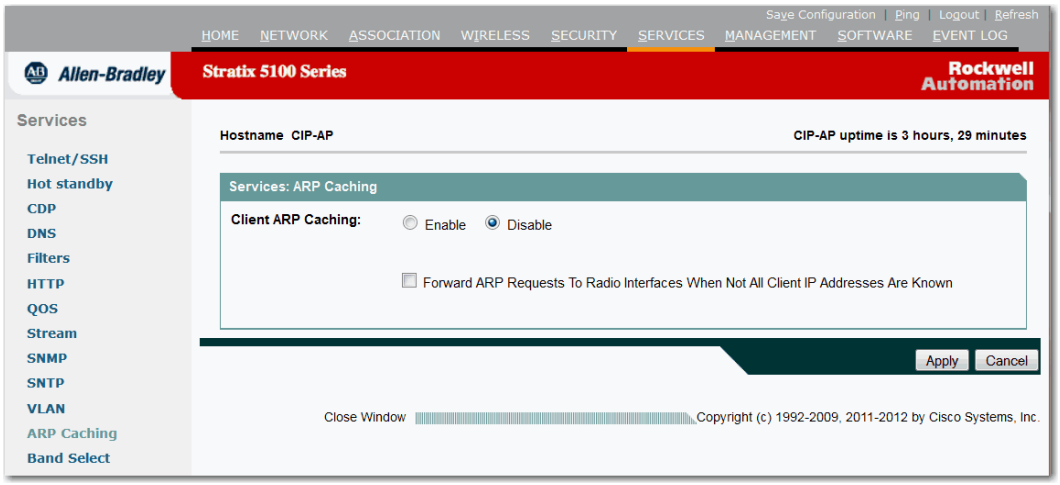


Table 61 - ARP Caching Page Parameter Descriptions

Parameter	Description
Client ARP Caching	Click the appropriate radio button to enable or disable client ARP caching.
Forward ARP Requests to Radio Interfaces When Not All Client IP Addresses Are Known	When a non-Cisco client device is associated to an access point and is not passing data, the access point can not know the client's IP address. If this situation occurs frequently on your wireless LAN, you can enable this checkbox. In this case, the access point responds on behalf of clients with IP addresses known to the access point but forwards out its radio port any ARP requests addressed to unknown clients. When the access point learns the IP addresses for all associated clients, it drops ARP requests not directed to its associated clients.

Band Select Page

Band selection encourages client radios that are capable of dual-band (2.4 and 5 GHz) operation to move to a less congested 5 GHz radio on the access point. The 2.4 GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three non-overlapping channels. To combat these sources of interference and improve overall network performance, you can configure band selection on the access point.

Band selection works by regulating probe responses to clients. It makes 5 GHz channels more attractive to clients by delaying probe responses to clients on 2.4 GHz channels.

You can enable band selection globally and for a particular SSID. This is useful if you want to disable it for a select group of clients (such as time-sensitive voice clients).

IMPORTANT Only modify these settings if you are a qualified network engineer and test the results before deploying in production. Some clients may respond differently or experience issues when Band Select is enabled.

Figure 67 - Band Select Page

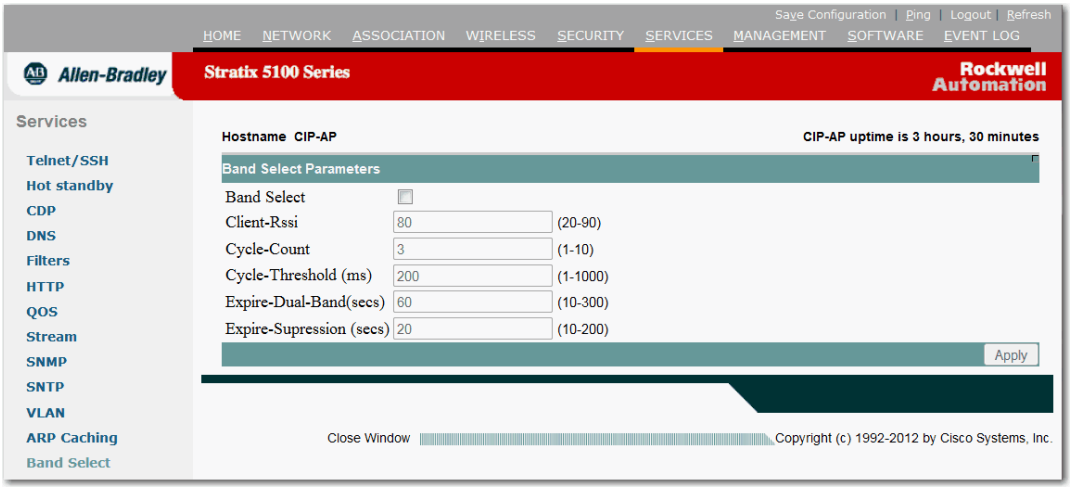


Table 62 - Band Select Page Parameter Descriptions

Parameter	Description
Band Select	Enable/Disable
Client-Rssi	20…90 The RSSI is a received signal strength indicator. It shows you the signal strength in dBm of a wireless client.
Cycle-Count	1…10 The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2

Table 62 - Band Select Page Parameter Descriptions (Continued)

Parameter	Description
Cycle-Threshold	1…1000 ms
Expire-Dual-Band	10…300 s Sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.
Expire-Suppression	10…2000 s Sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Management Page

The Management page is where you manage guest user accounts. This is where your business can create guest wireless user access by creating a web authentication page.

For example, if users want to login to a network that allows guest access, they are brought to a web page that states the Terms and Conditions of using the Wi-Fi. Once the guests accept the terms and Enter the password (if necessary) they are able to access the web.

Figure 68 - Management Page

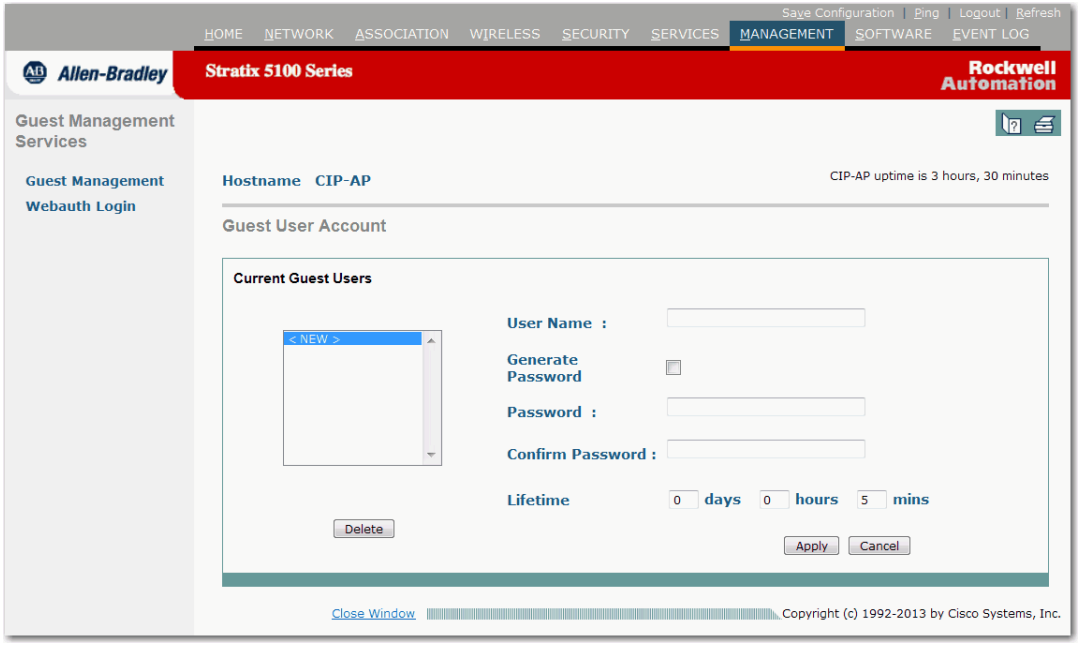


Table 63 - Management Page Parameter Descriptions

Parameter	Description
Current Guest Users	Current Guest Users
User Name	User Name
Generate Password	Generate Password
Password	Password
Confirm Password	Confirm Password
Lifetime	days/hours/minutes

Webauth Login

This page lets you customize the appearance of the Login page. The Login page is presented to web users the first time they access the Wireless Network if 'Web Authentication' is turned on SSID.

Figure 69 - Webauth Login Page

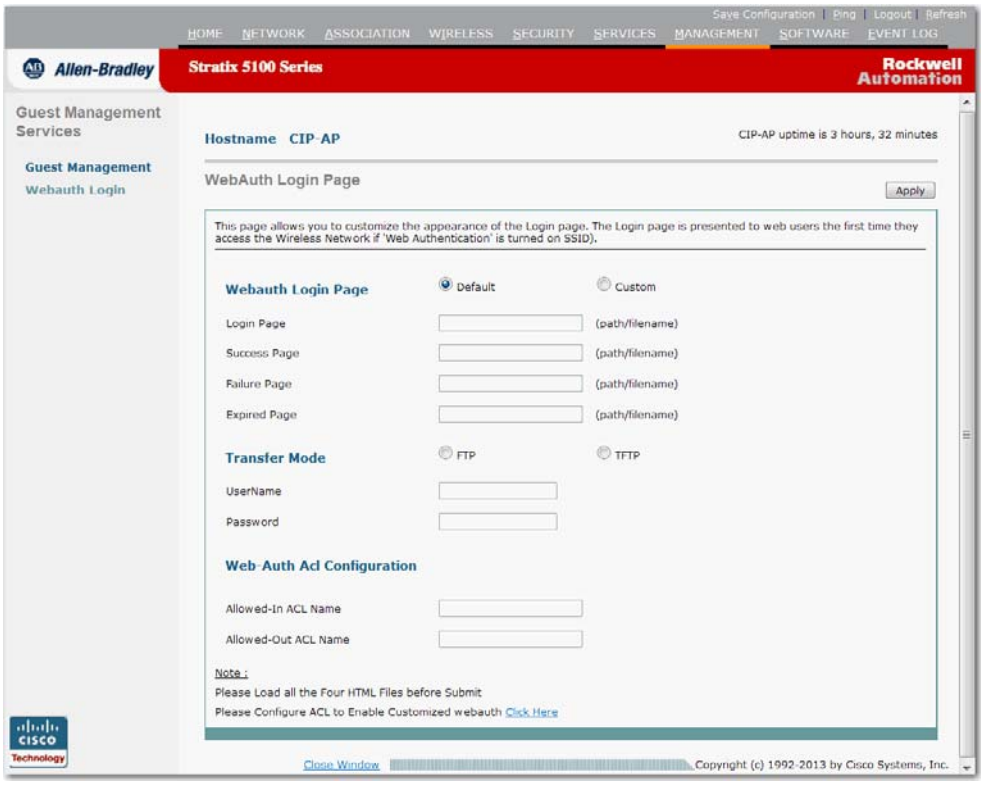


Table 64 - Webauth Login Page Parameter Descriptions

Parameter	Description
Webauth Login Page	Login Page Success Page Failure page Expired Page
Transfer Mode	FTP TFTP Username Password
Web-Auth ACL Configuration	Allowed-In ACL Name Allowed-Out ACL Name

Software Page

The Software page provides version information for the Cisco IOS software.

Figure 70 - Software Page

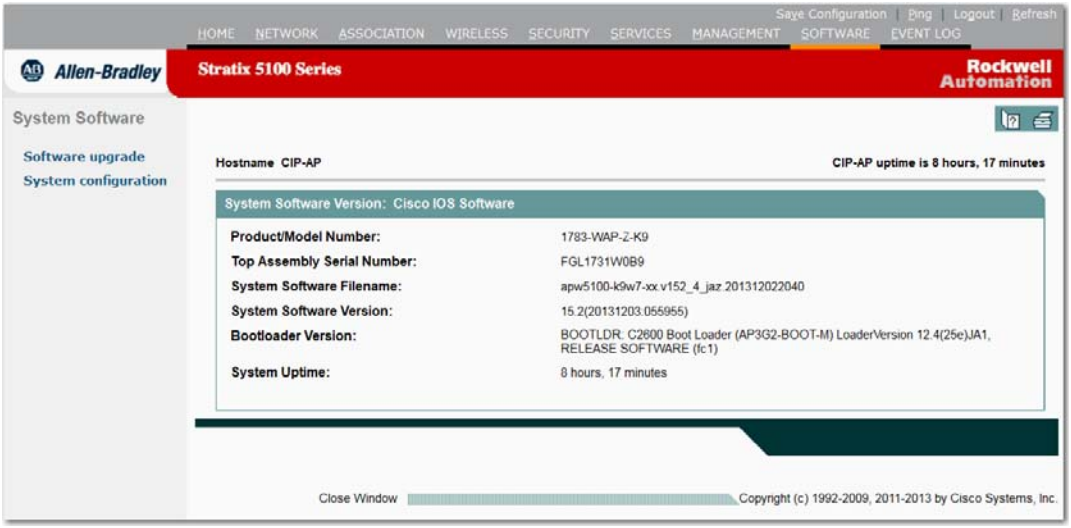


Table 65 - Software Page Parameter Descriptions

Parameter	Description
Product/Model Number	The model number of the access point.
Top Assembly Serial Number	The serial number of the access point.
System Software Filename	The software file that was installed on the system.
System Software Version	The version of Cisco IOS software that is running on the access point.
Bootloader Version	The version of bootloader that is installed. The bootloader does not change when the system image is changed.
System Uptime	The days, hours, and minutes that the access point has been powered up.

Software Upgrade HTTP Page

An HTTP upgrade requires you to load the image into the access point memory. If there is not enough system memory for an HTTP upgrade, the upgrade fails. If it fails, try using TFTP upgrade or upgrading HTTP again after disabling the radio interfaces, shutting off high memory usage features (such as WDS), and rebooting.

Figure 71 - Software Upgrade HTTP Page

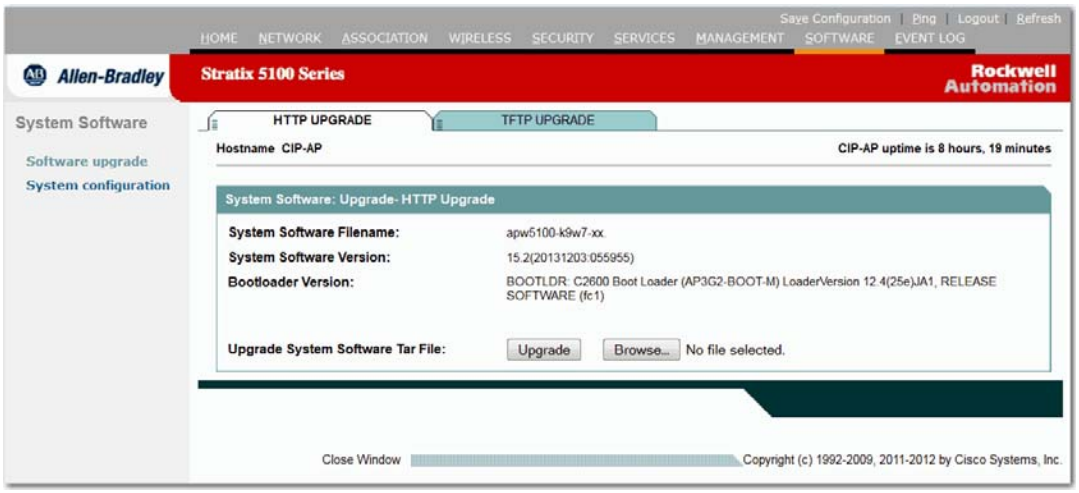


Table 66 - Software HTTP Upgrade Page Parameter Descriptions

Parameter	Description
System Software Filename	The software file that is installed on the system.
System Software Version	The version of Cisco IOS software that is running on the access point.
Bootloader Version	The version of bootloader that is installed. The bootloader does not change when the system image is changed.
Upgrade System Software Tar File	To install a newer version of Cisco IOS software, follow these steps. 1. Insert the correct path and filename of the new system software tar file. 2. Go to Cisco.com and download the newest system software version to your local drive. 3. Click Browse, locate the new system software file. 4. Click Upgrade to copy the file to the access point. Upgrades can take several minutes to complete and can cause the access point to reboot.

Software Upgrade TFTP Page

Use the Software Upgrade TFTP page to upgrade the Wireless AP via a TFTP Server. (You need to supply the TFTP server) This lets the WAP connect to the user supplied TFTP server to download a new version of software and upgrade it.

You need to enter the TFTP IP address or DNS name and then the path/ filename to the upgrade version of software that you need to install.

Figure 72 - Software Upgrade TFTP Page

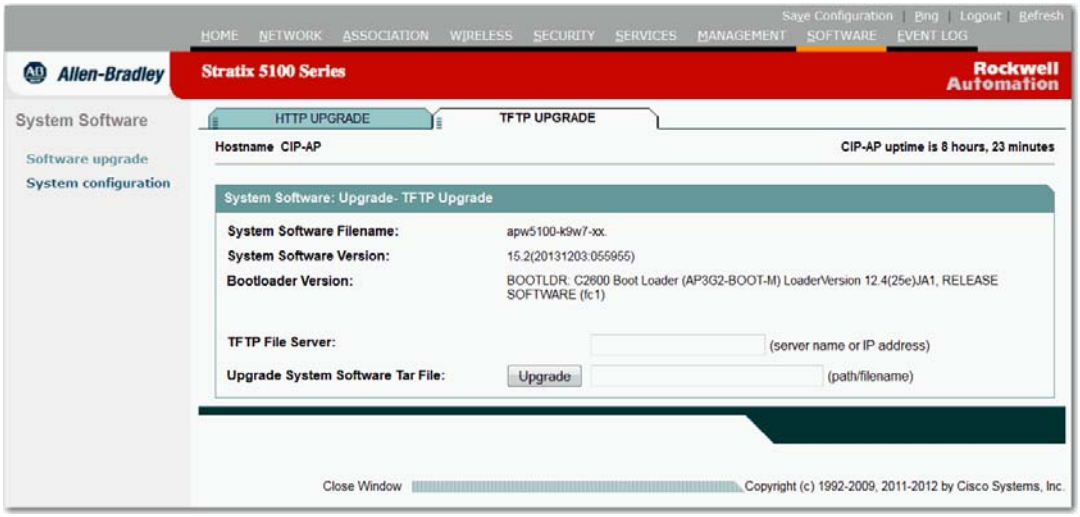


Table 67 - TFTP Upgrade Parameter Descriptions

Parameter	Description
System Software Filename	The software file that is installed on the system.
System Software Version	The version of Cisco IOS software that is running on the access point.
Bootloader Version	The version of bootloader that is installed. The bootloader does not change when the system image is changed.
TFTP File Server	This is the IP address of your TFTP Server. The TFTP is a server that makes files available.
Upgrade System Software Tar File	To install a newer version of Cisco IOS software follow these instructions. 1. Insert the correct path and filename of the new system software tar file. 2. Go to Cisco.com and download the newest system software version to your local drive. 3. Click Browse and locate the new system software file. 4. Click Upgrade to copy the file to the access point. Upgrades can take several minutes to complete and cause the access point to reboot.

System Configuration Page

This is where the system configuration information can be found. On this page, you can load new configuration files, pull your show-tech information, reset the device, and adjust PoE settings.

Figure 73 - System Configuration Page

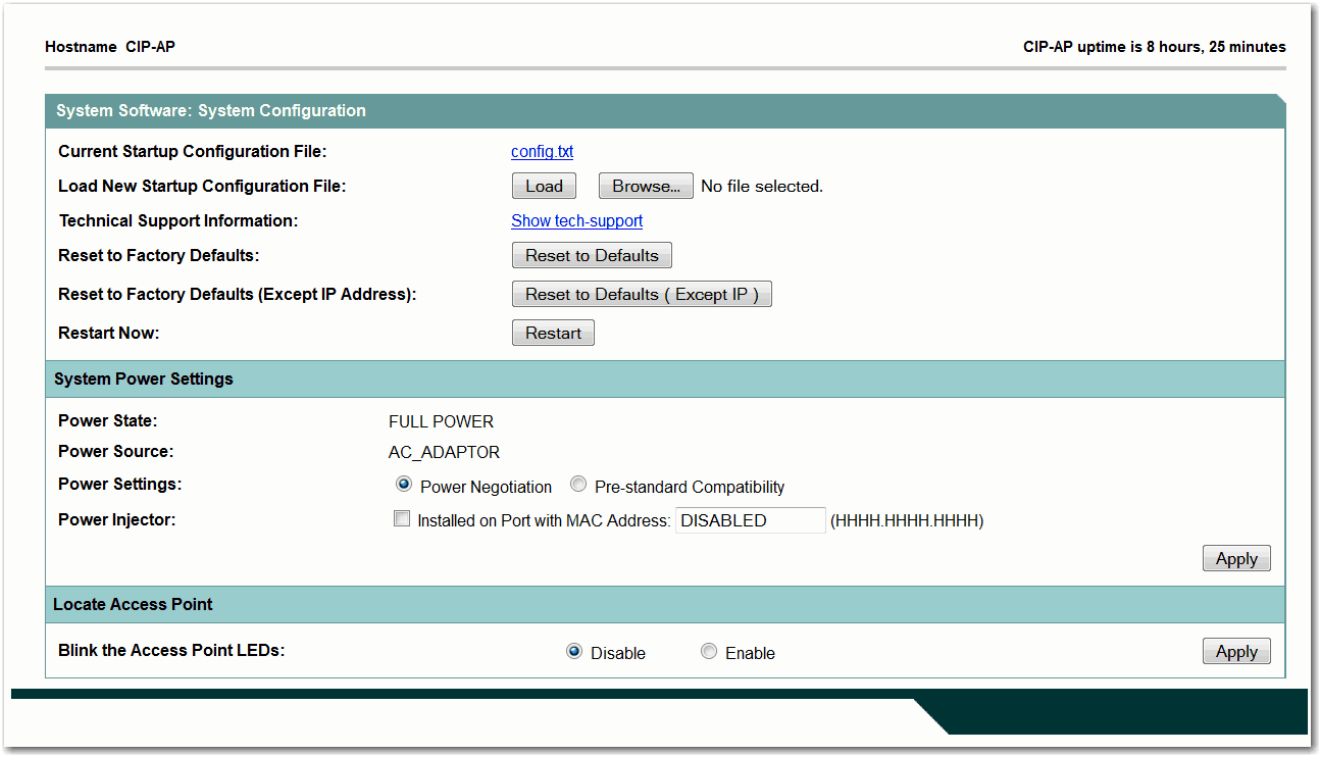


Table 68 - Software System Configuration Parameter Descriptions

Parameter	Description
Current Startup Configuration File	Right click on this link to save the config.txt file to your local hard disk. You can then edit the file and configure the access point as you wish. Use the Load New Startup Configuration File feature to upload the new file to any access point you want configured the same.
Load New Startup Configuration File	Browse to the location where you stored the config.txt file you saved using the Current Startup Configuration File feature. Click Load to upload the new file to any access point you want configured the same. The access point reboots when the new configuration is loaded.
Technical Support Information	The `show-tech` command that pulls a great deal of system information that is very helpful in determining what is wrong with a product. Your technical support staff requests this information to begin troubleshooting the device. Right click on this link to save the tech-support information to your local hard disk. You can then e-mail this information to your technical support staff to assist them in configuring your access point.
Reset to Factory Defaults	Returns all access point settings to their factory defaults. The IP address is set to DHCP. Click Reset to Defaults to cause the access point to restart. The default password for the access point is wirelessap.

Table 68 - Software System Configuration Parameter Descriptions (Continued)

Parameter	Description
Reset to Factory Defaults (Except IP Address)	Returns all access point settings to their defaults, except for a fixed IP address that remains the same if it is configured. Click Reset to Defaults (Except IP) to cause the access point to restart. The default password for the access point is wirelessap.
Restart Now	Click Restart to restart the system without having to find the access point and unplug it. A restart cold boot is needed only after recovering from network problems caused by power outages or lightning storms.
System Power Settings	This section displays current power status and settings, and allows configuring settings for power injectors and pre-standard Power over Ethernet (PoE) equipment. Identify your power source and switch condition and then make sure that your devices are configured.
Power State	Displays the power mode of the access point. A Warning condition indicates that the PSE is unable to provide sufficient power, or that the power injector has not been configured properly. See System Power Settings for instructions on how to correct this.
Power Source	Displays the power source as detected by the access point.
Power Settings	Select either Power Negotiation or Pre-standard Compatibility. Use the power negotiation setting to let a device negotiate inline power with a PSE that supports Cisco Intelligent Power Management. or when using a Cisco Aironet Power Injector. If you are using a non-Cisco switch, changes to the power settings are not required.
Power Injector	When a power injector is connected in front of a Cisco PSE that does not support Cisco Intelligent Power Management, the Installed on Port with MAC Address checkbox must be chosen. Ensure the MAC address for your switch port is displayed in the MAC address field. If your Cisco switch supports Intelligent Power Management negotiations, uncheck Installed on Port with MAC Address.
Locate Access Point	Blink the Access Point status indicators. Click Enable to make the status indicators on the access point blink so that you can locate a specific device.

Event Log Page

This is the page where you can view the Event log. In CLI, this command is `show logging`.

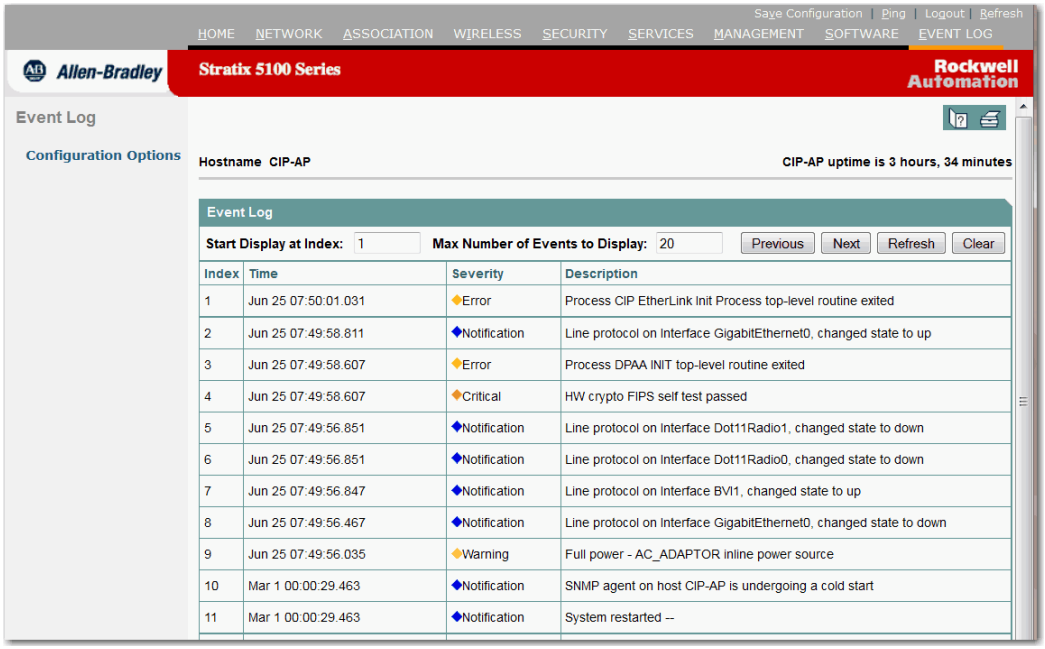


Table 69 - Event Log Page Parameter Descriptions

Parameter	Description
Start Display at Index	Enter the event where you want the event log to begin.
Max Number of Events to Display	Enter the number of events you want displayed on the event log.
Index	Sequentially numbers the events in the event log from the oldest to the newest.

Table 69 - Event Log Page Parameter Descriptions (Continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Time</td><td>Displays the time stamp that was recorded with the event. The displayed format is chosen on the Event Log: Configuration Options page. The time stamp format displayed is dependent on the time stamp format that was selected at the time the event occurred. Three time stamp formats are supported.
System Uptime
The length of time the system was operational when the event occurred. Initially, the length of time is displayed as number of seconds, increasing to minutes, days, and weeks. For example, 1w0d represents one week and zero days.
Global Standard Time
The time of day the event occurred in UTC time. This time is recorded as Month dd hh:mm:ss.usec and the three-letter time zone (UTC). The system clock must be set for this time stamp to work.
Local Time
The time of day the event occurred in the local time zone. This time is recorded as Month DD hh:mm:ss:usec and three-letter time zone. The system clock must be set for this time stamp to work.</td></tr>
<tr><td>Severity</td><td>This table lists the severity of events.<table><tr><th>Severity</th><th>Description</th></tr><tr><td>Emergency (level 0 severity)</td><td>The system is unusable</td></tr><tr><td>Alert (level 1 severity)</td><td>An immediate action is required.</td></tr><tr><td>Critical (level 2 severity)</td><td>The conditions are critical.</td></tr><tr><td>Error (level 3 severity)</td><td>Error conditions are recorded.</td></tr><tr><td>Warning (level 4 severity)</td><td>A warning message indicates a potential error condition.</td></tr><tr><td>Notification (level 5 severity)</td><td>Normal operation is occurring but significant conditions could result.</td></tr><tr><td>Informational (level 6 severity)</td><td>An Information message provides routine information on normal activity and does not indicate an error.</td></tr><tr><td>Debugging (level 7 severity)</td><td>Debugging messages are provided.</td></tr></table></td></tr>
<tr><td>Description</td><td>Gives a description of the error event.</td></tr>
</table>

For more information about error messages, see Error and Event Messages on page 519.

Configuration Options Page

These settings let you decide how you want to be notified of the different events that are logged and the level of logging that is to take place.

Figure 74 - Configuration Options Page

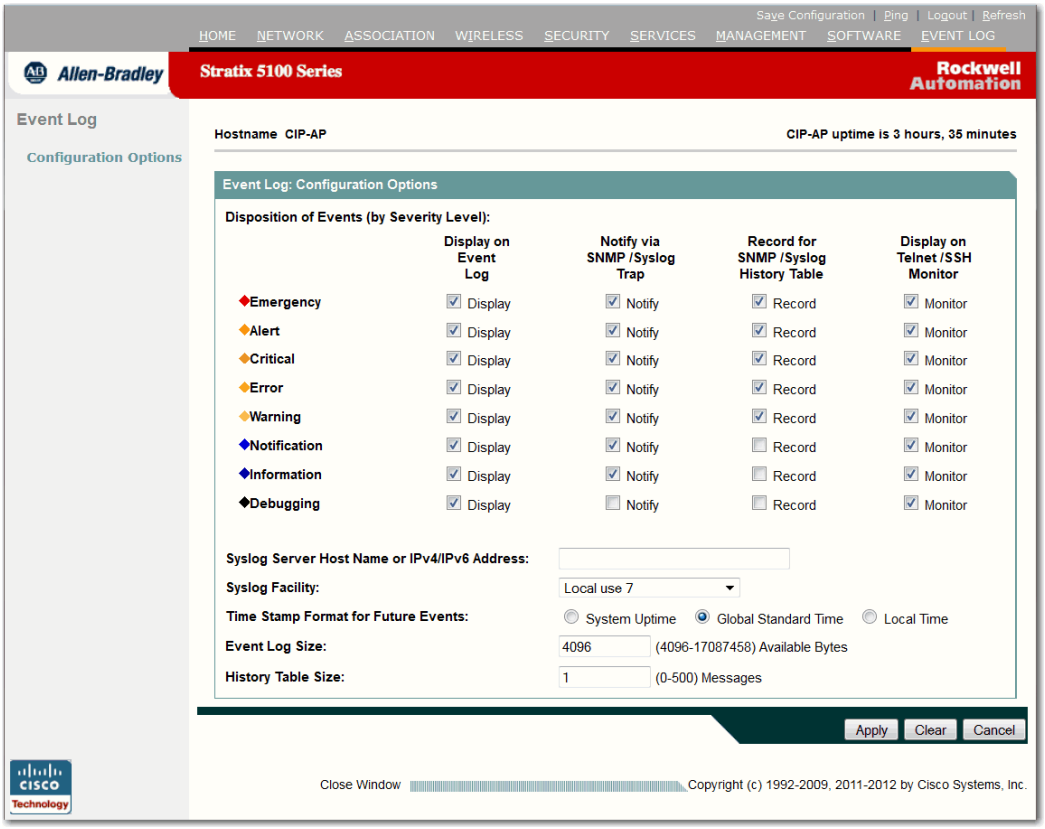


Table 70 - Event Log Configuration Parameter Descriptions

Parameter	Description
Disposition of Events (by Severity Level)	When a severity level is selected, all higher-priority severity levels are also selected.
Display on Event Log	Determine for each severity level whether you want the event displayed on the event log by placing a check mark in the checkbox. Events displayed on the event log are available on the event log page.
Notify via SNMP/Syslog Trap	Determine for each severity level whether you want to be notified by an SNMP/Syslog trap when the event occurs. The notification occurs when a check mark appears in the checkbox.
Record for SNMP/Syslog History Table	Determine for each severity level whether you want to record the event in the SNMP/Syslog history table. The event is recorded when a check mark appears in the checkbox.
Display on Telnet/SSH Monitor	Determine for each severity level whether you want to display the event on the Telnet/SSH monitor. The event displays on the monitor when a check mark appears in the checkbox.

Table 70 - Event Log Configuration Parameter Descriptions (Continued)

Parameter	Description
Time Stamp Format for Future Events	Choose the time format that you want the event time stamp information saved. The three supported time stamp formats are as follows. • System Uptime The length of time the system was operational when the event occurred. Initially, this time is displayed as number of seconds, growing to minutes, days, and weeks. For example, 1w0d represents one week and zero days. • Global Standard Time The time of day the event occurred in UTC time recorded as Month dd hh:mm:ss.usec and 3-letter time zone (UTC). The system clock must be set for this time stamp to work. • Local Time The time of day the event occurred in the local time zone recorded as Month DD hh:mm:ss.usec and 3-letter time zone. The system clock must be set for this time stamp to work.
Event Log Size	Determine the size of the buffer you want established for logging commands. The more memory you assign to the log, the less memory that is available to switch packets.
History Table Size	Determine the maximum number of syslog messages that you want stored in the access point's history table.

Access the Stratix 5100 Wireless Access Point/ Workgroup Bridge in Logix Designer

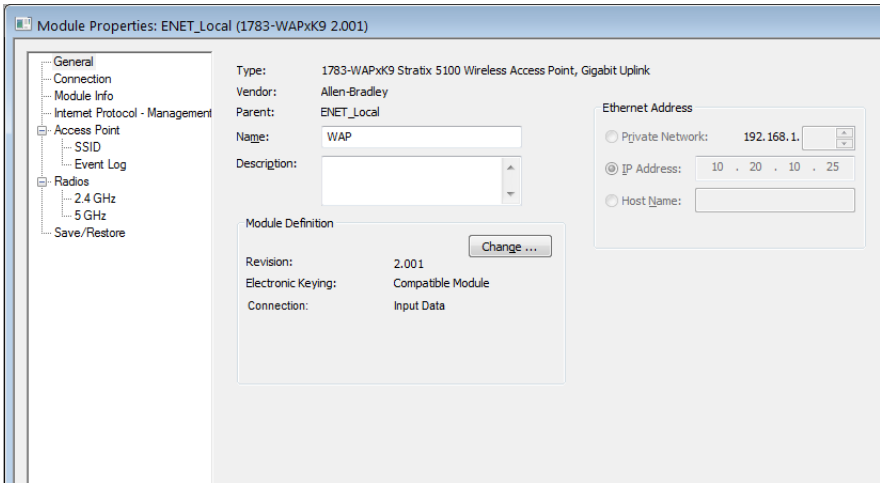
This chapter provides information about the basic access point/workgroup bridge parameters that you can configure and review status information in the Studio 5000 Logix Designer® application.

Topic	Page
General Dialog Box	172
Connection Dialog Box	174
Module Information Dialog Box	175
Internet Protocol Configuration Dialog Box	177
Access Point Dialog Box	180
Service Set Identifiers (SSID) Dialog Box	181
Event Log Dialog Box	182
Radios Dialog Box	183
2.4 GHz or 5 GHz Radio Dialog Box	184
Save/Restore Dialog Box	190

General Dialog Box

The General dialog box provides information such as the name, Ethernet address, and the revision.

Figure 75 - General Dialog Box



The General dialog box includes the following parameters.

Table 71 - General Parameter Descriptions

Parameter	Description
Type	Displays the type and description of the module being created (read only).
Vendor	Displays the vendor of the module being created (read only).
Parent	Displays the name of the parent module (read only). If the module is in the local chassis, displays `Local'.
Name	Enter the name of the module. The name must be IEC 1131-3 compliant. This is a required field and must be completed; otherwise, you receive an error message when you exit this dialog box. An error message is displayed if a duplicate name is detected or you enter an invalid character. If you exceed the maximum name length allowed by the software, the extra character(s) are ignored.
Description	Enter a description for the module up to 128 characters. Use any printable character in this field. If you exceed the maximum length, the software ignores any extra character(s).

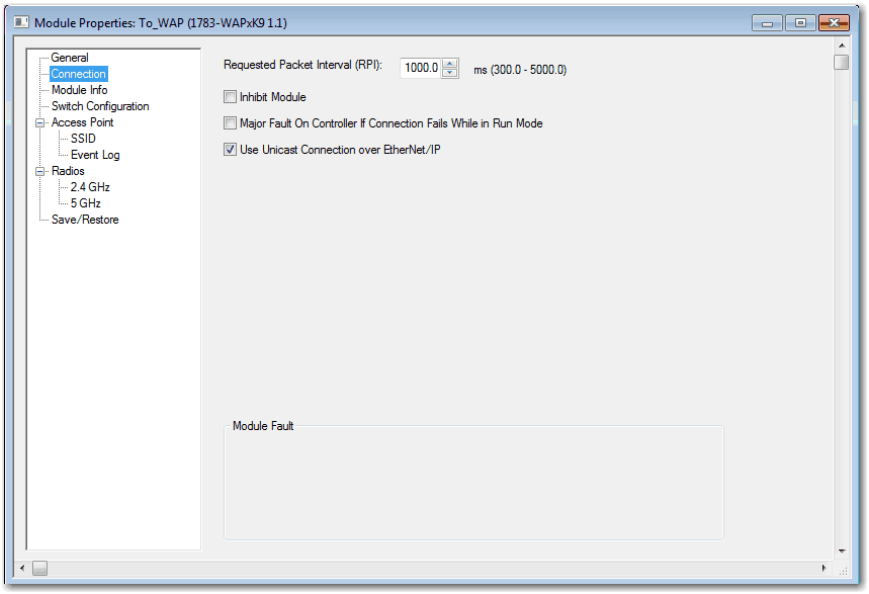
Table 71 - General Parameter Descriptions (Continued)

Parameter	Description
Ethernet Address	Enter a unique IP address to identify the module on the network. The IP address identifies each node on the IP network (or system of connected networks). Each TCP/IP node on a network must have a unique IP address. The IP address is a 32-bit identification number for each node on an Internet Protocol network. These addresses are represented as four sets of 8-bit numbers (numbers from 0 . . . 255), with decimals between them. The IP address has a net ID part and a host ID part. Networks are classified as A, B, C, or other. The class of the network determines how an IP address is formatted. You distinguish the class of the IP address from the first integer in its dotted-decimal IP address. • Each node on the same physical network must have an IP address of the same class and must have the same net ID. • Each node on the same network must have a different Host ID thus, giving it a unique IP address. The first octet of the IP Address cannot be 127, or a number greater than 223. If any of these values are entered and you attempt to download this configuration using the Set button, an error message is displayed, and no values are sent to the module. For example, the 32-bit IP address: 00000011 00000000 00000000 00000001 is written as 3.0.0.1. Distinguish the class of an IP address from the first integer in its dotted-decimal IP address as follows: **Range of First Integer** **Class** 0...127 A 128...191 B 192...223 C 224...255 Other Contact your network administrator or the Network Information Center for a unique IP address to assign to your module. The IP address cannot be changed when online.
Electronic Keying	Select one of these keying options for your module during initial module configuration. **Exact Match** All the parameters described below must match or the inserted module will reject the connection. **Compatible Module** The following criteria must be met, or else the inserted module will reject the connection: The Module Types, Catalog Number, and Major Revision must match. The Minor Revision of the physical module must be equal to or greater than the one specified in the software. **Disable Keying** The controller does not employ keying at all. Changing the RPI and Electronic Keying selections can cause the connection to the module to be broken and can result in a loss of data.  **WARNING:** Be extremely cautious when using this option; if used incorrectly, this option can lead to personal injury or death, property damage or economic loss.
Connection	You have the option to change the module definition at any time without deleting the existing module and creating a new module. The profile will attempt to bring forward all configuration data for the new settings. Any configuration data that cannot be brought forward will be set to a default value. Once the new settings are applied, these settings become the base configuration and all previous Data Format configurations are lost. Note that with the Combo module, a System Issue exists that needs to be resolved before Input is implemented. The Input connection will need to generate a partial Configuration data type to just configure inputs. **Input** Input and Configuration data types and tags are generated. If this connection is established, it owns the Configuration; it shares the Input. **Output** Input, Output, and Configuration data types and tags are generated. If this connection is established, it owns the Configuration and Output; it shares the Input.

Connection Dialog Box

In the Connection dialog box, you can at which data updates over a connection, inhibit or uninhibit your connection to the module.

Figure 76 - Connection Dialog Box



The Connection dialog box includes the following parameters.

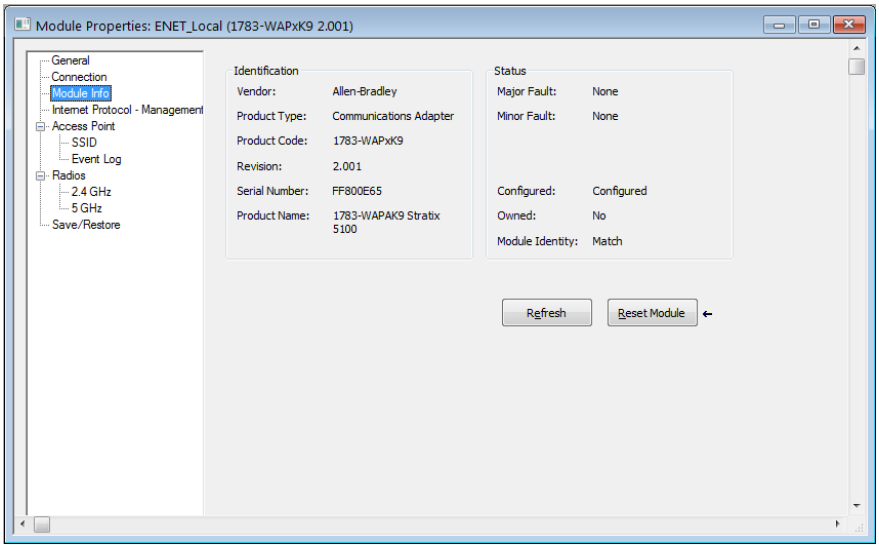
Table 72 - Connection Parameter Descriptions

Parameter	Description
Requested Packet Interval (RPI)	The Requested Packet Interval (RPI) setting determines the period (in ms) at which data updates over a connection. The RPI control appears dimmed because each controller can have its own individual RPI setting.
Inhibit Module	**Inhibit Module** Inhibit or uninhibit your connection to the module. Inhibiting the module causes the connection to the module to be broken. Inhibiting the module causes the connection to the module to be broken and can result in loss of data.
Major Fault	Failure of the connection to this module causes a major fault on the controller if the connection for the module fails.
Use Unicast	Enabled when the module supports Unicast at the current revision, and any part of the module path crosses EtherNet/IP.
Module Fault	Connection Request Error - The controller is attempting to make a connection to the module and has received an error. The connection was not made. Service Request Error - The controller is attempting to request a service from the module and has received an error. The service was not performed successfully. Module Configuration Invalid - The configuration in the module is invalid. (This error is commonly caused by the Electronic Key Passed fault.) Electronic Keying Mismatch - Electronic Keying is enabled and some part of the keying information differs between the software and the module.

Module Information Dialog Box

In the Module Information dialog box, you can view status and reset the access point.

Figure 77 - Module Information Dialog Box



The Module Information dialog box includes the following parameters.

Table 73 - Module Information Parameter Descriptions

Item	Description
Type	Displays the type and description of the module being created (read only).
Identification	Displays the module's: • Vendor • Product type • Product Code • Revision • Serial number • Product name
Revision	Select the minor revision number of your module. To change the Revision, click the Change button to access the Module Definition dialog. The revision is divided into the major revision and minor revision. The major revision is displayed statically on this dialog; you edit this value from the Select Module Type dialog. The major revision is used to indicate the revision of the interface to the module. The minor revision is used to indicate the firmware revision.
Change...	Click this button to access the Module Definition dialog, from which you change the values that define the module definition, Electronic Keying, and minor revision.
Faults	Status of major and minor faults
Configured	Indicates whether the module has been configured.
Owned	Displays whether a controller is currently connected to the module.

Table 73 - Module Information Parameter Descriptions (Continued)

Item	Description
Match	This agrees with what is specified on the General Tab. In order for the Match condition to exist, all of the following must agree: • Vendor • Module Type (the combination of Product Type and Product Code for a particular Vendor) • Major Revision Mismatch does not agree with what is specified on the General Tab.
Refresh	Refreshes the dialog box with new data from the module.
Reset Module	Returns a module to its power-up state by emulating the cycling of power.  **WARNING:** Resetting a module causes all connections to or through the module to be closed, and this may result in loss of control.

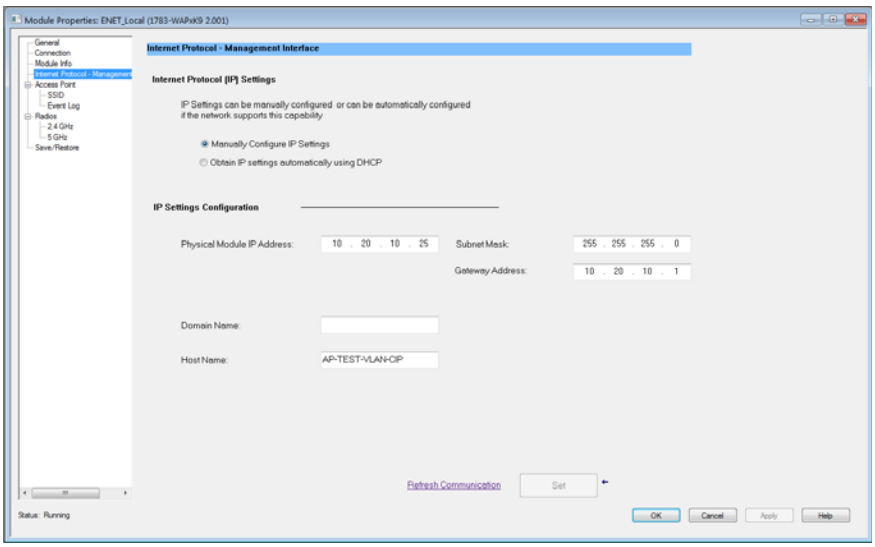
Internet Protocol Configuration Dialog Box

In the Switch Configuration dialog box, you can configure the access point. Parameters that you can configure include, for example, the IP address, Server address, and the Host name.

The IP address can be manually assigned (static) or it can be automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static.

We recommend that you select Static and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the switch.

Figure 78 - Internet Protocol Dialog Box



The Switch Configuration dialog box includes these.

Table 74 - Switch Configuration Parameter Descriptions

Item	Description
Static	The IP address, subnet mask, and gateway are manually entered for the access point/workgroup bridge. Static is the default.
DHCP	The access point automatically obtains an IP address, default gateway, and subnet mask from the DHCP server. As long as the access point is not restarted, it continues to use the assigned IP information.
IP Address	Enter an IP address for the access point. The IP address is a 32-bit identification number for the switch. It is represented as 4 octets with periods between them (xxx.xxx.xxx.xxx). Set each octet between 0…255. This value must match the IP address you entered in the Device Manager during Express Setup as well as the address on the General tab. If you reconfigure your switch with a different IP address, you can lose communications with the switch when you click Set. To correct this, you must go back to the Express Setup and General tab, set the new IP address, and download to the controller. The IP address should not be lower than 0.1.0.0 or between 224.0.0.0 through 255.255.255.255. Contact your network administrator or the Network Information Center for a unique IP address to assign to your access point.
Subnet Mask	Enter the appropriate subnet mask for the access point. The subnet mask is a 32-bit number. Set each octet between 0…255. The default is 255.255.255.0 The value must match the subnet mask you entered in the Device Manager during Express Setup.
Gateway Address	(Optional) Enter the IP address of the gateway. A gateway is a router or other network device through which the access point communicates with devices on other networks or subnetworks. The gateway IP address should be part of the same subnet as the access point IP address. The access point IP address and the default gateway IP address cannot be the same.
Primary DNS Server Address	Enter the address of the primary Domain Name System (DNS) server. Set each octet between 0…255. The first octet cannot be 127, or a number greater than 223.
Secondary DNS Server Address	(Optional) Enter the IP address of the gateway. A gateway is a router or other network device through which the switch communicates with devices on other networks or subnetworks. The gateway IP address should be part of the same subnet as the access point IP address. The access point IP address and the default gateway IP address cannot be the same.
Domain Name	Enter the name of the domain in which the module resides. The domain name consists of a sequence of name labels separated by periods, for example rockwellautomation.com. The domain name has a 48-character limit and is restricted to ASCII letters a… z, digits 0…9, and periods and hyphens.
Host Name	Enter a unique host name for your computer. The host name is the unique name for a computer within its domain. It is always the first element of a full name and, with its domain and top-level domain suffix, creates the unique name of that computer on the Internet. For example, if a trading website is www.trading.com, the host name is www, which is not unique on the web, but is unique within the trading domain. The host name also refers to the Fully Qualified Domain Name (FQDN), or in this example, www.trading.com. Both naming methods are generally used interchangeably.

Table 74 - Switch Configuration Parameter Descriptions (Continued)

Item	Description
Contact	Enter contact information for the access point, up to 200 characters. This feature is optional. The contact information can include alphanumeric characters, special characters, and carriage returns.
Geographic Location	Enter a geographic location of the access point, up to 200 characters. This feature is optional. The geographic location can include alphanumeric characters, special characters, and carriage returns.
Refresh Communication	Click refresh the dialog box with new data from the module. The Refresh button is not available in offline mode.

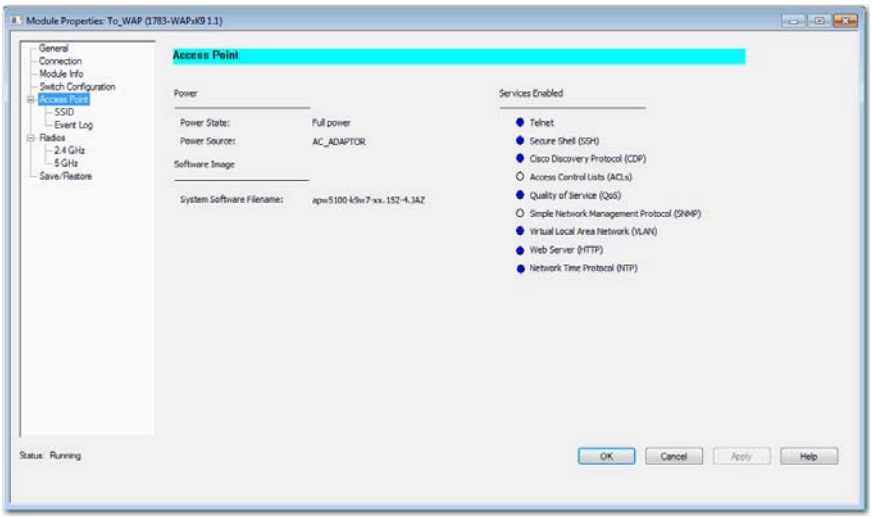
Access Point Dialog Box

Use this dialog box to view information about the wireless access point. You can view the following on the Access Point dialog box.

- Power mode of the access point.
- Power source detected by the access point.
- Services that are enabled in the access point.
- Filename and version of the firmware uploaded to switch.

The data is only displayed when the module is online.

Figure 79 - Access Point Dialog Box



Access Point Parameters

The Access Point dialog box includes these parameters.

Table 75 - Access Point Parameter Descriptions

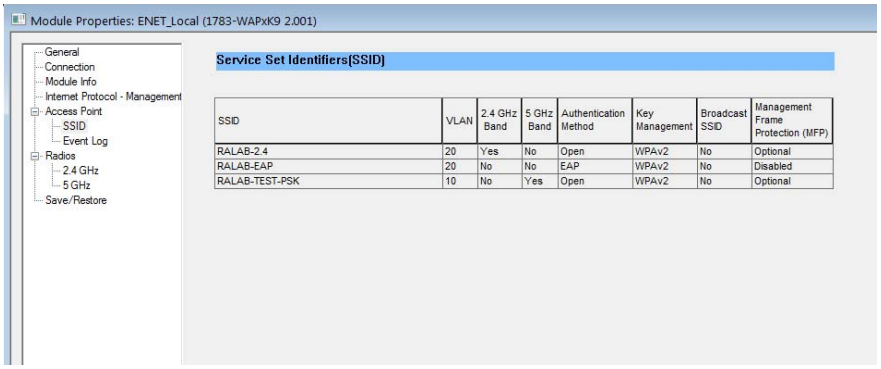
Parameter	Description
Power State	The power mode of the access point. Full Power, Insufficient Power
Power Source	The power source as detected by the access point. AC Adapter Power over Ethernet (PoE)
System Software Filename	The filename of the firmware uploaded in the switch.
Services Enabled	Main services that are currently enabled or disabled. A service is enabled when the indicator is blue. • Telnet • Secure Shell (SSH) • Cisco Discovery Protocol (CDP) • Access Control Lists (ACLs) • Quality of Service (QoS) • Simple Network Management Protocol (SNMP) • Virtual Local Area Network (VLAN) • Web Server (HTTP • Network Protocol (NTP)

Service Set Identifiers (SSID) Dialog Box

Use this dialog box to show information about the SSIDs. You can view the following on the SSID dialog box.

- SSIDs associated with the radio
- VLAN associated with the SSID
- Authentication method used on the SSID
- Encryption mode for the SSID VLAN
- Whether the access point is broadcasting the SSID
- Management Frame Protection used for the SSID The data is only displayed when the module is online.

Figure 80 - Service Set Identifiers (SSID) Dialog Box



The Service Set Identifiers (SSID) dialog box includes the following parameters.

Table 76 - Service Set Identifiers (SSID) Parameter Descriptions

Parameter	Description
SSID	Unique identifier used to associate with the radio.
VLAN	The VLAN associated with the SSID.
2.4GHz Band	Indicates whether the 2.4 GHz band is enabled for the SSID.
5GHz Band	Indicates whether the 5 GHz band is enabled for the SSID.
Authentication Method	The authentication method that the SSID uses to authenticate to the network. This includes Open, Shared, and EAP
Key Management	The key management method for the SSID's VLAN. • WPA • WPAv1 • WPAv2
Broadcast SSID	Indicates whether the SSID is broadcast.
Management Frame Protection (MFP)	The management frame protection setting for the SSID. • Disabled • Optional • Required

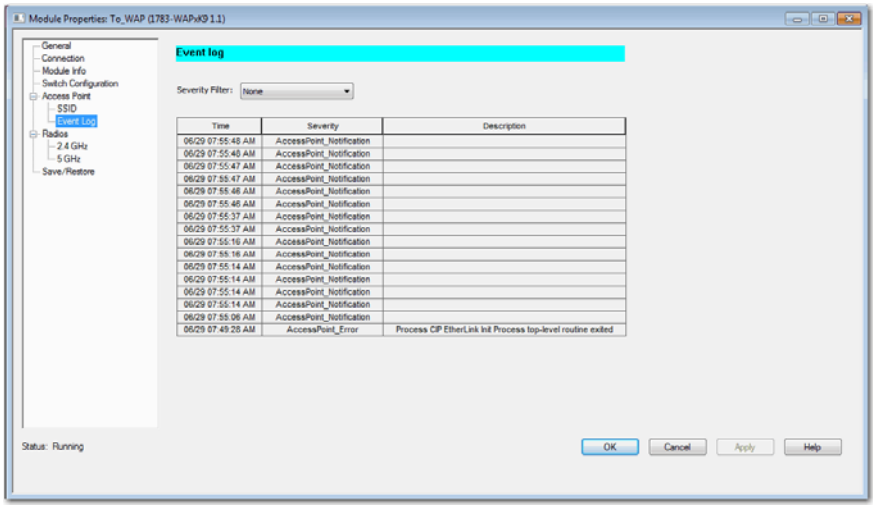
Event Log Dialog Box

The Event dialog box displays the Event log. You can do the following on the Event log dialog box.

- Select which severity of event to view or view all of the recorded events.
- View when the event occurred.
- View the severity of the event.
- View the description of the event.

The data is only displayed when the module is online.

Figure 81 - Event Log Dialog Box



The Event log dialog box includes the following parameters.

Table 77 - Event Log Parameter Descriptions

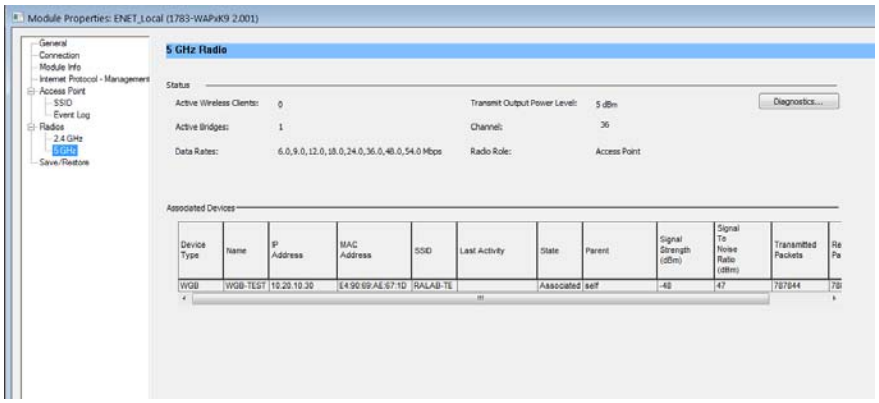
Parameter	Description
Severity Filter	Use this to select which severity of event to display in the event log table. • AccessPoint_Emergency - system is unusable • AccessPoint_Alert - immediate action is required • AccessPoint_Critical - conditions are critical • AccessPoint_Error - error conditions are recorded • AccessPoint_Warning - indicates a potential error condition • AccessPoint_Notification - normal operation is occurring but significant conditions could result • AccessPoint_Informational - an information message provides routine information on normal activity; does not indicate an error • AccessPoint_Debugging - debugging messages are provided • None - display all events
Time	Time stamp that was recorded with the event.
Severity	The severity of the event. • AccessPoint_Emergency • AccessPoint_Alert • AccessPoint_Critical • AccessPoint_Error AccessPoint_Warning • AccessPoint_Notification • AccessPoint_Informational • AccessPoint_Debugging None
Description	Description of the error event.

Radios Dialog Box

Use this dialog box to show summary information about the radios contained in the Stratix 5100. The Stratix 5100 contains simultaneous dual-band radios (2.4 GHz and 5 GHz). You can view the following on the Radios dialog box:

- Description of the radios.
- MAC address associated with the radios.
- Time the radios have been up and running.
- Status of the software and hardware.
- The data is only displayed when the module is online.

Figure 82 - 2.4 GHz or 5 GHz Radio Dialog Box



The Radios dialog box includes the following parameters.

Table 78 - Radios Dialog Box Parameter Descriptions

Parameter	Description
Radio (GHz)	The dual-band radio. Stratix 5100 contains a 2.4 GHz and 5 GHz radio.
Description	Description of the radio.
MAC Address	MAC address associated with the radio
Uptime	Time since the network management system was started.
Software Status	Administrative status of the interface. • Up • Down • Testing • Unknown • Dormant • Not Present • LowerLayerDown
Hardware Status	Indicates whether the line protocol for the interface is enabled or disabled.

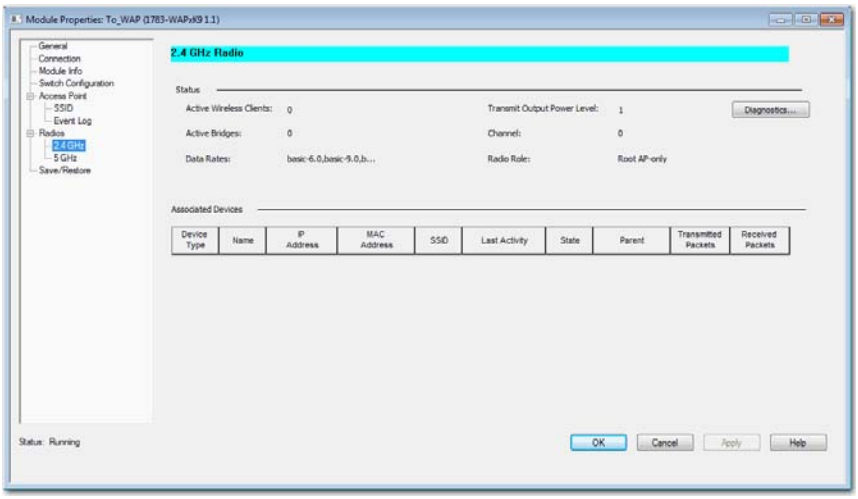
2.4 GHz or 5 GHz Radio Dialog Box

Use this dialog box to view information about the 2.4 GHz or 5 GHz band radio. You can do the following on the 2.4 GHz or 5 GHz Radio dialog box.

- View the number of active wireless clients and bridges currently associating with the radio.
- View the power level and data rate used to transmit data.
- View the role of the radio and the type of client device.
- View the IP address, MAC address, state of the client device, and number of packets sent to and received from the client.
- Open a Diagnostic dialog box to view counters and statistics per rate of the radio.

The data is only displayed when the module is online.

Figure 83 - 2.4 GHz or 5 GHz Radio Dialog Box



The 2.4 GHz or 5 GHz Radio dialog box includes the following parameters.

Table 79 - 2.4 GHz or 5 GHz Radio Parameter Descriptions

Parameter	Description
Active Wireless Clients	Number of wireless clients currently associating with the device on this interface.
Active Bridges	Number of bridges currently associating with this device on this interface.
Data Rates	The rate the device uses to transmit data. • 1.0, 2.0, 5.5, 11.0, 6.0, 9.0, 12.0, 18.0, 24.0, 36,0, 48.0, and 54.0 Mbps • 802.11n rates: m0…m23
Transmit Output Power Level	The power level used to transmit data. The power level depends on the band and the channel.
Channel	The current operating frequency channel.

Table 79 - 2.4 GHz or 5 GHz Radio Parameter Descriptions (Continued)

Parameter	Description
Radio Role	Identifies the role of the radio. • Non-Root Bridge • Non-Root Bridge with Wireless Clients • Repeater • Root Access Point • Root AP-only • Root Bridge • Root Bridge with Wireless Clients • Scanner • Workgroup Bridge
Diagnostic	Opens the Diagnostic dialog box where you can view the counters and statistics per rate for the radio. This dialog box provides information for monitoring and diagnosing the access point operation.
Device Type	The type of device. • Unknown • WGB-Client • WGB • Client • Repeater • Bridge Name
Name	Name of the device.
IP Address	IP address of the client device.
MAC Address	MAC address of the client device.
SSID	SSID which the client associated to the WAP.
Last Activity	Time since the device has been active.
State	State of the client device. • Association-Processing • EAP-Associated • MAC-Associated • Associated
Parent	Name of the parent wireless client device.
Transmitted Packets	Number of packets sent to the client.
Received Packets	Number of packets received from the client.

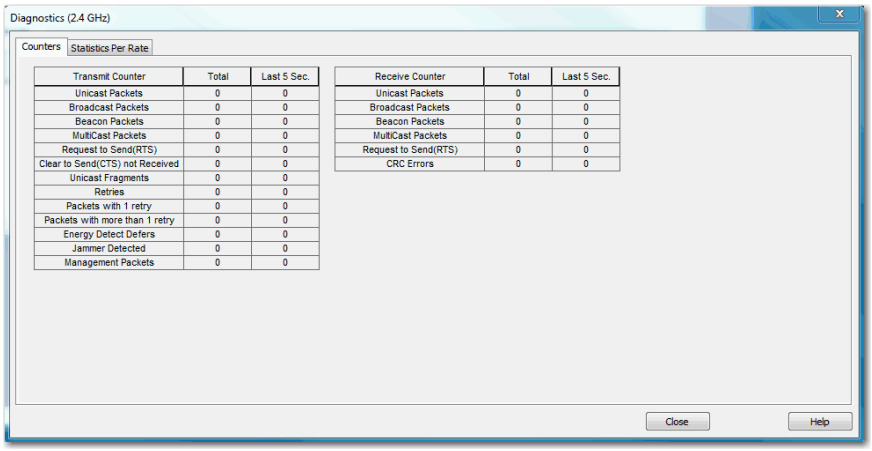
Counters Dialog Box

Use this dialog box to view information about the data packets received and transmitted in the last 5 seconds as well as a cumulative total. This dialog box and the Statistics Per Rate dialog box provide useful information for monitoring and diagnosing the access point operation. To get to the Counters dialog box, you need to click Diagnostic in the Radio page.

You can view the following on the Counters dialog box:

- Unicast, Broadcast, Beacon, and Multicast packets sent/received by the access point
- Request to Send (RTS) and Clear to Send (CTS) sent/received by the access point
- Number of times the access point attempts to send a packet
- Packets deferred because another radio was transmitting
- An interference source was detected but ignored
- Packets with CRC errors

The data is only displayed when the module is online.



The Counters dialog box includes the following parameters.

Table 80 - Counters Parameter Descriptions

Parameter	Description
Transmit Counter	Transmit statistics.
Receive Counter	Receive statistics
Total	Number of total packets transmitted to or received from the client.
Last 5 Sec.	Number of transmitted or received packets in the last 5 seconds.
Unicast Packets	Number of unicast packets sent/received by the access point.
Broadcast Packets	Number of broadcast packets sent/received by the access point.
Beacon Packets	Number of beacon packets sent/received by the access point.
Multicast Packets	Number of multicast packets sent/received by the access point.

Table 80 - Counters Parameter Descriptions (Continued)

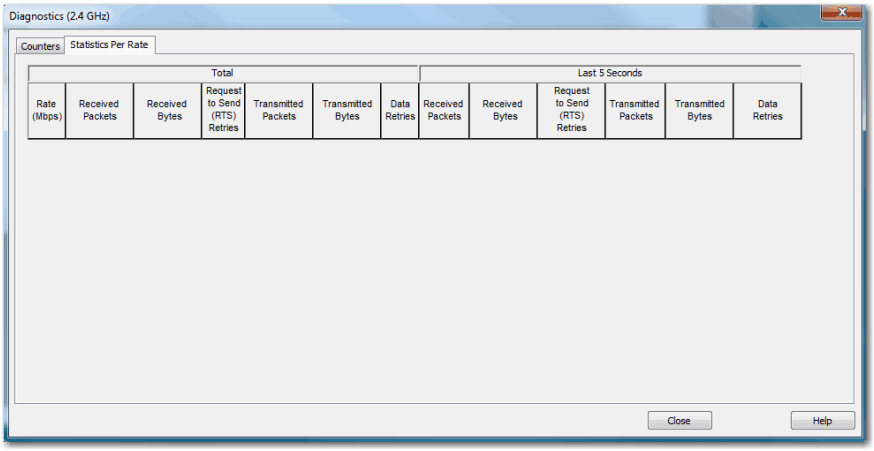
Parameter	Description
Request to Send (RTS)	Number of times an RTS was sent/received by the access point.
Clear to Send (CTS) not Received	Number of times an RTS was sent but a CTS was not received in response.
Unicast Fragments	Number of whole or partial fragmented packet sent.
Retries	Number of times the access point attempts to send a packet or RTS.
Packets with 1 retry	Number of times the access point attempts only once to send a packet.
Packets with more than 1 retry	Number of times the access point attempts more than once to send a packet.
Energy Detect Defers	Number of times a packets was deferred from sending because the energy detect circuitry indicates that another radio was transmitting.
Jammer Detected	Number of times an interference source was detected that lasted longer than a legal 802.11 packet. The interference source was ignored and the transmission was repeated.
Management Packets	Number of management packet sent by the access point.
CRC Errors	Number of packets with CRC errors.

Statistics Per Rate Dialog Box

Use this dialog box to view information about the data packets received and transmitted in the last 5 seconds as well as a cumulative total. This dialog box and the Counters dialog box provide useful information for monitoring and diagnosing the access point operation.

You can view the following on the Statistics Per Rate dialog box.

- Rate used to transmit data
- Number of packets and bytes received
- Number of times the access point attempts to send the Request to Send (RTS)
- Number of packets and bytes sent from the access point



The data is only displayed when the module is online.

Table 81 - Statistics Per Rate Parameter Descriptions

Parameter	Description
Total	Number of total packets transmitted to or received from the client.
Last 5 Seconds	Number of transmitted or received packets in the last 5 seconds.
Rate (Mbps)	Rate used to transmit data. Rates are expressed in megabits per second.
Received Packets	Number of packets being received.
Received Bytes	Number of bytes being received.
Request to Send (RTS) Retries	Number of times the access point attempts to send the RTS packet.
Transmitted Packets	Number of packets sent from the access point.
Transmitted Bytes	Number of bytes sent from the access point.
Data Retries	Number of times the access point attempts to send the data packets.

Module-Defined Data Types

The table below lists and describes module-defined data types for the Stratix 5100 Wireless Access Point. The table includes information for input, as indicated by an 'I'.

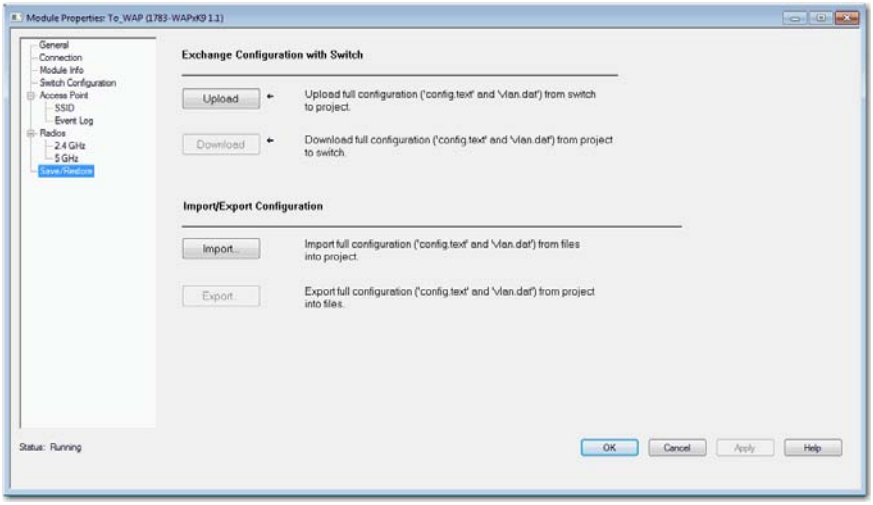
Table 82 - Module-Defined Data Type: AB:STRATIX_5100_1PORT:I:0

Member Name	Type	Default Display Style
Fault	DINT	Binary
Radio2_4GHzEnabled	BOOL	Decimal
Radio5GHzEnabled	BOOL	Decimal
Radio2_4GHzUptime	DINT	Decimal
Radio5GHzUptime	DINT	Decimal
ClientsConnected	INT	Decimal
WorkGroupBridgesConnected	INT	Decimal
UnicastPacketsSent	DINT	Decimal
UnicastPacketsReceived	DINT	Decimal
CRCErrors	DINT	Decimal
TotalPacketsMoreThan1Retry	DINT	Decimal
TotalRetries	DINT	Decimal
SSIDsDefined	INT	Decimal
PortGiConnected	BOOL	Decimal
PortGiSpeed	DINT	Decimal
PortGiFullDuplex	BOOL	Decimal

Save/Restore Dialog Box

The Save and Restore dialog box upload and downloads the project to and from the access point.

Figure 84 - Save/Restore Dialog Box



The Save/Restore dialog box includes the following parameters.

Table 83 - Save/Restore Parameter Descriptions

Item	Description
Exchange Configuration with Switch	**Upload** Upload the full configuration from the switch to the project when online. This includes the config.txt file. Upload is not available in offline mode. **Download** Download the full configuration from the project to the switch when online. This includes the config.txt file. Download is not available in offline mode.
Import/Export Configuration	**Import** Import the switch configuration from a file stored locally on a computer to the project file when online. This includes the config.txt file. When the Import dialog box appears: 1. Enter the name of the config.txt file (and full path) that contains the content you want to import. 2. Click Import. The system imports the file into the project. The switch configuration files are provided in the Projects Samples directory. If you want to reset the switch to its out-of-box defaults remotely, import the files into the project, and download them to the switch. **Export** Export the switch configuration data from the project to a file when online. When the Export dialog box appears, follow these steps. 1. Enter the name for the config.txt file (and full path). 2. Click Export. The system exports the content. Export is not available in offline mode.

Configure the Stratix 5100 WAP Using the Command-Line Interface

This chapter describes the Cisco IOS command-line interface (CLI) that you can use to configure the wireless device.

Topic	Page
Cisco IOS Command Modes	191
Get Help	192
Abbreviate Commands	193
Use No and Default Forms of Commands	193
Understand CLI Messages	194
Command History	194
Use Editing Features	195
Search and Filter Output of show and more Commands	198
Access CLI	198
Open CLI with Secure Shell	199

Cisco IOS Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on the mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

When you start a session on the wireless device, you begin in user mode, often called user EXEC mode. A subset of the Cisco IOS commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as show commands, that show the current configuration status, and clear commands, that clear counters or interfaces. The user EXEC commands are not saved when the wireless device restarts.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you must enter privileged EXEC mode before you can enter the global configuration mode.

You can make changes to the running configuration by using the configuration modes: global, interface, and line. If you save the configuration, these commands are stored and used when the wireless device restarts. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the host name ap.

Table 84 - Command Modes

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with the wireless device.	ap>	Enter logout or quit.	Use this mode to: • Change terminal settings • Perform basic tests • Display system information
Privileged EXEC	While in user EXEC mode, enter the enable command.	ap#	Enter disable to exit.	Use this mode to display device configuration, diagnostics, and debug information. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the configure command.	ap(config)#	To exit to privileged EXEC mode, enter exit or end, or press Ctrl-Z.	Use this mode to configure parameters that apply to the entire wireless device.
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	ap(config-if)#	To exit to global configuration mode, enter exit. To return to privileged EXEC mode, press Ctrl-Z or enter end.	Use this mode to configure parameters for the Ethernet and radio interfaces. • The 802.11n 2.4 GHz radio is radio 0 • The 802.11n 5 GHz radio is radio 1

Get Help

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command, as shown in this table.

Table 85 - Help Summary

Command	Purpose
help	Obtains a brief description of the help system in any command mode.

abbreviated-command-entry?	Obtains a list of commands that begin with a particular character string.
	For example:
	`ap# di?`
	`dir  disable  disconnect`

abbreviated-command-entry<Tab>	Completes a partial command name.
	For example:
	`ap# sh conf<tab>`
	`ap# show configuration`

Table 85 - Help Summary (Continued)

Command	Purpose
?	Lists all commands available for a particular command mode. For example: `ap> ?`
command ?	Lists the associated keywords for a command. For example: `ap> show ?`
command keyword ?	Lists the associated arguments for a keyword. For example: `ap(config)# cdp holdtime ?` <10-255> Length of time (in sec) that receiver must keep this packet

Abbreviate Commands

You have to enter only enough characters for the wireless device to recognize the command as unique. This example shows how to enter the show configuration privileged EXEC command:

```
ap# show conf
```

Use No and Default Forms of Commands

Most configuration commands also have a no form. In general, use the no form to disable a feature or function or reverse the action of a command. For example, the no shutdown interface configuration command reverses the shutdown of an interface. Use the command without the keyword `no` to enable a disabled feature again or enable a feature that is disabled by default.

Configuration commands can also have a default form. The default form of a command returns the command setting to its default. Most commands are disabled by default, so the default form is the same as the `no` form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the default command enables the command and sets variables to their default values.

Understand CLI Messages

This table lists some error messages that you can encounter while using CLI to configure the wireless device.

Table 86 - CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: show con	You did not enter enough characters for the wireless device to recognize the command.	Enter the command followed by a question mark (**?**) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
% Incomplete command.	You did not enter all the keywords or values required by this command.	Enter the command followed by a question mark (**?**) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
% Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (**?**) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command are displayed.

Command History

The CLI provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize the command history feature to suit your needs.

Change the Command History Buffer Size

By default, the wireless device records ten command lines in its history buffer. Beginning in privileged EXEC mode, enter this command to change the number of command lines that the wireless device records during the current terminal session:

```
ap# terminal history[size number-of-lines]
```

The range is from 0...256.

Beginning in line configuration mode, enter this command to configure the number of command lines the wireless device records for all sessions on a particular line:

```
ap(config-line)# history [size number-of-lines]
```

The range is from 0...256.

Recall Commands

To recall commands from the history buffer, perform one of the actions listed in this table.

Table 87 - Recall Command Actions and Results

Action[1]	Result
Press Ctrl-P or the up arrow key.	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press Ctrl-N or the down arrow key.	Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history	While in privileged EXEC mode, list the last several commands that you just entered. The number of commands that are displayed is determined by the setting of the terminal history global configuration command and history line configuration command.

(1) The arrow keys function only on ANSI-compatible terminals such as VT100s.

Disable the Command History Feature

The command history feature is automatically enabled.

- To disable the feature during the current terminal session, enter the terminal no history privileged EXEC command.
- To disable command history for the line, enter the no history line configuration command.

Use Editing Features

This section describes the editing features that can help you manipulate the command line.

Enable and Disable Editing Features

Although enhanced editing mode is automatically enabled, you can disable it.

To enable the enhanced editing mode again for the current terminal session, enter this command in privileged EXEC mode:

```
ap# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
ap(config-line)# editing
```

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
ap(config-line)# no editing
```

Edit Commands by Using Keystrokes

This table shows the keystrokes that you need to edit command lines.

Table 88 - Editing Commands Through Keystrokes

Capability	Keystroke(1)	Purpose
Move around the command line to make changes or corrections.	Ctrl-B or the left arrow key	Move the cursor back one character.
	Ctrl-F or the right arrow key	Move the cursor forward one character.
	Ctrl-A	Move the cursor to the beginning of the command line.
	Ctrl-E	Move the cursor to the end of the command line.
	Esc B	Move the cursor back one word.
	Esc F	Move the cursor forward one word.
	Ctrl-T	Transpose the character to the left of the cursor with the character at the cursor.
Recall commands from the buffer and paste them in the command line. The wireless device provides a buffer with the last ten items that you deleted.	Ctrl-Y	Recall the most recent entry in the buffer.
	Esc Y	Recall the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press Esc Y more than ten times, you cycle to the first buffer entry.
Delete entries if you make a mistake or change your mind.	Delete or Backspace	Erase the character to the left of the cursor.
	Ctrl-D	Delete the character at the cursor.
	Ctrl-K	Delete all characters from the cursor to the end of the command line.
	Ctrl-U or Ctrl-X	Delete all characters from the cursor to the beginning of the command line.
	Ctrl-W	Delete the word to the left of the cursor.
	Esc D	Delete from the cursor to the end of the word.
Capitalize or lowercase words or capitalize a set of letters.	Esc C	Capitalize at the cursor.
	Esc L	Change the word at the cursor to lowercase.
	Esc U	Capitalize letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	Ctrl-V or Esc Q	
Scroll down a line or screen that are longer than the terminal screen can display. The `More` prompt appears for output that has more lines than can be displayed on the terminal screen, including show command output. You can use the Return and Space bar keystrokes whenever you see the `More` prompt.	Return	Scroll down one line.
	Space	Scroll down one screen.
Redisplay the current command line if the wireless device suddenly sends a message to your screen.	Ctrl-L or Ctrl-R	Redisplay the current command line.

(1) The arrow keys function only on ANSI-compatible terminals such as VT100s.

Edit Command Lines that Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command.

To scroll back to the beginning of the command entry, press Ctrl-B or the left arrow key repeatedly. You can also press Ctrl-A to immediately move to the beginning of the line.

The arrow keys function only on ANSI-compatible terminals such as VT100s.

In this example, the `access-list global configuration` command entry extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign `$` shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
ap(config)# access-list 101 permit tcp 131.108.2.5
255.255.255.0 131.108.1

ap(config)# $ 101 permit tcp 131.108.2.5
255.255.255.0 131.108.1.20 255.25

ap(config)# $t tcp 131.108.2.5 255.255.255.0
131.108.1.20 255.255.255.0 eq

ap(config)# $108.2.5 255.255.255.0 131.108.1.20
255.255.255.0 eq 45
```

After you complete the entry, press Ctrl-A to check the complete syntax before pressing the Return key to execute the command. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right:

```
ap(config)# access-list 101 permit tcp 131.108.2.5
255.255.255.0 131.108.1$
```

The software assumes you have a terminal screen that is 80 columns wide. If you have a width other than that, use the terminal width privileged EXEC command to set the width of your terminal.

Use line wrapping with the command history feature to recall and modify previous complex command entries. For information about recalling previous command entries, see Edit Commands by Using Keystrokes on page 196.

Search and Filter Output of `show` and `more` Commands

You can search and filter the output for show and more commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you don't need to see.

To use this functionality, enter a show or more command followed by the pipe character (|), one of the keywords begin, include, or exclude, and an expression that you want to search for or filter out:

```
command | {begin | include | exclude} regular-expression
```

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output are not displayed, but the lines that contain Output are displayed.

This example shows how to include in the output display only lines where the expression protocol appears:

```
ap# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```

Access CLI

You can open the wireless device CLI by using Telnet or Secure Shell (SSH).

Open CLI with Telnet

Follow these steps to open CLI with Telnet. These steps are for a computer running Microsoft Windows with a Telnet terminal application. Check your computer operating instructions for detailed instructions for your operating system.

1. Click Start>Programs>Accessories>Telnet.

   If Telnet is not listed in your Accessories menu, click Start>Run, type Telnet in the entry field, and press Enter.
2. When the Telnet page appears, click Connect and choose Remote System.
3. In the Host Name field, type the wireless device IP address and click Connect.
4. At the username and password prompts, enter your administrator username and password.

   Default username is blank, default password is **`wirelessap`**. The default enable password is also **`wirelessap`**. Usernames and passwords are case sensitive.

Open CLI with Secure Shell

Secure Shell Protocol is a protocol that provides a secure, remote connection to networking devices. Secure Shell (SSH) is a software package that provides secure login sessions by encrypting the entire session. SSH features strong cryptographic authentication, strong encryption, and integrity protection. For detailed information on SSH, visit the homepage of SSH Communications Security, Ltd. at this URL: http://www.ssh.com/.

SSH provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. SSH versions 1 and 2 are supported in this release.

See Configure the Access Point for Secure Shell on page 239 for detailed instructions on setting up the wireless device for SSH access.

Reset Default Settings by Using CLI

ATTENTION: Do not delete any of the system files prior to resetting defaults or reloading software.

If you want to reset the access point to its default settings, use either of the following commands.

```
write erase
erase startup-config
```

From the privileged EXEC mode, you can reset the access point/bridge configuration to factory default values by using CLI by following these steps:

1. Enter `write erase` or `erase startup-config`.
2. Enter `Y` when the following CLI message appears:

   ```
   Erasing the nvram filesystem will remove all
   configuration files! Continue? [confirm].
   ```

3. Enter reload when the following CLI message appears:

   ```
   Erase of nvram: complete. This command reloads the
   operating system.
   ```

4. Enter `Y` when the following CLI message appears:

   ```
   Proceed with reload? [confirm].
   ```

ATTENTION: Avoid damaging the configuration, don't interrupt the startup process. Wait until the access point/bridge Install Mode status indicator begins to blink green before continuing with CLI configuration changes.

After the access point/bridge restarts, you can reconfigure the access point by using the Device Manager or CLI.

By default, the access point is configured to receive an IP address by using DHCP. To display the IP address for an access point/bridge, you can use the `show interface bvi1` command.

Security CLI Configuration Examples

The examples in this section show CLI commands that are equivalent to creating SSIDs by using each security type on the Security menu. This section contains these example configurations:

Example 1: No Security

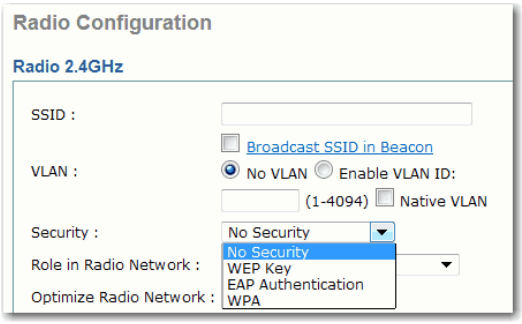
This example shows part of the configuration that results from using the Security page to create an SSID called `no_security_ssid`, including the SSID in the beacon, assigning it to VLAN 10, and choosing VLAN 10 as the native VLAN.

TIP These examples are not entire configurations, just examples of what a configuration can look like in CLI.

```
!
dot11 ssid no_security_ssid
authentication open
vlan 10
!
interface Dot11Radio1
 no ip address
 no ip route-cache
!
ssid no_security_ssid
!
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
48.0 54.0
 rts threshold 2312
 station-role root
!
interface Dot11Radio1.10
 encapsulation dot1Q 10 native
no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
```

```
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
```

For the instructions in Device Manager, see Configure Security on page 58.



Example 2: WPA with Pre-shared Keys (WPA2-PSK)

This example shows part of the configuration that results from using the Security page to create an SSID called `wpa2_psk_ssid`. It describes excluding the SSID from the beacon, assigning the SSID to VLAN 20, and configuring WPA2 key management with a pre-shared key and AES encryption.

```
ssid wpa2_psk_ssid
      vlan 20
      authentication open
authentication key-management wpa version 2
wpa-psk ascii 7 06345F2247590C48544541
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
encryption vlan 20 mode ciphers aes-ccm
!
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0
 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
```

```
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled

   ssid wpa2_psk_ssid
!
interface Dot11Radio0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 subscriber-loop-control
 bridge-group 20 block-unknown-source
 no bridge-group 20 source-learning
 no bridge-group 20 unicast-flooding
 bridge-group 20 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
encryption vlan 20 mode ciphers aes-ccm
 !
 ssid wpa2_psk_ssid
!
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0
36.0 48.0 54.0
station-role root
bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
```

```
bridge-group 20 subscriber-loop-control
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
bridge-group 20 spanning-disabled
```

For more information instructions in Device Manager, see Easy Setup Network Configuration Security Limitations on page 59

Example 3: WPA and EAP

This example shows part of the configuration that results from using the Security page to:

- create an SSID called `wpa_ssid`
- configure WPA key management with EAP
- excluding the SSID from the beacon
- assigning the SSID to VLAN 40

```
dot11 ssid wpa_ssid
    vlan 40
    authentication open eap eap_methods
    authentication network-eap eap_methods
    authentication key-management wpa
 !
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.91.104.92 auth-port 1645 acct-port 1646
!
aaa authentication login eap_methods group rad_eap
aaa authorization exec default local
aaa session-id common
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 40 mode ciphers tkip
 !
     ssid wpa_ssid
!
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
48.0 54.0
```

```
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
 bridge-group 40 spanning-disabled
!
    ssid wpa_ssid
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 no bridge-group 40 source-learning
 bridge-group 40 spanning-disabled
!
```

```
ip radius source-interface BVI1
radius-server host 10.91.104.92 auth-port 1645
acct-port 1646 key 7 091D1C5A4D5041
!
```

For the instructions in Device Manager, see Configure Security on page 58.

Assign an IP Address by Using CLI

When you connect the wireless device to the wired LAN, the wireless device links to the network by using a bridge virtual interface (BVI) that it creates automatically. Instead of tracking separate IP addresses for the wireless device Ethernet and radio ports, the network uses the BVI.

When you assign an IP address to the wireless device by using CLI, you must assign the address to the BVI. Beginning in privileged EXEC mode, follow these steps to assign an IP address to the wireless device BVI:

1. Enter the global configuration mode to configure the terminal.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the BVI.

   ```
   interface bvil
   ```

3. Assign an IP address and address mask to the BVI.

   ```
   ip address address mask
   ```

   TIP If you are connected to the wireless device by using a Telnet session, you lose your connection to the wireless device when you assign a new IP address to the BVI. If you need to continue configuring the wireless device by using Telnet, use the new IP address to open another Telnet session to the wireless device.

For the instructions in Device Manager, see Obtain and Assign an IP Address on page 48

Configure the 802.1X Supplicant

Traditionally, the `dot1x` authenticator/client relationship has always been a network device and a personal computer client respectively, as it was the personal computer user that had to authenticate to gain access to the network. However, wireless networks introduce unique challenges to the traditional authenticator/client relationship.

First, access points can be placed in public places, inviting the possibility that they can be unplugged and their network connection used by an outsider. Second, when a repeater access point is incorporated into a wireless network, the repeater access point must authenticate to the root access point in the same way as a client does.

The supplicant is configured in two phases:

- Create and configure a credentials profile
- Apply the credentials to an interface or SSID

You can complete the phases in any order, but they must be completed before the supplicant becomes operational.

Create a Credentials Profile

Beginning in privileged EXEC mode, follow these steps to create an 802.1X credentials profile.

For information in Device Manager, see AP Authentication on page 119.

1. Enter the global configuration mode to configure the terminal.

   ```
   configure terminal
   ```

2. Creates a `dot1x` credentials profile and enters the `dot1x` credentials configuration submode.

   ```
   dot1x credentials profile
   ```

3. Enter the anonymous identity to be used. This is optional.

   ```
   anonymous-id description
   ```

4. (Optional) Enter a description for the credentials profile.

   ```
   description description
   ```

5. Enter the authentication user id.

   ```
   username username
   ```

6. Enter an unencrypted password for the credentials.
   - 0, an unencrypted password follows.
   - 7, a hidden password follows. Hidden passwords are used when applying a previously saved configuration.
   - LINE, an unencrypted (clear text) password. Unencrypted and clear text are the same. You can enter a 0 followed by the clear text password, or omit the 0 and enter the clear text password.

   ```
   password {0 | 7 | LINE}
   ```

7. (Optional and used only for EAP-TLS)—Enter the default pki-trustpoint.

   ```
   pki-trustpoint pki-trustpoint
   ```

8. Return to the privileged EXEC mode.

   ```
   end
   ```

9. (Optional) Save your entries in the configuration file.

   ```
   copy running config startup-config
   ```

Use the `no` form of the `dot1x creden` command to negate a parameter.

The following example creates a credentials profile named *test* with the username *Rockwell* and a the unencrypted password *wirelessap*.

```
ap1240AG>enable
Password:xxxxxxx
ap1240AG#config terminal
Enter configuration commands, one per line. End
with CTRL-Z.
ap1240AG(config)# dot1x credentials test
```

```
ap1240AG(config-dot1x-creden)#username Rockwell
ap1240AG(config-dot1x-creden)#password wirelessap
ap1240AG(config-dot1x-creden)#exit
ap1240AG(config)#
```

Apply the Credentials Profile to an SSID Used for the Uplink

If you have a workgroup bridge or a repeater access point in your wireless network and are using the 802.1X supplicant on the root access point, you must apply the 802.1X supplicant credentials to the SSID the workgroup bridge or a repeater uses to associate with and authenticate to the root access point.

Beginning in the privileged EXEC mode, follow these steps to apply the credentials to an SSID used for the uplink.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter the 802.11 SSID.

The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. The first character cannot contain the !, #, or ; character. The characters +,], /, ", TAB, and trailing spaces are invalid characters for SSIDs.

```
dot11 ssid ssid
```

3. Enter the name of a preconfigured credentials profile.

   ```
   dot1x credentials profile
   ```

4. Exits the dot1x credentials configuration submode

   ```
   end
   ```

5. Save your entries in the configuration file. This is optional.

   ```
   copy running config startup-config
   ```

The following example applies the credentials profile test to the `ssid testap1` on a repeater access point.

```
repeater-ap>enable
Password:xxxxxxx
repeater-ap#config terminal
Enter configuration commands, one per line. End
with CTRL-Z.
repeater-ap(config-if)#dot11 ssid testap1
repeater-ap(config-ssid)#dot1x credentials test
repeater-ap(config-ssid)#end
repeater-ap(config)
```

Create and Apply EAP Method Profiles

You can optionally configure an EAP method list to enable the supplicant to recognize a particular EAP method. See Create and Apply EAP Method Profiles for the 802.1X Supplicant on page 347.

Administer the WAP Access

This chapter describes how to administer the wireless device.

Topic	Page
Disable the Mode Button	212
Prevent Unauthorized Access to Your Access Point	213
Protect Access to Privileged EXEC Commands	213
Control Access Point Access with RADIUS	219
Control Access Point Access with TACACS+	226
Configure Ethernet Speed and Duplex Settings	229
Configure the Access Point for Local Authentication and Authorization	230
Configure the Authentication Cache and Profile	232
Configure the Access Point to Provide DHCP Service	236
Configure the Access Point for Secure Shell	239
Configure Client ARP Caching	240
Manage the System Time and Date	241
Define HTTP Access	246

Disable the Mode Button

You can disable the mode button on access points having a console port by using the `[no] boot mode-button` command. This command prevents password recovery and is used to prevent unauthorized users from gaining access to the access point CLI.

IMPORTANT This command disables password recovery. If you lose the privileged EXEC mode password for the access point after entering this command, you need to contact the Cisco Technical Assistance Center (TAC) to regain access to the access point CLI.

The mode button is enabled by default. Beginning in the privilege EXEC mode, follow these steps to disable the access point mode button.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Disables the access point mode button.

   ```
   no boot mode-button
   ```

3. It is not necessary to save the configuration.

   ```
   end
   ```

You can check the status of the mode-button by executing the `show boot` or `show boot mode-button` commands in the privileged EXEC mode. The status does not appear in the running configuration. The following shows a typical response to the `show boot and show boot mode-button` commands.

```
ap#show boot
BOOT path-list: flash:/c1200-k9w7-mx-
v123_7_ja.20050430/c1200-k9w7-mx.v123_7_ja.20050430
Config file: flash:/config.txt
Private Config file: flash:/private-config
Enable Break: no
Manual boot:no
Mode button:on
Enable IOS break: no
HELPER path-list:
NVRAM/Config file
     buffer size: 32768

ap#show boot mode-button
on
ap#
```

As long as the privileged EXEC password is known, you can restore the mode button to normal operation by using the `boot mode-button` command.

Prevent Unauthorized Access to Your Access Point

You can prevent unauthorized users from reconfiguring the wireless device and viewing configuration information. Typically, you want network administrators to have access to the wireless device while you restrict access to users who connect through a terminal or workstation from within the local network.

To prevent unauthorized access to the wireless device, configure one of these security features:

- Username and password pairs, that are locally stored on the wireless device. These pairs authenticate each user before that user can access the wireless device. You can also assign a specific privilege level (read-only or read/write) to each username and password pair.
- Username and password pairs stored centrally in a database on a security server.

TIP Characters TAB, ?, $, +, and [are invalid characters for passwords.

For more information in CLI, see the Configure Username and Password Pairs on page 216.

The default username is blank, and the default password is `wirelessap`. Usernames and passwords are case-sensitive.

- For more information, see the Control Access Point Access with RADIUS on page 219.
- For more information, see the Configure Security on page 58.

Protect Access to Privileged EXEC Commands

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can issue after they have logged into a network device.

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Security Command Reference for Release 12.3.

Default Password and Privilege Level Configuration

This table shows the default password and privilege level configuration.

Table 89 - Default Password and Privilege Levels

Feature	Default Setting
Username and password	Default username is blank and the default password is *wirelessap*.
Enable password and privilege level	Default password is *wirelessap*. The default is level 15 (privileged EXEC level). The password is encrypted in the configuration file.
Enable secret password and privilege level	The default enable password is *wirelessap*. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
Line password	Default password is *wirelessap*. The password is encrypted in the configuration file.

Set or Change a Static Enable Password

The enable password controls access to the privileged EXEC mode. The `no enable password` global configuration command removes the enable password, but use extreme care when using this command. If you remove the enable password, you are locked out of the EXEC mode.

Beginning in privileged EXEC mode, follow these steps to set or change a static enable password.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Define a new password or change an existing password for access to privileged EXEC mode.

   ```
   enable password password
   ```

The default password is *wirelessap*.

For *password*, specify a string from 1...25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces.

TIP Characters TAB, ?, $, +, and [are invalid characters for passwords.

3. Return to privileged EXEC mode.

   ```
   end
   ```

4. Verify your entries.

   ```
   show running-config
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

The enable password is not encrypted and can be read in the wireless device configuration file.

This example shows how to change the enable password to *l1u2c3k4y5*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
AP(config)# enable password l1u2c3k4y5
```

Protect Enable and Enable Secret Passwords with Encryption

To provide an additional layer of security, you can use either the `enable password` or `enable secret` global configuration commands. Both commands accomplish the same thing; that is, you can establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify.

We recommend that you use the `enable secret` command because it uses an improved encryption algorithm.

If you configure the `enable secret` command, it takes precedence over the `enable password` command; the two commands cannot be in effect simultaneously.

Beginning in privileged EXEC mode, follow these steps to configure encryption for enable and enable secret passwords.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Define a new password or change an existing password for access to privileged EXEC mode.

   ```
   enable password [level level] {password |
   encryption-type encrypted-password}
   ```

or

```
enable secret [level level] {password | encryption-
type encrypted-password}
```

Define a secret password, that is saved by using a nonreversible encryption method.

- (Optional) For `level`, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges).
- For `password`, specify a string from 1...25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.
- (Optional) For `encryption-type`, type only a 5, a Cisco proprietary encryption algorithm, is available. If you specify an encryption type, you must provide an encrypted password—an encrypted password you copy from another access point configuration.

TIP If you specify an encryption type and then enter a clear text password, you can not re-enter privileged EXEC mode. You cannot recover a lost encrypted password by any method.

3. (Optional) Encrypt the password when the password is defined or when the configuration is written.

   ```
   service password-encryption
   ```

Encryption prevents the password from being readable in the configuration file.

4. Return to privileged EXEC mode.

   `end`

5. (Optional) Save your entries in the configuration file.

   `copy running-config startup-config`

If both the enable and enable secret passwords are defined, users must enter the enable secret password.

Use the `level` keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the `privilege level` global configuration command to specify commands accessible at various levels. For more information, see the Configure Multiple Privilege Levels on page 218.

If you enable password encryption, it applies to all passwords including username passwords, authentication key passwords, the privileged command password, and console and virtual terminal line passwords.

- To remove a password and level, use the `no enable password [level level]` or `no enable secret [level level]` global configuration command.
- To disable password encryption, use the `no service password-encryption` global configuration command.

This example shows how to configure the encrypted password *1FaD0$Xyti5Rkls3LoyxzS8* for privilege level 2:

```
AP(config)# enable secret level 2 5
$1$FaD0$Xyti5Rkls3LoyxzS8
```

Configure Username and Password Pairs

You can configure username and password pairs, that are locally stored on the wireless device. These pairs are assigned to lines or interfaces and authenticate each user before that user can access the wireless device. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

Beginning in privileged EXEC mode, follow these steps to establish an authentication system based on a username that requests a login username and a password.

1. Enter global configuration mode.

   `configure terminal`

2. Enter the username, privilege level, and password for each user.

```
username name [privilege level] {password
encryption-type password}
```

- For `name`, specify the user ID as one word. Spaces and quotation marks are not allowed.
- (Optional) For `level`, specify the privilege level the user has after gaining access. The range is 0...15.

  Level 15 gives privileged EXEC mode access. Level 1 gives user EXEC mode access.
- For `encryption-type`, enter `0` to specify that an unencrypted password follows.
- Enter `7` to specify that a hidden password follows.
- For `password`, specify the password the user must enter to gain access to the wireless device.

  The password must be from 1...25 characters, can contain embedded spaces, and must be the last option specified in the `username` command.

3. Enable local password checking at login time. Authentication is based on the username specified in Step 2.

   ```
   login local
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. Verify your entries.

   ```
   show running-config
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

- To disable username authentication for a specific user, use the `no username name` global configuration command.
- To disable password checking and allow connections without a password, use the `no login` line configuration command.

TIP You must have at least one username configured and you must have login local set to open a Telnet session to the wireless device. If you enter no username for the only username, you can be locked out of the wireless device.

Configure Multiple Privilege Levels

By default, Cisco IOS software has two modes of password security: user EXEC and privileged EXEC. You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

For example, if you want many users to have access to the `clear line` command, you can assign it level 2 security and distribute the level 2 password fairly widely. But if you want more restricted access to the `configure` command, you can assign it level 3 security and distribute that password to a more restricted group of users.

Set the Privilege Level for a Command

Beginning in privileged EXEC mode, follow these steps to set the privilege level for a command mode.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Set the privilege level for a command.
   - For *mode*, enter `configure` for global configuration mode, `exec` for EXEC mode, `interface` for interface configuration mode, or `line` for line configuration mode.
   - For *level*, the range is from 0...15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the `enable` password.
   - For *command*, specify the command that you want to have restricted access.

   ```
   privilege mode level level command
   ```

3. Specify the enable password for the privilege level.

- For *level*, the range is from 0...15. Level 1 is for normal user EXEC mode privileges.

- For *password*, specify a string from 1...25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.

  TIP Characters TAB, ?, $, +, and [are invalid characters for passwords.

  ```
  enable password level level password
  ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. Verify your entries.

   The first command provides the password and access level configuration. The second command provides the privilege level configuration.

```
show running-config
or
show privilege
```

6. (Optional) Save your entries in the configuration file.

```
copy running-config startup-config
```

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the `show ip route` command to level 15, the `show` commands and `show ip` commands are automatically set to privilege level 15 unless you set them individually to different levels.

To return to the default privilege for a given command, use the `no privilege` *`mode`* `level` *`level command`* global configuration command.

This example shows how to set the `configure` command to privilege level 14 and define *`SecretPswd14`* as the password users must enter to use level 14 commands:

```
AP(config)# privilege exec level 14 configure
AP(config)# enable password level 14 SecretPswd14
```

Log Into and Exiting a Privilege Level

Beginning in privileged EXEC mode, follow these steps to log in to a specified privilege level and to exit to a specified privilege level:

1. Log in to a specified privilege level.

   For *level*, the range is 0...15.

   ```
   enable level
   ```

2. Exit to a specified privilege level.

   For *level*, the range is 0...15.

   ```
   disable level
   ```

Control Access Point Access with RADIUS

This section describes how to control administrator access to the wireless device by using Remote Authentication Dial-In User Service (RADIUS). For complete instructions on configuring the wireless device to support RADIUS, see Configure RADIUS and TACACS+ Servers on page 373.

RADIUS provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS is facilitated through AAA and can be enabled only through AAA commands.

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Security Command Reference for Release 12.3.

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

To prevent a lapse in security, you cannot configure RADIUS through a network management application by using SNMP. When enabled, RADIUS can authenticate users accessing the wireless device through CLI or HTTP (Device Manager).

Configure RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication and sequence to be performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list. The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a back-up system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list.

This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable AAA.

   ```
   aaa new-model
   ```

3. Create a login authentication method list.

   ```
   aaa authentication login {default | list-name}
   method1 [method2...]
   ```

   - To create a default list that is used when a named list is not specified in the `login authentication` command, use the `default` keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.

- For *list-name*, specify a character string to name the list you are creating.
- For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Choose one of these methods:

- `local`

  Use the local username database for authentication. You must enter username information in the database. Use the `username password` global configuration command.
- `radius`

  Use RADIUS authentication. You must configure the RADIUS server before you can use this authentication method. For more information, see Identify the RADIUS Server Host on page 376.

4. Enter line configuration mode and apply the authentication list.

   ```
   line [console | tty | vty] line-number [ending-line-number]
   ```

5. Apply the authentication list to a line or set of lines.
   - If you specify `default`, use the default list created with the `aaa authentication login` command.
   - For *list-name*, specify the list created with the `aaa authentication login` command.

   ```
   login authentication {default | list-name}
   ```

6. Return to privileged EXEC mode.

   ```
   end
   ```

7. Verify your entries.

   ```
   show running-config
   ```

8. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

- To disable AAA, use the `no aaa new-model` global configuration command.
- To disable AAA authentication, use the `no aaa authentication login {default | list-name} method1 [method2...]` global configuration command.
- To either disable RADIUS authentication for logins or to return to the default value, use the `no login authentication {default | list-name}` line configuration command.

Define AAA Server Groups

You can configure the wireless device to use AAA server groups to group existing server hosts for authentication. You choose a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, that lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), letting different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service (such as accounting), the second configured host entry acts as a fail-over backup to the first one.

You use the `server` group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional `auth-port` and `acct-port` keywords.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable AAA.

   ```
   aaa new-model
   ```

3. Specify the IP address or host name of the remote RADIUS server host.

   `radius-server host {`*`hostname`* `|` *`ip-address`*`} [auth-port` *`port-number`*`] [acct-port` *`port-number`*`] [timeout` *`seconds`*`] [retransmit` *`retries`*`] [key` *`string`*`]`

   - (Optional) For `auth-port` *`port-number`*, specify the UDP destination port for authentication requests.
   - (Optional) For `acct-port` *`port-number`*, specify the UDP destination port for accounting requests.
   - (Optional) For `timeout` *`seconds`*, specify the time interval that the wireless device waits for the RADIUS server to reply before retransmitting. The range is 1...1000. This setting overrides the `radius-server timeout` global configuration command setting. If no timeout is set with the `radius-server host` command, the setting of the `radius-server timeout` command is used.
   - (Optional) For `retransmit` *`retries`*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1...1000. If no retransmit value is set with the `radius-server host` command, the setting of the `radius-server retransmit` global configuration command is used.

- (Optional) For `key string`, specify the authentication and encryption key used between the wireless device and the RADIUS daemon running on the RADIUS server.

  TIP The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, don't enclose the key in quotation marks unless the quotation marks are part of the key.

To configure the wireless device to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The wireless device software searches for hosts in the order that you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.

4. Define the AAA server-group with a group name.

   This command puts the wireless device in a server group configuration mode.

   `aaa group server radius group-name`

5. Associate a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group.

   Each server in the group must be previously defined in Step 2.

   `server ip-address`

6. Return to privileged EXEC mode.

   `end`

7. Verify your entries.

   `show running-config`

8. (Optional) Save your entries in the configuration file.

   `copy running-config startup-config`

9. Enable RADIUS login authentication.

   See Configure RADIUS Login Authentication on page 220 for more information.

   - To remove the specified RADIUS server, use the `no radius-server host hostname | ip-address` global configuration command.
   - To remove a server group from the configuration list, use the `no aaa group server radius group-name` global configuration command.
   - To remove the IP address of a RADIUS server, use the `no server ip-address` server group configuration command.

In this example, the wireless device is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```
AP(config)# aaa new-model

AP(config)# radius-server host 172.20.0.1 auth-port
1000 acct-port 1001

AP(config)# radius-server host 172.10.0.1 auth-port
1645 acct-port 1646

AP(config)# aaa group server radius group1

AP(config-sg-radius)# server 172.20.0.1 auth-port
1000 acct-port 1001

AP(config-sg-radius)# exit

AP(config)# aaa group server radius group2

AP(config-sg-radius)# server 172.20.0.1 auth-port
2000 acct-port 2001

AP(config-sg-radius)# exit
```

Configure RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the wireless device uses information retrieved from the user profile, that is in the local user database or on the security server, to configure the user session. The user is granted access only to a requested service if the information in the user profile permits it.

You can use the `aaa authorization` global configuration command with the `radius` keyword to set parameters that restrict a user network access to privileged EXEC mode.

The `aaa authorization exec radius local` command sets these authorization parameters.

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

TIP Authorization is bypassed for authenticated users who log in through CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services:

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Configure the wireless device for user RADIUS authorization for all network-related service requests.

   ```
   aaa authorization network radius
   ```

3. Configure the wireless device for user RADIUS authorization to determine if the user has privileged EXEC access.

   The `exec` keyword can return user profile information (such as `autocommand` information).

   ```
   aaa authorization exec radius
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. Verify your entries.

   ```
   show running-config
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

   To disable authorization, use the `no aaa authorization {network | exec}` *`method1`* global configuration command.

Display the RADIUS Configuration

To display the RADIUS configuration, use the `show running-config` privileged EXEC command.

Control Access Point Access with TACACS+

This section describes how to control administrator access to the wireless device by using Terminal Access Controller Access Control System Plus (TACACS+).

For complete instructions on configuring the wireless device to support TACACS+, see Configure RADIUS and TACACS+ Servers on page 373.

TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through AAA and can be enabled only through AAA commands.

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Security Command Reference for Release 12.3.

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application by using SNMP. When enabled, TACACS+ can authenticate administrators accessing the wireless device through CLI or HTTP (Device Manager).

Configure TACACS+ Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication that is performed and the sequence that they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed.

The only exception is the default method list. The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a back-up system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails, the software selects the next authentication method in the method list.

This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

1. Enter global configuration mode.

   `configure terminal`

2. Enable AAA.

   `aaa new-model`

3. Create a login authentication method list.

   `aaa authentication login {default | list-name} method1 [method2...]`

- To create a default list that is used when a named list is **not** specified in the `login authentication` command, use the `default` keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.

- For *`list-name`*, specify a character string to name the list you are creating.

- For *`method1`*..., specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Choose one of these methods:

- `local`

  Use the local username database for authentication. You must enter username information into the database. Use the `username` *`password`* global configuration command.

- `tacacs+`

  Use TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method.

4. Enter line configuration mode and apply the authentication list.

   `line [console | tty | vty] line-number [ending-line-number]`

5. Apply the authentication list to a line or set of lines.
   - If you specify `default`, use the default list created with the `aaa authentication login` command.
   - For *list-name*, specify the list created with the `aaa authentication login` command.

   `login authentication {default | list-name}`

6. Return to privileged EXEC mode.

   `end`

7. Verify your entries.

   `show running-config`

8. (Optional) Save your entries in the configuration file.

   `copy running-config startup-config`

- To disable AAA, use the `no aaa new-model` global configuration command.
- To disable AAA authentication, use the `no aaa authentication login {default | list-name} method1 [method2...]` global configuration command.
- To either disable TACACS+ authentication for logins or to return to the default value, use the `no login authentication {default | list-name}` line configuration command.

Configure TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the wireless device uses information retrieved from the user profile, that is either in the local user database or on the security server, to configure the user session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the `aaa authorization` global configuration command with the `tacacs+` keyword to set parameters that restrict a user network access to privileged EXEC mode.

The `aaa authorization exec tacacs+ local` command sets these authorization parameters:

- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

TIP Authorization is bypassed for authenticated users who log in through CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for privileged EXEC access and network services.

1. Enter global configuration mode.

   `configure terminal`

2. Configure the wireless device for user TACACS+ authorization for all network-related service requests.

   `aaa authorization network tacacs+`

3. Configure the wireless device for user TACACS+ authorization to determine if the user has privileged EXEC access.

   The `exec` keyword can return user profile information (such as `autocommand` information).

   ```
   aaa authorization exec tacacs+
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. Verify your entries.

   ```
   show running-config
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

To disable authorization, use the `no aaa authorization {network | exec}` *`method1`* global configuration command.

Display the TACACS+ Configuration

To display TACACS+ server statistics, use the `show tacacs` privileged EXEC command.

Configure Ethernet Speed and Duplex Settings

You can assign the wireless device Ethernet port speed and duplex settings. We recommend that you use `auto`, the default setting, for both the speed and duplex settings on the wireless device Ethernet port. When the wireless device receives inline power from a switch, any change in the speed or duplex settings that resets the Ethernet link restarts the wireless device.

If the switch port that the wireless device is connected to is not set to `auto`, you can change the wireless device port to `half` or `full` to correct a duplex mismatch and the Ethernet link is not reset. However, if you change from `half` or `full` back to `auto`, the link is reset and, if the wireless device receives inline power from a switch, the wireless device restarts.

IMPORTANT The speed and duplex settings on the wireless device Ethernet port must match the Ethernet settings on the port where the wireless device is connected.

If you change the settings on the port where the wireless device is connected, change the settings on the wireless device Ethernet port to match.

The Ethernet speed and duplex are set to `auto` by default. Beginning in privileged EXEC mode, follow these steps to configure Ethernet speed and duplex.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter configuration interface mode.

   ```
   interface gigabitEthernet0
   ```

3. Configure the Ethernet speed. We recommend that you use `auto`, the default setting.

   ```
   speed {10 | 100 | 1000 | auto}
   ```

4. Configure the duplex setting. We recommend that you use `auto`, the default setting.

   ```
   duplex {auto | full | half}
   ```

5. Return to privileged EXEC mode.

   ```
   end
   ```

6. Verify your entries.

   ```
   show running-config
   ```

7. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Configure the Access Point for Local Authentication and Authorization

You can configure AAA to operate without a server by configuring the wireless device to implement AAA in local mode. The wireless device then handles authentication and authorization. No accounting is available in this configuration.

TIP You can configure the wireless device as a local authenticator for 802.1x-enabled client devices to provide a back-up for your main server or to provide authentication service on a network without a RADIUS server.

See Configure an Access Point as a Local Authenticator on page 303 for detailed instructions on configuring the wireless device as a local authenticator.

Beginning in privileged EXEC mode, follow these steps to configure the wireless device for local AAA.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable AAA.

   ```
   aaa new-model
   ```

3. Set the login authentication to use the local username database.

The `default` keyword applies the local user database authentication to all interfaces.

```
aaa authentication login default local
```

4. Configure user AAA authorization to determine if the user is allowed to run an EXEC shell by checking the local database.

   ```
   aaa authorization exec local
   ```

5. Configure user AAA authorization for all service requests that are network related.

   ```
   aaa authorization network local
   ```

6. Enter the local database, and establish an authentication system based on the username.

   Repeat this command for each user.

   - For *name*, specify the user ID as one word. Spaces and quotation marks are not allowed.
   - (Optional) For *level*, specify the privilege level the user has after gaining access. The range is 0...15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access.
   - For *encryption-type*, enter `0` to specify that an unencrypted password follows. Enter **7** to specify that a hidden password follows.
   - For *password*, specify the password the user must enter to gain access to the wireless device. The password must be from 1...25 characters, can contain embedded spaces, and must be the last option specified in the `username` command.

     TIP Characters TAB, ?, $, +, and [are invalid characters for passwords.

   ```
   username name [privilege level] {password
   encryption-type password}
   ```

7. Return to privileged EXEC mode.

   ```
   end
   ```

8. Verify your entries.

   ```
   show running-config
   ```

9. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

To disable AAA, use the `no aaa new-model` global configuration command. To disable authorization, use the `no aaa authorization {network | exec} method1` global configuration command.

Configure the Authentication Cache and Profile

The authentication cache and profile feature allows the access point to cache the authentication/authorization responses for a user so that subsequent authentication/authorization requests don't need to be sent to the AAA server.

TIP On the access point, this feature is supported only for Admin authentication.

The following commands that support this feature are in the Cisco IOS Release 12.3(7) and later:

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```

For a list of Cisco IOS commands CLI, see the Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Guide.

The following is a configuration example from an access point configured for Admin authentication by using TACACS+ with the auth cache enabled. While this example is based on a TACACS server, the access point can be configured for Admin authentication by using RADIUS:

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
username Cisco password 7 123A0C041104
username admin privilege 15 password 7
01030717481C091D25
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.134.229 auth-port 1645 acct-port
1646
!
aaa group server radius rad_mac
server 192.168.134.229 auth-port 1645 acct-port
1646
!
aaa group server radius rad_acct
server 192.168.134.229 auth-port 1645 acct-port
1646
!
aaa group server radius rad_admin
server 192.168.134.229 auth-port 1645 acct-port
1646
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server tacacs+ tac_admin
server 192.168.133.231
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local cache
tac_admin group tac_admin
aaa authentication login eap_methods group rad_eap
```

```
aaa authentication login mac_methods local
aaa authorization exec default local cache
tac_admin group tac_admin
aaa accounting network acct_methods start-stop
group rad_acct
aaa cache profile admin_cache
all
!
aaa session-id common
!
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-
11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 192.168.133.207 255.255.255.0
no ip route-cache
```

```
!
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/
779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
tacacs-server host 192.168.133.231 key 7
105E080A16001D1908
tacacs-server directed-request
radius-server attribute 32 include-in-access-req
format %h
radius-server host 192.168.134.229 auth-port 1645
acct-port 1646 key 7 111918160405041E00
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
transport preferred all
transport output all
line vty 0 4
transport preferred all
transport input all
transport output all
line vty 5 15
transport preferred all
transport input all
transport output all
!
end
```

Configure the Access Point to Provide DHCP Service

By default, access points are configured to receive IP settings from a DHCP server on your network. You can also configure an access point to act as a DHCP server to assign IP settings to devices on both your wired and wireless LANs.

TIP When you configure the access point as a DHCP server, it assigns IP addresses to devices on its subnet. The devices communicate with other devices on the subnet but not beyond it. If data needs to be passed beyond the subnet, you must assign a default router. The IP address of the default router must be on the same subnet as the access point configured as the DHCP server.

For detailed information on commands related to DHCP commands and options, see Configuring DHCP in the Cisco IOS IP Configuration Guide, Release 12.3.

Set up the DHCP Server

Beginning in privileged EXEC mode, follow these steps to configure an access point to provide DHCP service and specify a default router.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Exclude the wireless device IP address from the range of addresses the wireless device assigns. Enter the IP address in four groups of characters, such as 10.91.6.158.

   The wireless device assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients. You must specify the IP addresses that the DHCP Server must not assign to clients.

   (Optional) To enter a range of excluded addresses, enter the address at the low end of the range followed by the address at the high end of the range.

   ```
   ip dhcp excluded-address low_address [ high_address ]
   ```

3. Create a name for the pool of IP addresses that the wireless device assigns in response to DHCP requests, and enter DHCP configuration mode.

   ```
   ip dhcp pool pool_name
   ```

4. Assign the subnet number for the address pool. The wireless device assigns IP addresses within this subnet.

   (Optional) Assign a subnet mask for the address pool, or specify the number of bits that comprise the address prefix. The prefix is an alternative way of assigning the network mask. The prefix length must be preceded by a forward slash (/).

   ```
   network subnet_number
   [ mask | prefix-length ]
   ```

5. Configure the duration of the lease for IP addresses assigned by the wireless device.
   - days, configure the lease duration in number of days
   - (optional) hours, configure the lease duration in number of hours
   - (optional) minutes, configure the lease duration in number of minutes
   - infinite, set the lease duration to infinite

   ```
   lease { days [ hours ] [ minutes ] |
   infinite }
   ```

6. Specify the IP address of the default router for DHCP clients on the subnet. One IP address is required; however, you can specify up to eight addresses in one command line.

   ```
   default-router address [address2 ... address 8]
   ```

7. Return to privileged EXEC mode.

   ```
   end
   ```

8. Verify your entries.

   ```
   show running-config
   ```

9. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the no form of these commands to return to default settings.

This example shows how to configure the wireless device as a DHCP server, exclude a range of IP address, and assign a default router:

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 172.16.1.1
172.16.1.20
AP(config)# ip dhcp pool wishbone
AP(dhcp-config)# network 172.16.1.0 255.255.255.0
AP(dhcp-config)# lease 10
AP(dhcp-config)# default-router 172.16.1.1
AP(dhcp-config)# end
```

Monitor and Maintain the DHCP Server Access Point

You can use `show` and `clear` commands to monitor and maintain the DHCP server access point.

Show Commands

In Exec mode, enter the commands in this table to display information about the wireless device as DHCP server.

Table 90 - Show Commands for DHCP Server

Command	Purpose
`show ip dhcp conflict [ address ]`	Provides a list of all address conflicts recorded by a specific DHCP Server. Enter the wireless device IP address to show conflicts recorded by the wireless device.
`show ip dhcp database [ url ]`	Provides recent activity on the DHCP database. Use this command in privileged EXEC mode.
`show ip dhcp server statistics`	Provides count information about server statistics and messages sent and received.

Clear Commands

In privileged Exec mode, use the commands in this table to clear DHCP server variables.

Table 91 - Clear Commands for DHCP Server

Command	Purpose
`clear ip dhcp binding { address | * }`	Deletes an automatic address binding from the DHCP database. Specifying the address argument clears the automatic binding for a specific (client) IP address. Specifying an asterisk (*) clears all automatic bindings.
`clear ip dhcp conflict { address | * }`	Clears an address conflict from the DHCP database. Specifying the address argument clears the conflict for a specific IP address. Specifying an asterisk (*) clears conflicts for all addresses.
`clear ip dhcp server statistics`	Resets all DHCP Server counters to 0.

Debug Command

To enable DHCP server debugging, use this command in privileged EXEC mode:

```
debug ip dhcp server { events | packets | linkage }
```

Use the `no` form of the command to disable debugging for the wireless device DHCP server.

Configure the Access Point for Secure Shell

This section describes how to configure the Secure Shell (SSH) feature.

For complete syntax and usage information for the commands used in this section, see Secure Shell Commands in Cisco IOS Security Command Reference for Release 12.3

Understand SSH

SSH is a protocol that provides a secure, remote connection to a Layer 2 or a Layer 3 device. There are two versions of SSH: SSH version 1 and SSH version 2. This software release supports both SSH versions. If you don't specify the version number, the access point defaults to version 2.

SSH provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. The SSH feature has an SSH server and an SSH integrated client. The client supports these user authentication methods:

- RADIUS

  See Control Access Point Access with RADIUS on page 219.

- Local authentication and authorization

  See the Configure the Access Point for Local Authentication and Authorization on page 230.

Configure SSH

For complete information about configuring SSH and displaying SSH settings, see these publications:

- Cisco IOS Security Configuration Guide for Release 12.3
- Configuring Secure Shell on Routers and Switches Running Cisco IOS

Configure Client ARP Caching

You can configure the wireless device to maintain an ARP cache for associated client devices. Maintaining an ARP cache on the wireless device reduces the traffic load on your wireless LAN. ARP caching is disabled by default.

ARP caching on the wireless device reduces the traffic on your wireless LAN by stopping ARP requests for client devices at the wireless device. Instead of forwarding ARP requests to client devices, the wireless device responds to requests on behalf of associated client devices.

When ARP caching is disabled, the wireless device forwards all ARP requests through the radio port to associated clients, and the client responds. When ARP caching is enabled, the wireless device responds to ARP requests for associated clients and does not forward requests to clients. When the wireless device receives an ARP request for an IP address not in the cache, the wireless device drops the request and does not forward it. In its beacon, the wireless device includes an information element to alert client devices that they can safely ignore broadcast messages to increase battery life.

Optional ARP Caching

If a client device is associated to an access point in not a Cisco device and is not passing data, the wireless device does not know the client IP address. If this situation occurs frequently on your wireless LAN, you can enable optional ARP caching. When ARP caching is optional, the wireless device responds on behalf of clients with IP addresses known to the wireless device but forwards out its radio port any ARP requests addressed to unknown clients. When the wireless device learns the IP addresses for all associated clients, it drops ARP requests not directed to its associated clients.

Configure ARP Caching

Beginning in privileged EXEC mode, follow these steps to configure the wireless device to maintain an ARP cache for associated clients:

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable ARP caching on the wireless device.
   - (Optional) Use the `optional` keyword to enable ARP caching only for the client devices whose IP addresses are known to the wireless device.

   ```
   dot11 arp-cache [ optional ]
   ```

3. Return to privileged EXEC mode.

   ```
   end
   ```

4. Verify your entries.

   ```
   show running-config
   ```

5. (Optional) Save your entries in the configuration file.

```
copy running-config startup-config
```

This example shows how to configure ARP caching on an access point:

```
AP# configure terminal
AP(config)# dot11 arp-cache
AP(config)# end
```

Manage the System Time and Date

You can manage the system time and date on the wireless device automatically, by using the Simple Network Time Protocol (SNTP), or manually, by setting the time and date on the wireless device.

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Configuration Fundamentals Command Reference and the Cisco IOS IP and IP Routing Command Reference.

Simple Network Time Protocol (SNTP) is a simplified, client-only version of NTP. SNTP can only receive the time from NTP servers; it cannot be used to provide time services to other systems. SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP.

You can configure SNTP to request and accept packets from configured servers or to accept NTP broadcast packets from any source. When multiple sources are sending NTP packets, the server with the best stratum is selected.

If multiple servers are at the same stratum, a configured server is preferred over a broadcast server. If multiple servers pass both tests, the first one to send a time packet is selected. SNTP chooses only a new server if it stops receiving packets from the currently selected server, or if a better server (according to the above criteria) is discovered.

Configure SNTP

SNTP is disabled by default. To enable SNTP on the access point, use one or both of these commands in global configuration mode:

Table 92 - SNTP Commands

Command	Purpose
`sntp server {address | hostname} [version number]`	Configures SNTP to request NTP packets from an NTP server.
`sntp broadcast client`	Configures SNTP to accept NTP packets from any NTP broadcast server.

Enter the `sntp server` command once for each NTP server. The NTP servers must be configured to respond to the SNTP messages from the access point.

If you enter both the `sntp server` command and the `sntp broadcast client` command, the access point accepts time from a broadcast server but prefers time from a configured server, assuming the strata are equal. To display information about SNTP, use the `show sntp` EXEC command.

Configure Time and Date Manually

If no other source of time is available, you can manually configure the time and date after the system is restarted. The time remains accurate until the next system restart. We recommend that you use manual configuration only as a last resort. If you have an outside source that the wireless device can synchronize to, you don't need to manually set the system clock.

Set the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you don't need to manually set the system clock.

Beginning in privileged EXEC mode, follow these steps to set the system clock.

1. Manually set the system clock by using one of these formats:
   - For `hh:mm:ss`, specify the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone.
   - For `day`, specify the day by date in the month.
   - For `month`, specify the month by name.
   - For `year`, specify the year (no abbreviation).

   `clock set hh:mm:ss day month year`

   or

   `clock set hh:mm:ss month day year`

2. Verify your entries.

   ```
   show running-config
   ```

3. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

This example shows how to manually set the system clock to 1:32 p.m. on July 23, 2001.

```
AP# clock set 13:32:00 23 July 2001
```

Display the Time and Date Configuration

To display the time and date configuration, use the `show clock [detail]` privileged EXEC command.

The system clock keeps an authoritative flag that shows whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source such as NTP, the flag is set. If the time is not authoritative, it is used only for display purposes. Until the clock is authoritative and the authoritative flag is set, the flag prevents peers from synchronizing to the clock when the peers' time is invalid.

The symbol that precedes the `show clock` display has this meaning:

- * Time is not authoritative.
- (blank) Time is authoritative.
- . Time is authoritative, but NTP is not synchronized.

Configure the Time Zone

Beginning in privileged EXEC mode, follow these steps to manually configure the time zone.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Set the time zone.

   The wireless device keeps internal time in universal time coordinated (UTC), so this command is used only for display purposes and when the time is manually set.

   - For *`zone`*, enter the name of the time zone to be displayed when standard time is in effect. The default is UTC.
   - For *`hours-offset`*, enter the hours offset from UTC.
   - (Optional) For *`minutes-offset`*, enter the minutes offset from UTC.

   ```
   clock timezone zone hours-offset [minutes-offset]
   ```

3. Return to privileged EXEC mode.

   `end`

4. Verify your entries.

   `show running-config`

5. (Optional) Save your entries in the configuration file.

   `copy running-config startup-config`

The *`minutes-offset`* variable in the `clock timezone` global configuration command is available for those cases where a local time zone is a percentage of an hour different from UTC. For example, the time zone for some sections of Atlantic Canada (AST) is UTC-3.5, where the 3 means 3 hours .5 means 50 percent. In this case, the necessary command is:

```
clock timezone AST -3 30.
```

To set the time to UTC, use the `no clock timezone` global configuration command.

Configure Summer Time (Daylight Saving Time)

Beginning in privileged EXEC mode, follow these steps to configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year.

1. Enter global configuration mode.

   `configure terminal`

2. Configure summer time to start and end on the specified days every year.

   Summer time is disabled by default. If you specify `clock summer-time` *`zone`* `recurring` without parameters, the summer time rules default to the United States rules.

- For *`zone`*, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect.
- (Optional) For *`week`*, specify the week of the month (1...5 or last).
- (Optional) For *`day`*, specify the day of the week (Sunday, Monday...).
- (Optional) For *`month`*, specify the month (January, February...).
- (Optional) For *`hh:mm`*, specify the time (24-hour format) in hours and minutes.
- (Optional) For *`offset`*, specify the number of minutes to add during summer time. The default is 60.

  `clock summer-time` *`zone`* `recurring [`*`week day month hh`*`:`*`mm week day month hh`*`:`*`mm`* `[`*`offset`*`]]`

3. Return to privileged EXEC mode.

   `end`

4. Verify your entries.

   ```
   show running-config
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

The first part of the `clock summer-time` global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

This example shows how to specify that summer time starts on the first Sunday in April at 02:00 and ends on the last Sunday in October at 02:00:

```
AP(config)# clock summer-time PDT recurring 1
Sunday April 2:00 last Sunday October 2:00
```

Beginning in privileged EXEC mode, follow these steps if summer time in your area does not follow a recurring pattern (configure the exact date and time of the next summer time events).

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Configure summer time to start on the first date and end on the second date.

   Summer time is disabled by default.

   - For *zone*, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect.
   - (Optional) For *week*, specify the week of the month (1...5 or last).
   - (Optional) For *day*, specify the day of the week (Sunday, Monday...).
   - (Optional) For *month*, specify the month (January, February...).
   - (Optional) For *hh*:*mm*, specify the time (24-hour format) in hours and minutes.
   - (Optional) For *offset*, specify the number of minutes to add during summer time. The default is 60.

   ```
   clock summer-time zone date [month date year hh:mm
   month date year hh:mm [offset]]
   ```

   or

   ```
   clock summer-time zone date [date month year hh:mm
   date month year hh:mm [offset]]
   ```

3. Return to privileged EXEC mode.

   ```
   end
   ```

4. Verify your entries.

   ```
   show running-config
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

The first part of the `clock summer-time` global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

To disable summer time, use the `no clock summer-time` global configuration command.

This example shows how to set summer time to start on October 12, 2000, at 02:00, and end on April 26, 2001, at 02:00:

```
AP(config)# clock summer-time pdt date 12 October
2000 2:00 26 April 2001 2:00
```

Define HTTP Access

By default, 80 is used for HTTP access, and port 443 is used for HTTPS access. These values can be customized by the user.

Use these commands to define the HTTP access.

```
ip http port <port number>
ip http secure-port <port number>
```

Configure a System Name and Prompt

You configure the system name on the wireless device to identify it. By default, the system name and prompt are `ap`.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol (>) is appended. The prompt is updated whenever the system name changes, unless you manually configure the prompt by using the `prompt` global configuration command.

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Configuration Fundamentals Command Reference and the Cisco IOS IP and IP Routing Command Reference.

Default System Name and Prompt Configuration

The default access point system name and prompt is `ap`.

Configure a System Name

Beginning in privileged EXEC mode, follow these steps to manually configure a system name.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Manually configure a system name.

   The default setting is `ap`.

   ATTENTION: When you change the system name, the wireless device radios reset, and associated client devices disassociate and quickly reassociate.

   You can enter up to 63 characters for the system name. However, when the wireless device identifies itself to client devices, it uses only the first 15 characters in the system name. If it is important for client users to distinguish between access points, make sure a unique portion of the system name appears in the first 15 characters.

   ```
   hostname name
   ```

3. Return to privileged EXEC mode.

   ```
   end
   ```

4. Verify your entries.

   ```
   show running-config
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

When you set the system name, it is also used as the system prompt.

To return to the default host name, use the `no hostname` global configuration command.

Understand DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database where you can map host names to IP addresses. When you configure DNS on the wireless device, you can substitute the host name for the IP address with all IP commands, such as `ping, telnet, connect`, and related Telnet support operations.

IP defines a hierarchical naming scheme that lets a device be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a com domain name, so its domain name is reckwellautomation.com. A specific device in this domain, such as the File Transfer Protocol (FTP) system, is identified as ftp.cisco.com.

To keep track of domain names, IP has defined the concept of a domain name server, that holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names, specify the name server that is present on your network, and enable the DNS.

Default DNS Configuration

This table shows the default DNS configuration.

Table 93 - Default DNS Configuration

Feature	Default Setting
DNS enable state	Disabled.
DNS default domain name	None configured.
DNS servers	No name server addresses are configured.

Set Up DNS

Beginning in privileged EXEC mode, follow these steps to set up the wireless device to use the DNS.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Define a default domain name that the software uses to complete unqualified host names (names without a dotted-decimal domain name).

   Don't include the initial period that separates an unqualified name from the domain name.

   At start up, no domain name is configured; however, if the wireless device configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name can be set by the BOOTP or DHCP server (if the servers were configured with this information).

   ```
   ip domain-name name
   ```

3. Specify the address of one or more name servers to use for name and address resolution.

   You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The wireless device sends DNS queries to the primary server first. If that query fails, the back-up servers are queried.

   `ip name-server server-address1 [server-address2 ... server-address6]`

   (Optional) Enable DNS-based host name-to-address translation on the wireless device. This feature is enabled by default.

   If your network devices require connectivity with devices in networks that you don't control name assignment for, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).

   `ip domain-lookup`

4. Return to privileged EXEC mode.

   `end`

5. Verify your entries.

   `show running-config`

   (Optional) Save your entries in the configuration file.

   `copy running-config startup-config`

If you use the wireless device IP address as its host name, the IP address is used and no DNS query occurs. If you configure a host name that contains no periods (.), a period followed by the default domain name is appended to the host name before the DNS query is made to map the name to an IP address.

The default domain name is the value set by the `ip domain-name` global configuration command. If there is a period (.) in the host name, Cisco IOS software looks up the IP address without appending any default domain name to the host name.

- To remove a domain name, use the `no ip domain-name name` global configuration command.
- To remove a name server address, `use the no ip name-server server-address` global configuration command.
- To disable DNS on the wireless device, use the `no ip domain-lookup` global configuration command.

Display the DNS Configuration

To display the DNS configuration information, use the `show running-config` privileged EXEC command. When DNS is configured on the wireless device, the `show running-config` command sometimes a server IP address appears instead of its name.

Configure Radio Settings

This chapter describes how to configure radio settings for the wireless access point.

Topic	Page
Enable the Radio Interface	252
Configure the Role in Radio Network	252
Universal Workgroup Bridge Mode	254
Radio Tracking	255
Configure Radio Data Rates	256
Access Points Send Multicast and Management Frames at Highest Basic Rate	257
Configure MCS Rates	260
Configure Radio Transmit Power	262
Configure Radio Channel Settings	264
Configure Transmit and Receive Antennas	271
Enable and Disable Gratuitous Probe Response	272
Disable and Enable Aironet Extensions	273
Configure the Ethernet Encapsulation Transformation Method	274
Enable and Disable Reliable Multicast to Workgroup Bridges	275
Enable and Disable Public Secure Packet Forwarding	277
Configure the Beacon Period and the DTIM	277
Configure RTS Threshold and Retries	279
Configure the Maximum Data Retries	280
Configuring the Fragmentation Threshold	280
Perform a Carrier Busy Test	282
Configure ClientLink	282
Debug Radio Functions	283

Enable the Radio Interface

The wireless access point radios are disabled by default.

IMPORTANT There is no default SSID in the Stratix 5100 out-of-box configuration. You must create an SSID before you can enable the radio interface.

Beginning in privileged EXEC mode, follow these steps to enable the access point radio.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter the SSID.

   The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.

   ```
   dot11 ssid ssid
   ```

3. Enter interface configuration mode for the radio interface.

   ```
   interface dot11radio {0 | 1}
   ```

   - The 802.11n 2.4 GHz radio is radio 0.
   - The 802.11n 5 GHz radio is radio 1.

4. Assign the SSID you created in Step 2 to the appropriate radio interface.

   ```
   ssid ssid
   ```

5. Enable the radio port.

   ```
   no shutdown
   ```

6. Return to privileged EXEC mode.

   ```
   end
   ```

7. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

   Use the shutdown command to disable the radio port.

Configure the Role in Radio Network

The Stratix 5100 Wireless Access Point/Workgroup Bridge has these roles in the radio network.

- Access point
- Access point (fallback to radio shutdown)
- Access point (fallback to repeater)
- Workgroup bridge
- Repeater
- Root bridge
- Non-root bridge
- Root bridge with wireless clients
- Non-root bridge with wireless clients
- Universal workgroup bridge
- Scanner

You can configure a fallback role also for root access points. The wireless device automatically assumes the fallback role when its Ethernet port is disabled or disconnected from the wired LAN. There are two possible fallback roles:

- Repeater

  When the Ethernet port is disabled, the wireless device becomes a repeater and associates to a nearby root access point. You do not have to specify a root access point to which the fallback repeater associates; the repeater automatically associates to the root access point that provides the best radio connectivity.

- Shutdown

  The wireless access point/workgroup bridge shuts down its radio and disassociates all client devices.

Beginning in privileged EXEC mode, follow these steps to set the wireless device radio network role and fallback role.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.
   - The 802.11n 2.4-Ghz radio is interface 0.
   - The 802.11n 5-GHz radio is interface 1.

   ```
   interface dot11radio { 0 | 1 }
   ```

3. Set the wireless device role.
   - Set the role to root access point, workgroup bridge, or non-root bridge with or without wireless clients, repeater access point, or scanner. The bridge mode radio supports point-to-point and point-to-multipoint configuration.
   - The Ethernet port is shut down when any one of the radios is configured as a repeater. Only one radio per access point may be configured as a workgroup bridge or repeater.
   - The `dot11radio 0|1 antenna-alignment` command is available when the access point is configured as a repeater.
   - (Optional) Select the root access point fallback role. If the wireless device Ethernet port is disabled or disconnected from the wired LAN, the wireless device can either shut down its radio port or become a repeater access point associated to any nearby root access point.

   ```
   station-role


   non-root {bridge | wireless-clients}


   repeater


   root {access-point | ap-only | [bridge  | wireless-
   clients] | [fallback | repeater | shutdown]}
   ```

```
scanner


workgroup-bridge {multicast | mode <client |
infrastructure>| universal <Ethernet client MAC
address>}
```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

TIP When you enable the role in the radio network as a Bridge/workgroup bridge and enable the interface using the no shut command, the physical status and the software status of the interface will be up only if the device on the other end access point or bridge is up. Otherwise, only the physical status of the device will be up. The software status of the device comes up only when the device on the other end is configured and up.

Universal Workgroup Bridge Mode

When configuring the universal workgroup bridge role, you must include the client MAC address. The workgroup bridge associates only with this MAC address if it is present in the bridge table and is not a static entry. If validation fails, the workgroup bridge associates with its BVI MAC address. In universal workgroup bridge mode, the workgroup bridge uses the Ethernet client MAC address to associate with Cisco or non-Cisco root devices. The universal workgroup bridge is transparent and is not managed.

IMPORTANT The universal workgroup bridge role supports only one wired client.

You can enable a recovery mechanism and make the workgroup bridge manageable again by disabling the Ethernet client, causing the universal workgroup bridge to associate with an access point by using its own BVI address.

Radio Tracking

You can configure the access point to track or monitor the status of one of its radios. It the tracked radio goes down or is disabled, the access point shuts down the other radio. If the tracked radio comes up, the access point enables the other radio.

- To track radio 0, enter the following command:

  ```
  # station-role root access-point fallback track d0
  shutdown
  ```

- To track radio 1, enter the following command:

  ```
  # station-role root access-point fallback track d1
  shutdown
  ```

Gigabit Ethernet Tracking

You can configure the access point for fallback when its Ethernet port is disabled or disconnected from the wired LAN.

TIP Gigabit Ethernet tracking does not support the Repeater mode.

Use this command to configure 802.11n access points for Gigabit Ethernet tracking in the radio interfaces configuration mode:

```
# station-role root fallback shutdown
```

MAC-Address Tracking

You can configure the radio whose role is root access point to go up or down by tracking a client access point, using its MAC address, on another radio. If the client disassociates from the access point, the root access point radio goes down. If the client reassociates to the access point, the root access point radio comes back up.

MAC-address tracking is most useful when the client is a non-root bridge access point connected to an upstream wired network.

For example, to track a client whose MAC address is 12:12:12:12:12:12, enter the following command:

```
# station-role root access-point fallback track
mac-address 12:12:12:12:12:12 shutdown
```

Configure Radio Data Rates

You use the data rate settings to choose the data rates the wireless access point uses for data transmission. The rates are expressed in megabits per second. The wireless access point always attempts to transmit at the highest data rate set enabled. If there are obstacles or interference, the wireless access point steps down to the highest rate that allows data transmission. You can set each data rate to one of three states:

- Basic (the GUI labels Basic rates as Required)

  Allows the transmission at this rate for all packets, both unicast and multicast. At least one of the wireless access point's data rates must be set to Basic.

- Enabled

  The wireless access point transmits only unicast packets at this rate; multicast packets are sent at one of the data rates set to Basic.

- Disabled

  The wireless access point does not transmit data at this rate.

TIP At least one data rate must be set to basic.

You can use the Data Rate settings to set an access point to serve client devices operating at specific data rates.

For example, to set the 2.4 GHz radio for 11 Mbps service only, set the 11 Mbps rate to Basic and set the other data rates to Disabled.

- To set the 2.4 GHz, 802.11g radio to serve only 802.11g client devices, set any Orthogonal Frequency Division Multiplexing (OFDM) data rate (6, 9, 12, 18, 24, 36, 48, 54) to Basic.

- To set only the 5 GHz radio for 54 Mbps service, set the 54 Mbps rate to Basic and set the other data rates to Disabled.

You can configure the wireless access point to set the data rates automatically to optimize either the range or the throughput. On the 2.4-GHz radio, the Range setting configures the 1.0 data rate to basic and the other data rates to supported. On the 5-GHz radio, the Range setting configures the 6.0 data rate to basic and the other data rates to supported.

The range setting lets the access point to extend the coverage area by compromising on the data rate. Therefore, if you have a client that is not able to connect to the access point while other clients can, one reason can be that the client is not within the coverage area of the access point. In such a case, the range option helps extend the coverage area and increases the ability of the client to connect to the access point.

However, allowing clients to communicate at the lowest data rate far from the AP can severely degrade performance for other clients.

TIP The range option is not recommended in most cases.

Typically the trade-off is between throughput and range. When the signal degrades (possibly due to distance from the access point,) the rates renegotiate down to maintain the link (but at a lower data rate). Contrast that against a link configured for a higher throughput that drops when the signal degrades enough to no longer sustain a configured high data rate, or roam to another access point with sufficient coverage, if one is available.

The balance between the two (throughput versus range) is one of those design decisions that has to be made based on resources available to the wireless project, for example:

- type of traffic the users pass
- service level desired
- the quality of the RF environment

When you enter throughput for the data rate setting, the wireless access point sets all data rates to basic.

Access Points Send Multicast and Management Frames at Highest Basic Rate

Access points running recent Cisco IOS versions are transmitting multicast and management frames at the highest configured basic rate, and is a situation that can cause reliability problems.

Because multicast frames are not retransmitted at the MAC layer, stations at the edge of the cell can fail to receive them successfully. If reliable reception is a goal,

then multicasts can be transmitted at a low data rate. If support for high data rate multicasts is required, then shrink the cell size and to disable all lower data rates.

Depending on your specific requirements, you can take the following action:

- If you need to transmit the multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, one that is low enough to reach the edges of the wireless cells.
- If you need to transmit the multicast data at a certain data rate to achieve a certain throughput, then configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of non-multicast clients.

Configuring Data Rates

Beginning in privileged EXEC mode, follow these steps to configure the radio data rates.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.

   The 2.4 GHz N radio is radio 0, and the 5 GHz N is radio 1.

   ```
   interface dot11radio {0 | 1}
   ```

3. Refer to Speed Command and Purpose descriptions.

Table 94 - Speed Command and Purpose Descriptions

Command	Purpose
`speed` **802.11n 2.4 GHz radio:** `{[1.0] [11.0] [12.0] [18.0] [2.0] [24.0] [36.0] [48.0] [5.5] [54.0] [6.0] [9.0] [basic-1.0] [basic-11.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-5.5] [basic-54.0] [basic-6.0] [basic-9.0] [default] [m0-7] [m0.] [m1.] [m10.] [m11.] [m12.] [m13.] [m14.] [m15.] [m2.] [m3.] [m4.] [m5.] [m6.] [m7.] [m8-15] [m8.] [m9.] [m16-23] [m16.] [m17.] [m18.] [m19.] [m20.] [m21.] [m22.] [m23.] [ofdm] [only-ofdm] | range | throughput}` **802.11n 5 GHz radio:** `{[12.0] [18.0] [24.0] [36.0] [48.0] [54.0] [6.0] [9.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-54.0] [basic-6.0] [basic-9.0] [default] [m0-7] [m0.] [m1.] [m10.] [m11.] [m12.] [m13.] [m14.] [m15.] [m2.] [m3.] [m4.] [m5.] [m6.] [m7.] [m8-15] [m8.] [m9.] [m16-23] [m16.] [m17.] [m18.] [m19.] [m20.] [m21.] [m22.] [m23.] | range | throughput}`	Set each data rate to basic or enabled, or enter range to optimize range or throughput to optimize throughput. Enter 1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, and 54.0 to set these data rates to enabled on the 802.11n 2.4 GHz radio. Enter 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, and 54.0 to set these data rates to enabled on the 5 GHz radio. To set these data rates to basic on the 802.11n, 2.4 GHz radio, enter the following: basic-1.0, basic-2.0, basic-5.5, basic-6.0, basic-9.0, basic-11.0, basic-12.0, basic-18.0, basic-24.0, basic-36.0, basic-48.0, and basic-54.0 **TIP** The client must support the basic rate that you select or it cannot associate to the wireless device. If you select 12 Mbps or higher for the basic data rate on the 802.11n radio, 802.11b client devices cannot associate to the wireless device 802.11n radio. To set these data rates to **basic** on the 5 GHz radio enter the following: basic-6.0, basic-9.0, basic-12.0, basic-18.0, basic-24.0, basic-36.0, basic-48.0, and basic-54.0. • (Optional) Enter range or throughput to automatically optimize radio range or throughput. When you enter range, the wireless access point sets the lowest data rate to basic and the other rates to enabled. When you enter throughput, the wireless access point sets all data rates to basic. • (Optional) On the 802.11n radio, enter speed throughput ofdm to set all OFDM rates (6, 9, 12, 18, 24, 36, and 48) to basic (required) and set all the CCK rates (1, 2, 5.5, and 11) to disabled. This setting disables 802.11b protection mechanisms and provides maximum throughput for802.11n clients. However, it prevents 802.11b clients from associating to the access point. • (Optional) Enter default to set the data rates to factory default settings – On the 802.11n 2.4 GHz radio, the default option sets rates 1.0, 2.0, 5.5, and 11.0 to enabled. – On the 802.11n 5 GHz radio, the default option sets rates to 6.0, 12.0, and 24.0 to enabled. The default MCS rate setting for both 802.11n radios is 0-23.

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the no form of the speed command to remove one or more data rates from the configuration. This example shows how to remove data rates basic-2.0 and basic-5.5 from the configuration:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# no speed basic-2.0 basic-5.5
ap1200(config-if)# end
```

Configure MCS Rates

Modulation Coding Scheme (MCS) is a specification of PHY parameters consisting of modulation order (BPSK, QPSK, 16-QAM, 64-QAM) and FEC code rate (1/2, 2/3, 3/4, 5/6). MCS is used in 802.11n radios, that define 32 symmetrical settings (8 per spatial stream):

- MCS 0–7
- MCS 8–15
- MCS 16–23
- MCS 24–31

MCS is an important setting because it provides for potentially greater throughput. High throughput data rates are a function of *MCS*, *bandwidth*, and *guard interval*. 802.11 a, b, and g radios use 20 MHz channel widths. This table shows the potential data rates based on MCS, guard interval, and channel width.

TIP The 2.4 GHz radios don't support 40 MHz channel width.

Table 95 - Data Rates Based on MCS Settings, Guard Interval, and Channel Width

MCS Index	Guard Interval = 800 ns		Guard Interval = 400 ns	
	20 Mhz Channel Width Data Rate (Mbps)	40 Mhz Channel Width Data Rate (Mbps)	20 Mhz Channel Width Data Rate (Mbps)	40 Mhz Channel Width Data Rate (Mbps)
0	6.5	13.5	7 2/9	15
1	13	27	14 4/9	30
2	19.5	40.5	21 2/3	45
3	26	54	28 8/9	60
4	39	81	43 1/3	90
5	52	109	57 5/9	120
6	58.5	121.5	65	135
7	65	135	72 2/9	152.5
8	13	27	14 4/9	30
9	26	54	28 8/9	60
10	39	81	43 1/3	90
11	52	108	57 7/9	120
12	78	162	86 2/3	180
13	104	216	115 5/9	240
14	117	243	130	270
15	130	270	144 4/9	300
16	19.5	40.5	21.7	45
17	39	81	43.3	90
18	58.5	121.5	65	135
19	78	162	86.7	180
20	117	243	130	270
21	156	324	173.3	360

Table 95 - Data Rates Based on MCS Settings, Guard Interval, and Channel Width (Continued)

MCS Index	Guard Interval = 800 ns		Guard Interval = 400 ns	
22	175.5	364.5	195	405
23	195	405	216.7	450
The legacy rates are: 5 GHz: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps 2.4 GHz: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps				

MCS rates are configured by using the speed command. The following example shows a speed setting for an 802.11n 5 GHz radio:

```
interface Dot11Radio0
   no ip address
   no ip route-cache
   !
   ssid 1250test
   !
   speed basic-1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0
   36.0 48.0 54.0 m0. m1. m2. m3. m4. m8. m9. m10. m11.
   m12. m13. m14. m15. m16. m17. m18. m19. m20. m21.
   m22. m23.
```

Configure Radio Transmit Power

Radio transmit power is based on the type of radio or radios installed in your access point and the regulatory domain where it operates.

Use this table to determine what transmit power, and the translation relationship between mW and dBm.

Table 96 - Translation Between mW and dBm

dBm	-1	2	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
mW	1	2	3	4	5	6	8	10	12	15	20	25	30	40	50	60	80	100	125	150	200	250

Beginning in privileged EXEC mode, follow these steps to set the transmit power on access point radios.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.

   The 2.4 GHz 802.11n radio is 0, and the 5 GHz 802.11n radio is 1.

   ```
   interface dot11radio {0 | 1}
   ```

3. Set the transmit power for the 2.4 GHz radio or the 5 GHz radio to one of the power levels allowed in your regulatory domain.

   ```
   power local
   ```

These options are available for the 2.4 GHz 802.11n radio (in dBM):

```
{ 4 | 7 | 10 | 13 | 16 | 19 | 22 }
```

These options are available for the 5 GHz 802.11n radio (in dBM):

```
{ 5 | 8 | 11 | 14 | 17 | 20 | 23 }
```

TIP Make sure the power settings match the settings for your regulatory domain.

TIP The 802.11g radio transmits at up to 100 mW for the 1, 2, 5.5, and 11 Mbps data rates. However, for the 6, 9, 12, 18, 24, 36, 48, and 54 Mbps data rates, the maximum transmit power for the 802.11g radio is 30 mW.

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the no form of the power command to return the power setting to maximum, the default setting.

Limit the Power Level for Associated Client Devices

You can also limit the power level on client devices that associate to the wireless access point. When a client device associates to the wireless access point, the wireless access point sends the maximum power level setting to the client.

TIP Cisco documentation uses the term Dynamic Power Control (DTPC) to refer to limiting the power level on associated client devices.

Beginning in privileged EXEC mode, follow these steps to specify a maximum allowed power setting on all client devices that associate to the wireless access point.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.

The 2.4 GHz radio is radio 0, and the 5 GHz radio is radio 1.

```
interface dot11radio {0 | 1}
```

3. Set the maximum power level allowed on client devices that associate to the wireless access point.
   - Setting the power level to local sets the client power level to that of the access point.
   - Setting the power level to `maximum` sets the client power to the allowed maximum.

     TIP The settings allowed in your regulatory domain can differ from the settings listed here.

   ```
   power client
   ```

These options are available:

```
{local | <-127 - 127> | maximum}
```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the `no` form of the client power command to disable the maximum power level for associated clients. Aironet extensions must be enabled to limit the power level on associated client devices. Aironet extensions are enabled by default.

Configure Radio Channel Settings

The default channel setting for the wireless access point radios is least congested; at startup, the wireless access point scans for and selects the least-congested channel. For the most consistent performance after a site survey, however, we recommend that you assign a static channel setting for each access point. The channel settings on the wireless access point correspond to the frequencies available in your regulatory domain. See the access point hardware installation guide for the frequencies allowed in your domain.

TIP In places where RF interference can be causing clients to occasionally get disconnected from the wireless network, setting the wireless interface to run on a different channel, can avoid the interference.

Each 2.4 GHz channel covers 22 MHz. The bandwidth for channels 1, 6, and 11 does not overlap, so you can set up multiple access points in the same vicinity without causing interference.

The 5 GHz radio operates in the frequency range 5180 - 5825 MHz. The number of channels can vary from 5 to 25 depending on the regulatory domain. Each channel covers 20 MHz, and the bandwidth for the channels overlaps slightly. For best performance, use channels that are not adjacent (44 and 48, for example) for radios that are close to each other.

TIP Too many access points in the same vicinity creates radio congestion that can reduce throughput. A careful site survey can determine the best placement of access points for maximum radio coverage and throughput. See the latest product specifications.

Because they change frequently, channel settings are not in this document. For up-to-date information on channel settings for your access point or bridge, see the latest product specifications.

802.11n Channel Widths

802.11n protocol allows you to use 40 MHz channel width consisting of 2 contiguous non-overlapping channels (for example 5 GHz channels 44 and 48). 40 MHz channel width is not supported for 2.4 GHz radios.

One of the 20 Mhz channels is called the control channel. Legacy clients and 20 Mhz 802.11n clients use the control channel. Beacons can be sent only on this channel. The second 20 Mhz channel is called the extension channel. 40 Mhz stations use this channel and the control channel simultaneously.

A 40 Mhz channel is specified as a channel and extension, such as 1,1. In this example, the control channel is channel 1 and the extension channel is above it.

Beginning in privileged EXEC mode, follow these steps to set the wireless access point channel width.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the 5 GHz radio interface.

```
interface dot11radio 1
```

3. Set the channel for the wireless access point radio.
   - Use the `width` option to specify a bandwidth to use.

   This option consists of three available settings: 20, 40-above, and 40-below. choosing 20 sets the channel width to 20 MHz. Choosing 40-above sets the channel width to 40 Mhz with the extension channel above the control channel. Choosing 40-below sets the channel width to 40 MHz with the extension channel below the control channel.

   ```
   channel
   {frequency | least-congested | width [20 | 40-above
   | 40-below] | dfs}
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Dynamic Frequency Selection

Access points with 5 GHz radios configured at the factory for use in the North America, Europe, now comply with regulations that require radio devices to use Dynamic Frequency Selection (DFS) to detect radar signals and avoid interfering with them. When an access points detects a radar on a certain channel, it avoids using that channel for 30 minutes. Radios configured for use in other regulatory domains don't use DFS.

TIP Because the DFS operation may disrupt client traffic for a prolonged period of time, we recommend not using DFS channels for critical data transmission.

When a DFS-enabled 5 GHz radio operates on one of the 15 channels listed in Table 97 on page 266, the access point automatically uses DFS to set the operating frequency. When DFS is enabled, the access point monitors its operating frequency for radar signals.

If it detects radar signals on the channel, the access point takes these steps:

- Blocks new transmissions on the channel.
- Flushes the power-save client queues.
- Broadcasts an 802.11h channel-switch announcement.
- Disassociates remaining client devices.
- If participating in WDS, sends a DFS notification to the active WDS device that it is leaving the frequency.
- Randomly selects a different 5 GHz channel.
- If the channel selected is one of the channels in Table 97 on page 266, scans the new channel for radar signals for 60 seconds.
- If there are no radar signals on the new channel, enables beacons and accepts client associations.

- If participating in WDS, sends a DFS notification of its new operating frequency to the active WDS device.

TIP You cannot manually select a channel for DFS-enabled 5 GHz radios in some regions, depending on the regulatory requirements. The access points randomly selects a channel in that case.

This table lists the channels and the frequencies that require DFS.

Table 97 - Channels Requiring DFS

Channel	MHz	Channel	MHz	Channel	MHz
52	5260	104	5500	124	5620
56	5280	108	5520	128	5640
60	5300	112	5560	132	5660
64	5320	116	5580	136	5680
100	5500	120	5600	140	5700

For autonomous operation, DFS requires random channel selection among the channels listed. The channels not listed don't require random selection and can be manually configured.

Prior to transmitting on any channels listed in Table 97 on page 266, the access point radio performs a Channel Availability Check (CAC). The CAC is a 60 second scan for the presence of radar signals on the channel. The following sample messages are displayed on the access point console showing the beginning and end of the CAC scan:

```
*Mar 6 07:37:30.423: %DOT11-6-DFS_SCAN_START: DFS: Scanning
frequency 5500 MHz for 60 seconds

*Mar 6 07:37:30.385: %DOT11-6-DFS_SCAN_COMPLETE: DFS scan
complete on frequency 5500 MHz
```

When operating on any of the DFS channels listed in Table 97 on page 266, in addition to performing the CAC, the access point constantly monitors the channel for radar. If radar is detected, the access point stops forwarding data packets within 200 ms and broadcasts five beacons that include an 802.11h channel switch announcement, indicating the channel number that the access point begins using. The following example message appears on the access point console when radar is detected:

```
*Mar 6 12:35:09.750: %DOT11-6-DFS_TRIGGERED: DFS: triggered on
frequency 5500 MHz
```

When radar is detected on a channel, that channel can not be used for 30 minutes. The access point maintains a flag in nonvolatile storage for each channel that it detects radar on in the last 30 minutes. After 30 minutes, the flag is cleared for the corresponding channel. If the access point is restarted before a flag is cleared, the non-occupancy time is reset to 30 minutes when the channel initializes.

TIP The maximum legal transmit power is greater for some 5 GHz channels than for others. When it randomly selects a 5 GHz channel where the power is restricted, the access point automatically reduces transmit power to comply with power limits for that channel.

TIP We recommend that you use the `world-mode dot11d country-code configuration interface` command to configure a country code on DFS-enabled radios.

The IEEE 802.11h protocol requires access points to include the country information element (IE) in beacons and probe responses. By default, however, the country code in the IE is blank. You use the world-mode command to populate the country code IE.

Radar Detection on a DFS Channel

When an access point detects a radar on a DFS channel, the access point creates a file in its flash memory. The file is based on the 802.11a radio serial number and contains the channel numbers where the radar is detected. This is an expected behavior and you can not remove this file.

CLI Commands

The following sections describe CLI commands that apply to DFS.

Confirm that DFS is Enabled

Use the `show controllers dot11radio1` command to confirm that DFS is enabled. The command also includes indications that uniform spreading is required and channels that are in the non-occupancy period due to radar detection.

This example shows a line from the output for the `show controller` command for a channel where the DFS is enabled. The indications listed in the previous paragraph are shown in bold:

```
ap#show controller dot11radio1
!
interface Dot11Radio1
Radio AIR-RM1251A, Base Address 011.9290ec0, BBlock
version 0.00, Software version 6.00.0
Serial number FOCO83114WK
Number of supported simultaneous BSSID on
Dot11Radio1: 8
Carrier Set: Americas (OFDM) (US )
Uniform Spreading Required: Yes
```

```
Current Frequency: 5300 MHz Channel 60 (DFS
enabled)

Current Frequency: 5300 MHz  Channel 60 (DFS
enabled)

Allowed Frequencies: 5180(36) 5200(40) 5220(44)
5240(48) *5260(52) *5280(56) *53

00(60) *5320(64) *5500(100) *5520(104) *5540(108)
*5560(112) *5580(116) *5660(13

2) *5680(136) *5700(140) 5745(149) 5765(153)
5785(157) 5805(161)

* = May only be selected by Dynamic Frequency
Selection (DFS)


Listen Frequencies: 5170(34) 5190(38) 5210(42)
5230(46) 5180(36) 5200(40) 5220(4

4) 5240(48) 5260(52) 5280(56) 5300(60) 5320(64)
5500(100) 5520(104) 5540(108) 55

60(112) 5580(116) 5600(120) 5620(124) 5640(128)
5660(132) 5680(136) 5700(140) 57

45(149) 5765(153) 5785(157) 5805(161) 5825(165)


DFS Blocked Frequencies: none

Beacon Flags: 0; Beacons are enabled; Probes are
enabled

Current Power: 17 dBm

Allowed Power Levels: -1 2 5 8 11 14 15 17

Allowed Client Power Levels: 2 5 8 11 14 15 17

...
```

Configure a Channel

Use the `channel` command to configure a channel. The command for the interface is modified only to let you select a specific channel number and to enable DFS.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter the configuration interface for the 802.11a radio

   ```
   interface dot11radio1
   ```

3. Enter Channel <number>:
   Channel numbers available are 36, 40, 44, 48, 149, 153, 157, 161, 165, 5180, 5200, 5220, 5240, 5745, 5765, 5785, 5805, or 5825.

   TIP This is specific to the -A domain (US/Canada).

   To use DFS channels, enter dfs and one of the following frequency bands to use dynamic frequency selection on the selected channel:

   1 - 5.150...5.250 GHz

   2 - 5.250...5.350 Ghz

   3 - 5.470...5.725 GHz

   4 - 5.725...5.825 GHz

If you attempt to configure a channel that can only be selected by dfs, the following message appears:

```
This channel number/frequency can only be used by
Dynamic Frequency Selection (DFS)
```

4. Return to the privileged EXEC mode.

   ```
   end
   ```

5. Verify your entries

   ```
   show running-config
   ```

6. (Optional) Save your entries to the configuration file.

   ```
   copy running-config startup-config
   ```

The following example selects channel 36 and configures it to use DFS on a frequency band 1:

```
ap#configure terminal
ap(config)interface dot11radio1
ap(config-if) channel 36
ap(config-if)
```

Block Channels from DFS Selection

If your regulatory domain limits the channels that you can use in specific locations--for example, indoors or outdoors, you can block groups of channels to prevent the access point from selecting them when DFS is enabled. Use this configuration interface command to block groups of channels from DFS selection:

```
[no] dfs band [1] [2] [3] [4] block
```

The 1, 2, 3, and 4 options designate blocks of channels:

- 1 - Specifies frequencies 5.150...5.250 GHz.

  This group of frequencies is also known as the UNII-1 band.
- 2 - Specifies frequencies 5.250...5.350 GHz.

  This group of frequencies is also known as the UNII-2 band.
- 3 - Specifies frequencies 5.470...5.725 GHz.
- 4 - Specifies frequencies 5.725...5.825 GHz.

  This group of frequencies is also known as the UNII-3 band.

This example shows how to prevent the access point from selecting frequencies 5.150...5.350 GHz during DFS:

```
ap(config-if)# dfs band 1 2 block
```

This example shows how to unblock frequencies 5.150...5.350 for DFS:

```
ap(config-if)# no dfs band 1 2 block
```

This example shows how to unblock all frequencies for DFS:

```
ap(config-if)# no dfs band block
```

Set the 802.11n Guard Interval

The 802.11n guard interval is the period in nanoseconds between packets. Two settings are available: short (400 ns) and long (800 ns). Short guard interval allows slightly better performance but may cause issues in environments with lots of reflections and multipath signals. We recommend that you do not modify the guard interval settings from default unless necessary.

Beginning in privileged EXEC mode, follow these steps to set the 802.11n guard interval.

1. Enter global configuration mode.

   ```
   configure terminal
   ```
2. Enter interface configuration mode for the radio interface.

- The 802.11n 2.4 GHz radio is radio 0
- The 802.11n 5 GHz radio is radio 1.

```
interface dot11radio {0 | 1}
```

3. Enter a guard interval.
   - `any` permits either the short (400 ns) or long (800 ns) guard interval
   - `long` permits only the long (800 ns) guard interval

   ```
   guard-interval {any | long}
   ```
4. Return to privileged EXEC mode.

   ```
   end
   ```
5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Configure Transmit and Receive Antennas

You can select the antenna the wireless access point uses to receive and transmit data.

Option	Description
a-antenna	use antenna A
ab-antenna	use antennas A and B
abc-antenna	use antennas A, B, and C
abcd-antenna	use antennas A, B, C, and D

Beginning in privileged EXEC mode, follow these steps to select the antennas the wireless access point uses to receive and transmit data.

1. Enter global configuration mode.

   ```
   configure terminal
   ```
2. Enter interface configuration mode for the radio interface.
   - The 802.11n 2.4 GHz radio is radio 0
   - The 802.11n 5 GHz radio is radio 1.

   ```
   interface dot11radio {0 | 1}
   ```
3. Specify the resultant gain of the antenna attached to the device by entering a value from -128...128 dB.

   If necessary, you can use a decimal in the value, such as 1.5.

   ```
   gain dB
   ```
4. Select what antennas to use:

   ```
   antenna {a-antenna | ab-antenna | abc-antenna |
   abcd-antenna}
   ```

For best performance, do not use this setting unless connecting a non-standard external antenna or disabling a damaged antenna port. Antenna ports are marked A, B, C, D on the AP case.

5. Return to privileged EXEC mode.

   ```
   end
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Enable and Disable Gratuitous Probe Response

Gratuitous Probe Response (GPR) aids in conserving battery power in dual mode phones that support cellular and WLAN modes of operation. GPR is available on 5 GHz radios and is disabled by default. You can configure two GPR settings:

- Period

  This setting determines the time between GPR transmissions in Kusec intervals from 10...255 (similar to the beacon period)

- Speed

  The speed is the data rate used to transmit the GPR. Selecting a longer period reduces the amount of RF bandwidth consumed by the GPR with the possibility of shorter battery life. Selecting higher transmission speeds also reduces the amount of bandwidth consumed but at the expense of a smaller cell size.

Beginning in privileged EXEC mode, follow these steps to enable GPR and set its parameters.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the 5 GHz radio interface.

   ```
   interface dot11radio {1}
   ```

3. Enable the Gratuitous Probe Response feature by using default period (10 Kusec) and speed (6.0 Mbps).

   ```
   probe-response gratuitous
   {period | speed}
   ```

4. (Optional) Enter a value from 10 to 255. The default value is 10

   ```
   period Kusec
   ```

5. (Optional) Sets the response speed in Mbps. The default value is 6.0.

   ```
   speed
   {[6.0] [9.0] [12.0] [18.0] [24.0] [36.0] [48.0 ]
   [54.0] }
   ```

6. Return to privileged EXEC mode.

   ```
   end
   ```

7. (Optional) Save your entries in the configuration file.

```
copy running-config startup-config
```

The optional parameters can be configured independently or combined when you don't want to use the defaults, as shown in the following examples:

```
(config-if)# probe-response gratuitous period 30
(config-if)# probe-response gratuitous speed 12.0
(config-if)# probe-response gratuitous period 30
speed 12.0
```

Use the no form of the command to disable the GPR feature.

Disable and Enable Aironet Extensions

By default, the wireless access point uses Aironet extensions to detect the capabilities of client devices and to support features that require specific interaction between the wireless access point and associated client devices. Aironet extensions must be enabled to support these features:

- Load balancing

  The wireless access point uses Aironet extensions to direct client devices to an access point that provides the best connection to the network based on factors such as number of users, bit error rates, and signal strength.

- Message Integrity Check (MIC)

  MIC is an additional WEP security feature that prevents attacks on encrypted packets called bit-flip attacks. The MIC, implemented on both the wireless access point and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof.

- Cisco Key Integrity Protocol (CKIP)

  Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group. The standards-based algorithm, TKIP, does not require Aironet extensions to be enabled.

- Repeater mode

  You must enable the Aironet extensions on repeater access points and on the associated root access points.

- World mode (legacy only)

  Client devices with legacy world mode enabled receive carrier set information from the wireless access point and adjust their settings automatically. Aironet extensions are not required for 802.11d world mode operation.

- Limiting the power level on associated client devices

When a client device associates to the wireless access point, the wireless access point sends the maximum allowed power level setting to the client.

Disabling Aironet extensions disables the features listed above, but it sometimes improves the ability of non-Cisco client devices to associate to the wireless access point.

Aironet extensions are enabled by default. Beginning in privileged EXEC mode, follow these steps to disable Aironet extensions.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface. The 2.4 GHz radio is radio 0, and the 5 GHz radio is radio 1.
   - The 802.11n 2.4 GHz radio is radio 0
   - The 802.11n 5 GHz radio is radio 1.

   ```
   interface dot11radio {0 | 1}
   ```

3. Disable Aironet extensions.

   ```
   no dot11 extension aironet
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the `dot11 extension aironet` command to enable Aironet extensions if they are disabled.

Configure the Ethernet Encapsulation Transformation Method

When the wireless access point receives data packets that are not 802.3 packets, the wireless access point must format the packets to 802.3 by using an encapsulation transformation method. These are the two transformation methods:

- 802.1H—This method provides good performance for Cisco Aironet wireless products.
- RFC 1042—Use this setting to verify good interoperability with non-Cisco Aironet wireless equipment. RFC 1042 is used by other manufacturers of wireless equipment and is the default setting.

Beginning in privileged EXEC mode, follow these steps to configure the encapsulation transformation method.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.
   - The 802.11n 2.4 GHz radio is radio 0

- The 802.11n 5 GHz radio is radio 1.

```
interface dot11radio {0 | 1}
```

3. Set the encapsulation transformation method to RFC 1042 (`rfc1042`, the default setting) or 802.1h (`dot1h`).

```
payload-encapsulation
rfc1042 | dot1h
```

4. Return to privileged EXEC mode.

```
end
```

5. (Optional) Save your entries in the configuration file.

```
copy running-config startup-config
```

Enable and Disable Reliable Multicast to Workgroup Bridges

The reliable multicast messages from the access point to workgroup bridges setting limits reliable delivery of multicast messages to approximately 20 Cisco Aironet Workgroup Bridges that are associated to the wireless access point. The default setting, disabled, reduces the reliability of multicast delivery to allow more workgroup bridges to associate to the wireless access point.

Access points and bridges in this mode treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. Treating a workgroup bridge as an infrastructure device means that the wireless access point reliably delivers multicast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge.

The performance cost of reliable multicast delivery, that is a duplication of each multicast packet sent to each workgroup bridge—limits the number of infrastructure devices, including workgroup bridges, that can associate to the wireless access point. To increase beyond 20 the number of workgroup bridges that can maintain a radio link to the wireless access point, the wireless access point must reduce the delivery reliability of multicast packets to workgroup bridges. With reduced reliability, the wireless access point cannot confirm whether multicast packets reach the intended workgroup bridge, so workgroup bridges at the edge of the wireless access point's coverage area can lose IP connectivity. When you treat workgroup bridges as client devices, you increase performance but reduce reliability.

TIP This feature is used with stationary workgroup bridges. Mobile workgroup bridges can encounter spots in the wireless device's coverage area where they don't receive multicast packets and lose communication with the wireless device even though they are still associated to it.

Beginning in privileged EXEC mode, follow these steps to configure the encapsulation transformation method.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the 2.4 GHz radio interface.

   ```
   interface dot11radio { 0 }
   ```

3. Enable reliable multicast messages to workgroup bridges.

   ```
   infrastructure-client
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the no form of the command to disable reliable multicast messages to workgroup bridges.

Enable and Disable Public Secure Packet Forwarding

Public Secure Packet Forwarding (PSPF) prevents client devices associated to an access point from inadvertently sharing files or communicating with other client devices associated to the access point. It provides Internet access to client devices without providing other capabilities of a LAN. This feature is useful for public wireless networks like those installed in airports or on college campuses.

TIP To prevent communication between clients associated to different access points, you must set up protected ports on the switch where the wireless devices are connected.

To enable and disable PSPF by using CLI commands on the wireless access point, you use bridge groups. You can find a detailed explanation of bridge groups and instructions for implementing them in this document:

- See Configuring Transparent Bridges in the Cisco IOS Bridging and IBM Networking Configuration Guide.

You can also enable and disable PSPF by using the web browser interface. The PSPF setting is on the Radio Settings pages.

PSPF is disabled by default. Beginning in privileged EXEC mode, follow these steps to enable PSPF.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.
   - The 802.11n 2.4 GHz radio is radio 0
   - The 802.11n 5 GHz radio is radio 1.

   ```
   interface dot11radio {0 | 1}
   ```

3. Enable PSPF.

   ```
   bridge-group group port-protected
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the no form of the command to disable PSPF.

Configure the Beacon Period and the DTIM

The beacon period is the amount of time between access point beacons in Kilomicroseconds. One Kμsec equals 1,024 microseconds. The Data Beacon Rate, always a multiple of the beacon period, determines how often the beacon

contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them.

For example, if the beacon period is set at 100, its default setting, and the data beacon rate is set at 2, its default setting, then the wireless access point sends a beacon containing a DTIM every 200 Kμsecs. One Kμsec equals 1,024 microseconds.

The default beacon period is 100, and the default DTIM is 2. Beginning in privileged EXEC mode, follow these steps to configure the beacon period and the DTIM.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.
   - The 802.11n 2.4 GHz radio is 0.
   - The 802.11n 5 GHz radio is 1.

   ```
   interface dot11radio {0 | 1}
   ```

3. Set the beacon period. Enter a value in Kilomicroseconds.

   ```
   beacon period value
   ```

4. Set the DTIM. Enter a value in Kilomicroseconds.

   ```
   beacon dtim-period value
   ```

5. Return to privileged EXEC mode.

   ```
   end
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Configure RTS Threshold and Retries

The RTS threshold determines the packet size that the wireless access point issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the wireless access point, or in areas where the clients are far apart and can detect only the wireless access point and not each other. You can enter a setting ranging from 0...2347 bytes.

Maximum RTS retries is the maximum number of times the wireless access point issues an RTS before stopping the attempt to send the packet over the radio. Enter a value from 1...128.

The default RTS threshold is 2347 for all access points and bridges, and the default maximum RTS retries setting is 32. Beginning in privileged EXEC mode, follow these steps to configure the RTS threshold and maximum RTS retries.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.
   - The 2.4 GHz 802.11n radio is 0.
   - The 5 GHz 802.11n radio is 1.

   ```
   interface dot11radio {0 | 1}
   ```

3. Set the RTS threshold. Enter an RTS threshold from 0...2347.

   ```
   rts threshold value
   ```

4. Set the maximum RTS retries. Enter a setting from 1...128.

   ```
   rts retries value
   ```

5. Return to privileged EXEC mode.

   ```
   end
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the no form of the command to reset the RTS settings to defaults.

Configure the Maximum Data Retries

The maximum data retries setting determines the number of attempts the wireless access point makes to send a packet in the best-effort QoS queue before giving up and dropping the packet.

The default setting is 32. Beginning in privileged EXEC mode, follow these steps to configure the maximum data retries.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.
   - The 2.4 GHz 802.11n radio is 0.
   - The 5 GHz 802.11n radio is 1.

   ```
   interface dot11radio {0 | 1}
   ```

3. Set the maximum data retries. Enter a setting from 1...128.

   ```
   packet retries value
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the no form of the command to reset the setting to defaults.

Configuring the Fragmentation Threshold

The fragmentation threshold determines the size that packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

The default setting is 2338 bytes. Beginning in privileged EXEC mode, follow these steps to configure the fragmentation threshold:

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.

- The 2.4 GHz 802.11n radio is 0.
- The 5 GHz 802.11n radio is 1.

```
interface dot11radio {0 | 1}
```

3. Set the fragmentation threshold.
   - Enter a setting from 256...2346 bytes for the 2.4 GHz radio.
   - Enter a setting from 256...2346 bytes for the 5 GHz radio.

   ```
   fragment-threshold value
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the no form of the command to reset the setting to defaults.

Perform a Carrier Busy Test

You can perform a carrier busy test to check the radio activity on wireless channels.

WARNING: During the carrier busy test, the wireless access point drops all associations with wireless networking devices for 4 seconds while it conducts the carrier test and then the test results appear.

In privileged EXEC mode, enter this command to perform a carrier busy test:

```
dot11 interface-number carrier busy
```

For *interface-number*, enter `dot11radio 0` to run the test on the 2.4 GHz radio, or enter `dot11radio 1` to run the test on the 5 GHz radio.

Use the `show dot11 carrier busy` command to show the carrier busy test results.

Configure ClientLink

Cisco ClientLink (referred to as Beam Forming) is an intelligent beamforming technology that directs the RF signal to 802.11a/g devices to improve performance by 65%, improve coverage by up to 27% percent, and reduce coverage holes.

Cisco ClientLink helps extend the useful life of existing 802.11a/g devices in mixed-client networks. It is beneficial for organizations that move to 802.11n and want to make sure that all clients on the network, regardless of type, are guaranteed the bandwidth and throughput they need.

Use CLI to Configure ClientLink

To enable ClientLink, enter this CLI command in interface configuration mode on 802.11n radio interfaces:

```
beamform ofdm
```

The ClientLink configuration option is not available through GUI. ClientLink is disabled by default.

Debug Radio Functions

Use the `debug dot11` `privileged EXEC` command to begin debugging of radio functions. Use the **no** form of this command to stop the debug operation. The command syntax is:

```
[no] debug dot11
{events | packets | forwarding | mgmt | network-map
| syslog | virtual-interface}
```

WARNING: Enabling debug mode can severely affect performance and even disrupt communication completely. Use only if instructed by the tech support.

Table 98 - Syntax for `debug dot11` Command

Syntax	Activates
`events`	Activates debugging of all radio related events
`packets`	Activates debugging of radio packets received and transmitted
`forwarding`	Activates debugging of radio forwarded packets
`mgmt`	Activates debugging of radio access point management activity
`network-map`	Activates debugging of radio association management network map
`syslog`	Activates debugging of radio system log
`virtual interface`	Activates debugging of radio virtual interfaces

This example shows how to begin debugging of all radio-related events:

```
AP# debug dot11 events
```

This example shows how to begin debugging of the radio system log:

```
AP# debug dot11 syslog
```

This example shows how to stop debugging of all radio related events:

```
AP# no debug dot11 events
```

TIP Debugging not enabled is the default of the command.

Notes:

Configure Multiple Service Set Identifiers (SSIDs)

This chapter describes how to configure and manage multiple service set identifiers (SSIDs) on the access point.

Topic	Page
Understand Multiple SSIDs	285
Configure Multiple SSIDs	286
Configure Multiple Basic SSIDs	290
Assign IP Redirection for an SSID	295
Include an SSID in an SSIDL IE	297

Understand Multiple SSIDs

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Don't include spaces in your SSIDs.

You can configure up to 16 SSIDs on your access point and assign different configuration settings to each SSID. All the SSIDs are active at the same time; that is, client devices can associate to the access point by using any of the SSIDs. These are the settings you can assign to each SSID:

- VLAN
- Client authentication method

TIP For detailed information on client authentication types, see Configure Authentication Types on page 337.

- Maximum number of client associations by using the SSID
- RADIUS accounting for traffic by using the SSID
- Guest mode
- Authentication profile (username and password) in a workgroup bridge or repeater mode
- Redirection of packets received from client devices

If you want the access point to allow associations from client devices that don't specify an SSID in their configurations, you can set up a guest SSID. The access point includes the guest SSID in its beacon. If the guest mode is disabled, the SSID is not broadcast in the beacon messages. If you don't want clients that don't

have a preconfigured SSID to connect to the wireless network, disable the guest SSID feature.

For information on how to configure guest mode SSID and disable Guest mode SSID, see Create an SSID Globally on page 286.

If your access point is a repeater or is root access point that acts as a parent for a repeater, you can set up an SSID for use in repeater mode. You can assign an authentication username and password to the repeater-mode SSID to let the repeater authenticate your network like a client device.

If your network uses VLANs, you can assign one SSID to a VLAN, and client devices by using the SSID are grouped in that VLAN.

IMPORTANT SSIDs, VLANs, and encryption schemes are mapped together on a one-to-one-to one basis; one SSID can be mapped to one VLAN, and one VLAN can be mapped to one encryption scheme. When using a global SSID configuration you can not configure one SSID with two different encryption schemes. For example, you can not apply SSID north with TKIP apply on interface dot11 0 and also apply SSID north with WEP128 on interface dot11 1.

Configure Multiple SSIDs

These sections contain configuration information for multiple SSIDs:

Default SSID Configuration

The Stratix 5100 WAP does not have a default SSID.

Create an SSID Globally

You can configure SSIDs globally or for a specific radio interface. When you use the `dot11 ssid` global configuration command to create an SSID, you can use the `ssid` configuration interface command to assign the SSID to a specific interface.

When an SSID has been created in global configuration mode, the `ssid` configuration interface command attaches the SSID to the interface but does not enter ssid configuration mode. However, if the SSID has not been created in global configuration mode, the `ssid` command puts CLI into SSID configuration mode for the new SSID.

Beginning in privileged EXEC mode, follow these steps to create an SSID globally. After you create an SSID, you can assign it to specific radio interfaces.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Create an SSID and enter SSID configuration mode for the new SSID.

   The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.

   - The first character cannot contain the!, #, or; character.
   - +,], /, ", TAB, and trailing spaces are invalid characters for SSIDs.

   ```
   dot11 ssid ssid-string
   ```

3. (Optional) Set an authentication username and password that the access point uses to authenticate to the network when in repeater mode.

4. (Optional) Set the username and password on the SSID that the repeater access point uses to associate to a root access point, or with another repeater.

   ```
   authentication client
   username username
   password password
   ```

5. (Optional) Enable RADIUS accounting for this SSID.

   For *list-name*, specify the accounting method list.

   ```
   accounting list-name
   ```

6. (Optional) Assign the SSID to a VLAN on your network.

   Client devices that associate by using the SSID are grouped into this VLAN. You can assign only one SSID to a VLAN.

   ```
   vlan vlan-id
   ```

7. (Optional) Designate the SSID as your access point guest-mode SSID.

   The access point includes the SSID in its beacon and allows associations from client devices that don't specify an SSID.

   `guest-mode`

8. This command controls the SSID that access points and bridges use when associating with one another. A root access point only lets a repeater access point to associate by using the infrastructure SSID.

   A root bridge only lets a non-root bridge to associate by using the infrastructure SSID. Repeater access points and non-root bridges use this SSID to associate with root devices.

   The access point and bridge GUI requires the configuration of infrastructure-ssid for repeater, and non-root bridge roles. It is not mandatory to configure infrastructure SSID for workgroup bridge roles. However, if you use CLI to configure the device role, you don't have to configure an infrastructure SSID unless multiple SSIDs are configured on the radio. If multiple SSIDs are configured on the radio, you must use the `infrastructure-ssid` command to specify the SSID the non-root bridge uses to connect to the root bridge.

   Repeaters don't associate with bridges when infrastructure-ssid is not configured irrespective of the presence of single or multiple SSIDs.

   `infrastructure-ssid [optional]`

9. Enter interface configuration mode for the radio interface that you want to assign to the SSID.

   `interface dot11radio { 0 | 1 }`

   - The 2.4 GHz 802.11n radio is 0.
   - The 5 GHz 802.11n radio is 1.

10. Assign the global SSID that you created in step 2 to the radio interface.

    `ssid ssid-string`

11. Return to privileged EXEC mode.

    `end`

12. (Optional) Save your entries in the configuration file.

    `copy running-config startup-config`

IMPORTANT You use the `ssid` command authentication options to configure an authentication type for each SSID. See Configure an Access Point as a Local Authenticator on page 303 for instructions on configuring authentication types.

Use the no form of the command to disable the SSID or to disable SSID features.

This example shows how to:

- Name an SSID.
- Set the maximum number of client devices that can associate by using this SSID to 15.
- Assign the SSID to a VLAN.
- Assign the SSID to a radio interface.

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# exit
AP(config)# interface dot11radio 0
AP(config-if)# ssid batman
AP(config-if)#end
```

View SSIDs Configured Globally

Use this command to view configuration details for SSIDs that are configured globally:

```
AP# show running-config ssid ssid-string
```

Restrict SSIDs by Using a RADIUS Server

To prevent client devices from associating to the access point by using an unauthorized SSID, you can create a list of authorized SSIDs that clients must use on your RADIUS authentication server.

The SSID authorization process consists of these steps.

1. A client device associates to the access point by using any SSID configured on the access point.
2. The client begins RADIUS authentication.
3. The RADIUS server returns a list of SSIDs that the client is allowed to use. The access point checks the list for a match of the SSID used by the client. There are three possible outcomes:
   a. If the SSID that the client used to associate to the access point matches an entry in the allowed list returned by the RADIUS server, the client is allowed network access after completing all authentication requirements.
   b. If the access point does not find a match for the client in the allowed list of SSIDs, the access point disassociates the client.

c. If the RADIUS server does not return any SSIDs (no list) for the client, then the administrator has not configured the list, and the client is allowed to associate and attempt to authenticate.

You must use the list of SSIDs from the RADIUS server in the form of Cisco VSAs. The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the access point and the RADIUS server by using the vendor-specific attribute (attribute 26).

Vendor-specific attributes (VSAs) let vendors support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. The Cisco vendor-ID is 9, and the supported option has vendor-type 1, that is named `cisco-avpair`. The Radius server can have zero or more SSID VSAs per client.

In this example, the following AV pair adds the SSID batman to the list of allowed SSIDs for a user:

```
cisco-avpair= "ssid=batman"
```

For instructions on configuring the access point to recognize and use VSAs, see the Configure the Access Point for Vendor-proprietary RADIUS Server Communication on page 390.

Configure Multiple Basic SSIDs

Access point 802.11a, 802.11g, and 802.11n radios support up to 8 basic SSIDs (BSSIDs), that are similar to MAC addresses. You use multiple BSSIDs to assign a unique DTIM setting for each SSID and to broadcast more than one SSID in beacons. A large DTIM value increases battery life for power-save client devices that use an SSID, and broadcasting multiple SSIDs makes your wireless LAN more accessible to guests.

Devices on your wireless LAN that are configured to associate to a specific access point based on the access point MAC address (for example, client devices, repeaters, hot standby units, or workgroup bridges) can lose their association when you add or delete a multiple BSSID. When you add or delete a multiple BSSID, check the association status of devices configured to associate to a specific access point. If necessary, reconfigure the disassociated device to use the new BSSID MAC address.

Configuration Requirements for Multiple BSSIDs

To configure multiple BSSIDs, your access points must meet these minimum requirements:

- VLANs must be configured
- Access points must contain a radio that supports multiple BSSIDs.

  To determine whether a radio supports multiple basic SSIDs, enter the `show controllers radio_interface` command. The radio supports multiple basic SSIDs if the results include this line:

  ```
  Number of supported simultaneous BSSID on
  radio_interface: 16
  ```

Guidelines for Multiple BSSIDs

Keep these guidelines in mind when configuring multiple BSSIDs:

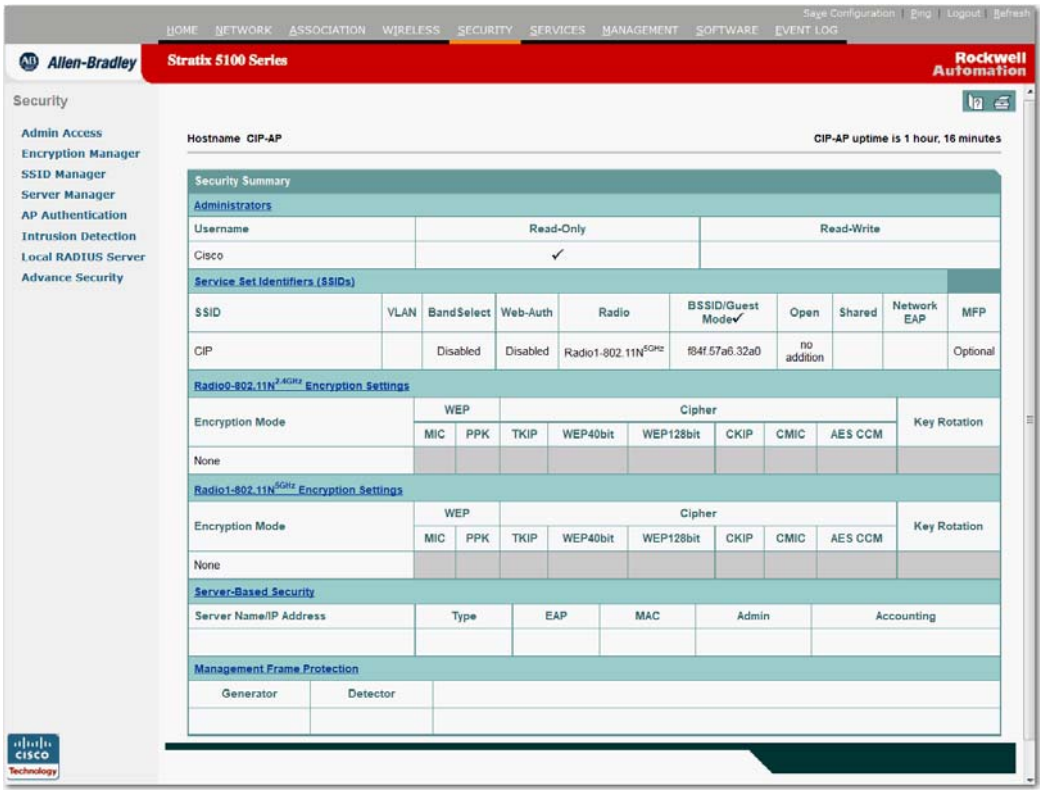
- RADIUS-assigned VLANs are not supported when you enable multiple BSSIDs.
- When you enable BSSIDs, the access point automatically maps a BSSID to each SSID. You can't manually map a BSSID to a specific SSID.
- When multiple BSSIDs are enabled on the access point, the SSIDL IE does not contain a list of SSIDs; it contains only extended capabilities.
- Any Wi-Fi certified client device can associate to an access point by using multiple BSSIDs.
- You can enable multiple BSSIDs on access points that participate in WDS.

Configure Multiple BSSIDs

Follow these steps to configure multiple BSSIDs.

1. Click Security.

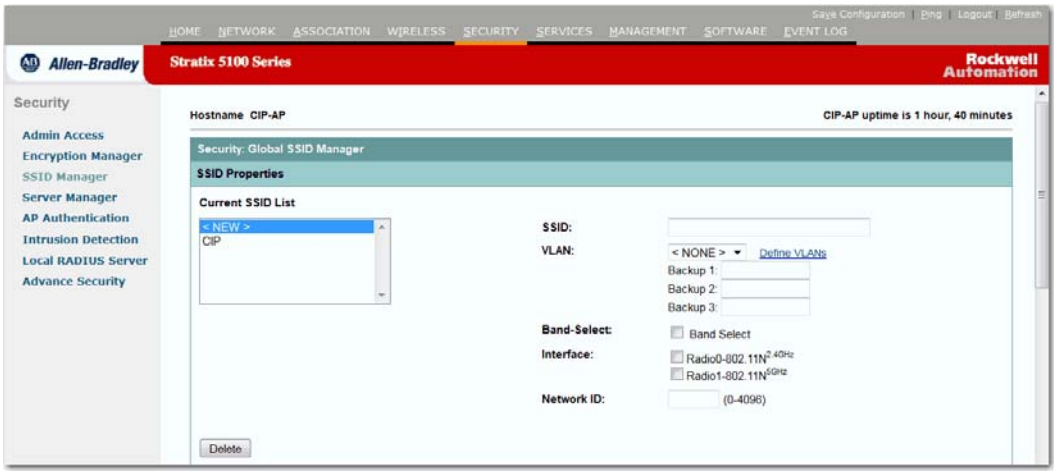
   The Security summary page appears.



   If you use CLI instead of the GUI, refer to CLI commands listed in the CLI Configuration Example on page 294.

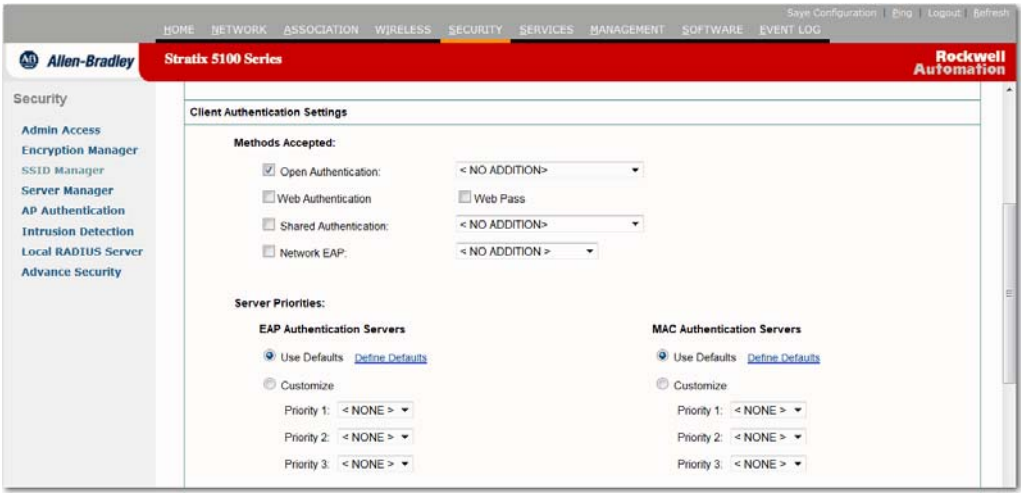
2. From the left menu, click SSID Manager.

   The SSID Manager page appears.



3. Enter the SSID name in the SSID field.
4. From the VLAN pull-down menu, choose the VLAN that is assigned to the SSID.
5. Select the radio interfaces where the SSID is enabled.

   The SSID remains inactive until you enable it for a radio interface.
6. Enter a Network ID for the SSID in the Network ID field.
7. Assign authentication, authenticated key management, and accounting settings to the SSID in the Authentication Settings, Authenticated Key Management, and Accounting Settings sections of the page.



   BSSIDs support all the authentication types that are supported on SSIDs.
8. (Optional) In the Multiple BSSID Beacon Settings section, select the Set SSID as Guest Mode check box to include the SSID in beacons.
9. (Optional) To increase the battery life for power-save clients that use this SSID, select the Set Data Beacon Rate (DTIM) check box and enter a beacon rate for the SSID.

   The beacon rate determines how often the access point sends a beacon containing a Delivery Traffic Indicator Message (DTIM).

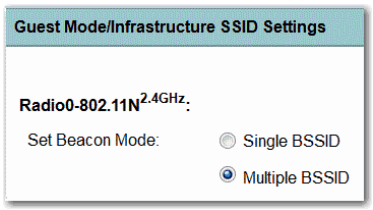
   When client devices receive a beacon that contains a DTIM, they normally wake up to check for pending packets. Longer intervals between DTIMs let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.

   The default beacon rate is 2. This means that every other beacon contains a DTIM.

10. Enter a beacon rate between 1...100.

    TIP Increasing the DTIM period count delays the delivery of multicast packets. Because multicast packets are buffered, large DTIM period counts can cause a buffer overflow.

11. In the Guest Mode/Infrastructure SSID Settings section, select Multiple BSSID.



12. Click Apply.

CLI Configuration Example

This example shows the CLI commands that you use to enable multiple BSSIDs on a radio interface, create an SSID called *visitor*, designate the SSID as a BSSID, specify that the BSSID is in the beacons, set a DTIM period for the BSSID, and assign the SSID *visitor* to the radio interface:

```
ap(config)# interface d0
ap(config-if)# mbssid
ap(config-if)# exit
ap(config)# dot11 ssid visitor
ap(config-ssid)# mbssid guest-mode dtim-period 75
ap(config-ssid)# exit
ap(config)# interface d0
ap(config-if)# ssid visitor
```

You can also use the `dot11 mbssid` global configuration command to simultaneously enable multiple BSSIDs on all radio interfaces that support multiple BSSIDs.

Display Configured BSSIDs

Use the `show dot11 bssid` privileged EXEC command to display the relationship between SSIDs and BSSIDs or MAC addresses. This example shows the command output:

```
AP1230#show dot11 bssid
Interface     BSSID           Guest  SSID
```

```
Dot11Radio1    0011.2161.b7c0  Yes  atlantic
Dot11Radio0    0005.9a3e.7c0f  Yes  WPA2-TLS-g
```

Assign IP Redirection for an SSID

When you configure IP redirection for an SSID, the access point redirects all packets sent from client devices associated to that SSID to a specific IP address. IP redirection is used mainly on wireless LANs serving handheld devices that use a central software application and are statically configured to communicate with a specific IP address.

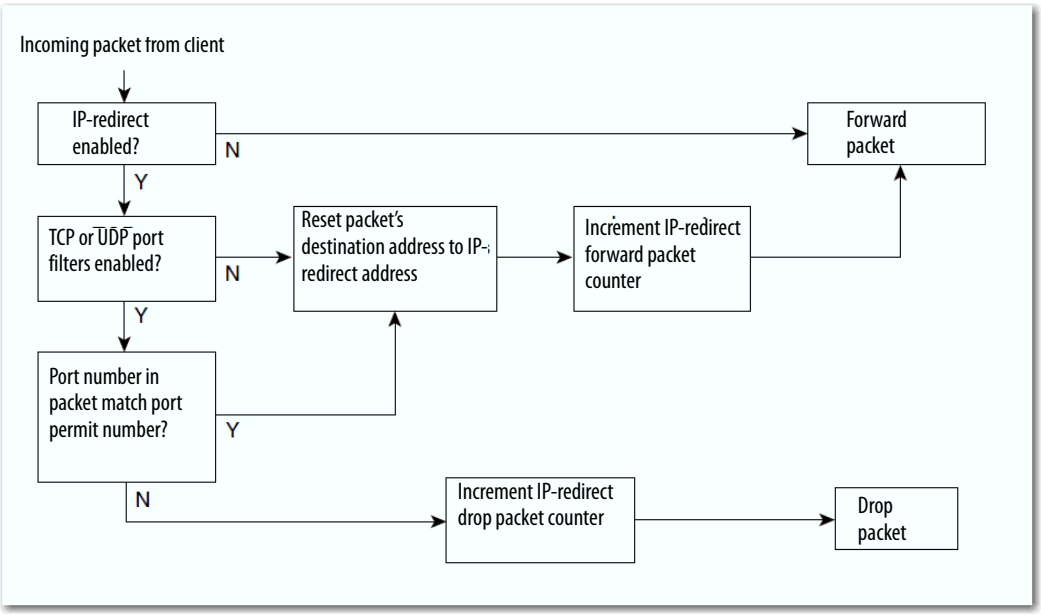
For example, the wireless LAN administrator at a retail store or warehouse can configure IP redirection for its bar code scanners. They use the same scanner application and send data to the same IP address.

You can redirect all packets from client devices associated by using an SSID or redirect only packets directed to specific TCP or UDP ports (as defined in an access control list). When you configure the access point to redirect only packets addressed to specific ports, the access point redirects those packets from clients and drops all other packets from clients by using the SSID.

TIP When you perform a ping test from the access point to a client device that is associated by using an IP-redirect SSID, the response packets from the client are redirected to the specified IP address and are not received by the sender.

This figure shows the process flow that occurs when the access point receives client packets from clients associated by using an IP-redirect SSID.

Figure 85 - Process Flow for IP Redirection



Guidelines for Using IP Redirection

Keep these guidelines in mind when using IP redirection:

- The access point does not redirect broadcast, unicast, or multicast BOOTP/DHCP packets received from client devices.
- Existing ACL filters for incoming packets take precedence over IP redirection.

Configure IP Redirection

Beginning in privileged EXEC mode, follow these steps to configure IP redirection for an SSID.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter configuration mode for a specific SSID.

   ```
   dot11 ssid ssid-string
   ```

3. Enter IP redirect configuration mode for the IP address. Enter the IP address with decimals, as in this example: 10.91.104.92

   If you don't specify an access control list (ACL) that defines TCP or UDP ports for redirection, the access point redirects all packets that it receives from client devices.

   ```
   ip redirection host ip-address
   ```

4. (Optional) Specify an ACL to apply to the redirection of packets.

   Only packets sent to the specific UDP or TCP ports defined in the ACL are redirected. The access point discards all received packets that don't match the settings defined in the ACL. The **in** parameter specifies that the ACL is applied to the incoming interface for the access point.

   ```
   ip redirection host ip-address access-group acl in
   ```

This example shows how to configure IP redirection for an SSID without applying an ACL. The access point redirects all packets that it receives from client devices associated to the SSID batman.

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config ssid)# ip redirection host 10.91.104.91
AP(config ssid-redirect)# end
```

This example shows how to configure IP redirection only for packets sent to the specific TCP and UDP ports specified in an ACL. When the access point receives packets from client devices associated by using the SSID `robin` command, it redirects packets sent to the specified ports and discards all other packets.

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config ssid)# ip redirection host 10.91.104.91
access-group redirect-acl in
AP(config ssid)# end
```

Include an SSID in an SSIDL IE

The access point beacon can advertise only one broadcast SSID. However, you can use SSIDL information elements (SSIDL IEs) in the access point beacon to alert client devices of additional SSIDs on the access point. When you designate an SSID to be in an SSIDL IE, client devices detect that the SSID is available, and they also detect the security settings required to associate by using that SSID.

IMPORTANT When multiple BSSIDs are enabled on the access point, the SSIDL IE does not contain a list of SSIDs; it contains only extended capabilities.

Beginning in privileged EXEC mode, follow these steps to include an SSID in an SSIDL IE.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter configuration mode for a specific SSID.

   ```
   dot11 ssid ssid-string
   ```

3. Include an SSIDL IE in the access point beacon that advertises the extended capabilities for the access point, such as 802.1x and support for Microsoft Wireless Provisioning Services (WPS).

   Use the advertisement option to include the SSID name and capabilities in the SSIDL IE. Use the wps option to set the WPS capability flag in the SSIDL IE.

   ```
   information-element ssidl [advertisement] [wps]
   ```

   Use the no form of the command to disable SSIDL IEs.

Configure Spanning Tree Protocol

This chapter describes how to configure Spanning Tree Protocol (STP) on your access point.

Topic	Page
Spanning Tree Protocol (STP)	299
Configure STP Features	300
Display Spanning-tree Status	302

IMPORTANT STP is available only when the access point is in bridge mode.

Spanning Tree Protocol (STP)

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, one active path can only exist between any two stations. Spanning-tree operation is transparent to end stations, that cannot detect whether they are connected to a single LAN segment or to a LAN of multiple segments.

When you create fault-tolerant internet-works, you must have a loop-free path between all nodes in a network. The spanning-tree algorithm calculates the best loop-free path throughout a Layer 2 network. Infrastructure devices such as wireless access points and switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The devices don't 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 can receive duplicate messages. Infrastructure devices can 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.

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

These meanings are separate from the Role in radio network setting that includes root and non-root options. A bridge whose Role in radio network setting is Root Bridge does not necessarily become the root bridge in the spanning tree. In this chapter, 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 interfaces on a bridge are part of a loop, the spanning-tree port priority and path cost settings determine the interface that is put in the forwarding state or the blocking state. The port priority value represents the location of an interface in the network topology and how well it is located to pass traffic. The path cost value represents media speed.

The access point supports both per-VLAN spanning tree (PVST) and a single 802.1q spanning tree without VLANs. The access point cannot run 802.1s MST or 802.1d Common Spanning Tree, that maps multiple VLANs into a one-instance spanning tree.

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

Configure STP Features

STP is available only when the access point is in bridge mode. Complete these major steps to configure STP on the access point.

1. If necessary, assign interfaces and sub-interfaces to bridge groups.
2. Enable STP for each bridge group.
3. Set the STP priority for each bridge group.

Default STP Configuration

STP is disabled by default. This table lists the default STP settings when you enable STP.

Table 99 - Default STP Values When STP is Enabled

Setting	Default Value
Bridge priority	32768
Bridge max age	20
Bridge hello time	2
Bridge forward delay	15
Ethernet port path cost	19
Ethernet port priority	128
Radio port path cost	33
Radio port priority	128

The radio and Ethernet interfaces and the native VLAN on the access point are assigned to bridge group 1 by default. When you enable STP and assign a priority on bridge group 1, STP is enabled on the radio and Ethernet interfaces and on the primary VLAN, and those interfaces adopt the priority assigned to bridge group 1. You can create bridge groups for sub-interfaces and assign different STP settings to those bridge groups.

Configure STP Settings

Beginning in privileged EXEC mode, follow these steps to configure STP on the access point.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for radio or Ethernet interfaces or sub-interfaces.
   - The 2.4 GHz 802.11n radio is 0.
   - The 5 GHz 802.11n radio is 1.

   The Gigabit Ethernet interface is 0.

   ```
   interface { dot11radio number | gigabitEthernet number }
   ```

3. Assign the interface to a bridge group. You can number your bridge groups from 1...255.

   ```
   bridge-group number
   ```

4. Counteract the command that automatically disables STP for a bridge group. STP is enabled on the interface when you enter the bridge *n* protocol ieee command.

   ```
   no bridge-group number spanning-disabled
   ```

5. Return to global configuration mode.

   ```
   exit
   ```

6. Enable STP for the bridge group. You must enable STP on each bridge group that you create with bridge-group commands.

   ```
   bridge number protocol ieee
   ```

7. (Optional) Assign a priority to a bridge group. The lower the priority, the more likely it is that the bridge becomes the spanning-tree root.

   ```
   bridge number priority priority
   ```

8. Return to privileged EXEC mode.

   ```
   end
   ```

9. Verify your entries.

   ```
   show spanning-tree bridge
   ```

10. (Optional) Save your entries in the configuration file.

    ```
    copy running-config startup-config
    ```

Display Spanning-tree Status

To display the spanning-tree status, use one or more of the privileged EXEC commands in this table.

Table 100 - Display Commands for Spanning-tree Status

Command	Description
show spanning-tree	Information on your network's spanning tree.
show spanning-tree blocked-ports	List of blocked ports on this bridge.
show spanning-tree bridge	Status and configuration of this bridge.
show spanning-tree active	Spanning-tree information on only active interfaces.
show spanning-tree root	Summary of information on the spanning-tree root.
show spanning-tree interface *interface-id*	Spanning-tree information for the specified interface.
show spanning-tree summary [totals]	Summary of port states or the total lines of the STP state section appear.

For information about other keywords for the show spanning-tree privileged EXEC command, see publication Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges.

Configure an Access Point as a Local Authenticator

This chapter describes how to configure the access point as a local authenticator to serve as a standalone authentication server or for a small wireless LAN or to provide back up authentication service. As a local authenticator, the access point performs LEAP, EAP-FAST, and MAC-based authentication for up to 50 client devices.

Topic	Page
Local Authentication	303
Configure a Local Authenticator	304
Configure EAP-FAST Settings	320
Limit the Local Authenticator to One Authentication Type	323
Unblock Locked Usernames	323
Debug Messages	325

Local Authentication

Many small wireless LANs that could be made more secure with 802.1x authentication don't have access to a RADIUS server. On many wireless LANs that use 802.1x authentication, access points rely on RADIUS servers housed in a distant location to authenticate client devices, and the authentication traffic must cross a WAN link. If the WAN link fails, or if the access points cannot access the RADIUS servers for any reason, client devices cannot access the wireless network even if the work they wish to do is entirely local.

To provide local authentication service or back-up authentication service in case of a WAN link or a server failure, you can configure an access point to act as a local authentication server. The access point can authenticate up to 50 wireless client devices by using LEAP, EAP-FAST, or MAC-based authentication. The access point performs up to 5 authentications per second.

You configure the local authenticator access point manually with client usernames and passwords because it does not synchronize its database with the main RADIUS servers. You can also specify a VLAN and a list of SSIDs that a client is allowed to use.

TIP If your wireless LAN contains only one access point, you can configure the access point as both the 802.1x authenticator and the local authenticator. However, users associated to the local authenticator access point can notice a drop in performance when the access point authenticates client devices.

You can configure your access points to use the local authenticator when they cannot reach the main servers, or you can configure your access points to use the local authenticator or as the main authenticator if you don't have a RADIUS server. When you configure the local authenticator as a back-up to your main servers, the access points periodically check the link to the main servers and stop by using the local authenticator automatically when the link to the main servers is restored.

IMPORTANT The access point you use as an authenticator contains detailed authentication information for your wireless LAN so you can secure it physically to protect its configuration.

Configure a Local Authenticator

Follow these guidelines when configuring an access point as a local authenticator.

- Use an access point that does not serve a large number of client devices. When the access point acts as an authenticator, performance can degrade for associated client devices.
- Secure the access point physically to protect its configuration.

Configuration Overview

Complete these four major steps to set up a local authenticator.

1. On the local authenticator, create a list of access points authorized to use the authenticator to authenticate client devices. Each access point that uses the local authenticator is a network access server (NAS).

   If your local authenticator access point also serves client devices, you must enter the local authenticator access point as an NAS. When a client associates to the local authenticator access point, the access point uses itself to authenticate the client.
2. On the local authenticator, create user groups and configure parameters to be applied to each group (optional).
3. On the local authenticator, create a list of up to 50 LEAP users, EAP-FAST users, or MAC addresses that the local authenticator is authorized to authenticate.

   You don't have to specify the type of authentication that you want the local authenticator to perform. It automatically performs LEAP, EAP-FAST, or MAC-address authentication for the users in its user database.
4. On the access points that use the local authenticator, enter the local authenticator as a RADIUS server.

If your local authenticator access point also serves client devices, you must enter the local authenticator as a RADIUS server in the local authenticator's configuration. When a client associates to the local authenticator access point, the access point uses itself to authenticate the client.

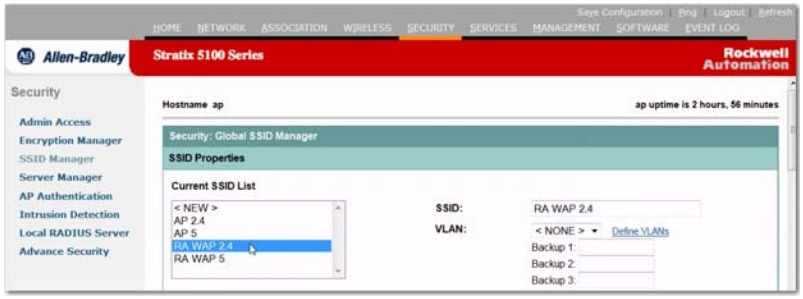
Configure/Enable Local MAC Authentication

Two modes of MAC authentication are used. One is MAC Authentication Only where MAC address authentication is a means of augmenting Open, Shared Key, or Network-EAP authentication. The second is MAC authentication co-existing with EAP authentication. This mode enables a combination of MAC address authentication and EAP for authenticating the device or user. The first step in either method is to configure the SSID.

Configure the SSID

Follow these steps to configure the SSID.

1. Click Security.
2. From the Security menu, click SSID Manager to go the SSID Manager page.
3. In the Current SSID list, select the SSID for the MAC authentication.

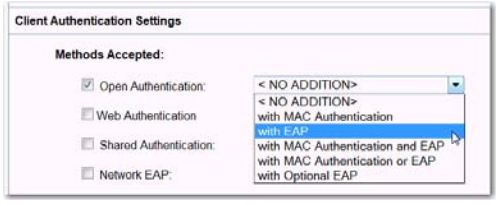


If you need to create a new SSID, continue to step 4. Otherwise, skip to step 7.

4. Select <NEW> from the Current SSID List.
5. Provide the SSID name in the SSID text field.
6. From the VLAN pull-down list, select the VLAN to be used for this SSID.

   Select <NONE> if VLANs are not enabled.

7. Under Authentication Methods Accepted, select the authentication type to use on this SSID.

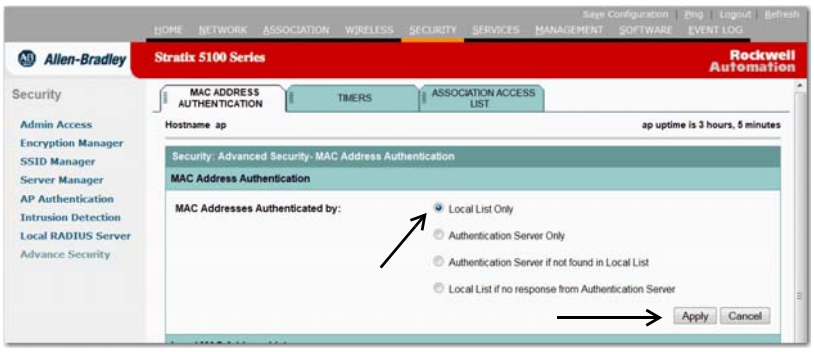


8. Click Apply to create the SSID.

Create Local MAC Address Lists

Now that the SSID is configured, you can create the local MAC address list.

1. Click Security.
2. From the Security menu, click Advanced Security.
3. Click the MAC Address Authentication tab to move to the MAC Address Authentication page.



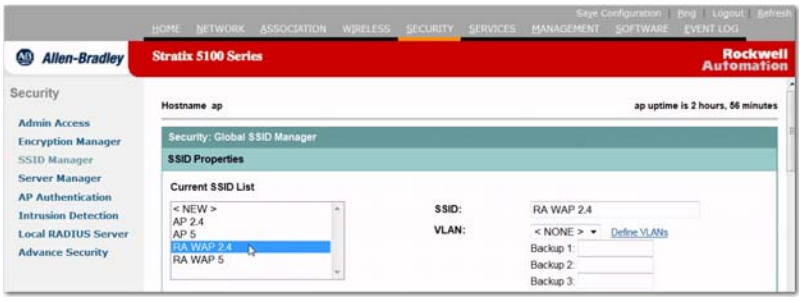
4. Select Local List Only for the MAC Address Authenticated by parameter.
5. Click Apply on that MAC Address Authentication portion of the page.
6. In the Local MAC Address List section, enter the authorized MAC address in the New MAC Address parameter.

7. Click Apply on that Local MAC Address List portion of the page.

Create and Enable MAC Authentication by Using RADIUS Server

You must first configure the SSID. Complete the following steps to configure the SSID.

1. Click Security.
2. From the Security menu, click SSID Manager.
3. In the Current SSID list, select the SSID for the MAC authentication.

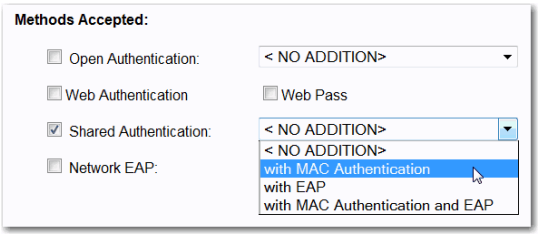


   If you need to create a new SSID, continue to step 4. Otherwise, skip to step 7.

4. Select <NEW> from the Current SSID List.
5. Provide the SSID name in the SSID text field.
6. At the VLAN list, select the VLAN to be used for this SSID.

   Select <NONE> if VLANs are not enabled.

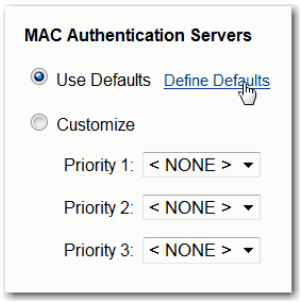
7. Under Authentication Methods Accepted, select the authentication type to use on this SSID.
8. Use the pull-down menu to choose MAC Authentication, or you can also select MAC and EAP authentication or MAC or EAP authentication.



9. Determine how you are going to use specific RADIUS servers on this SSID by using the EAP and MAC Authentication Server sections.

   You can choose to use the defaults or customize the priority by using the pull-down menu.

If you click to enable the use of the defaults, click the Define Defaults link to go to the Server Manager page. This is where you can configure the RADIUS server.



10. Click Apply.

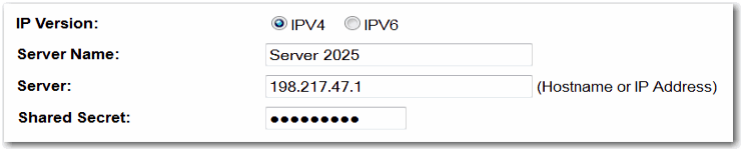
Add the RADIUS Server

Now that the SSID is configured, you can add the RADIUS or TACACS+ server. Complete these steps to add the RADIUS server.

1. Click Security.
2. From the Security menu, click Server Manager.
3. From the Current Server List pull-down menu, select the server to be used for MAC authentication.

   If you need to create a new server, continue to step 4Step 4. Otherwise, skip to step 11.

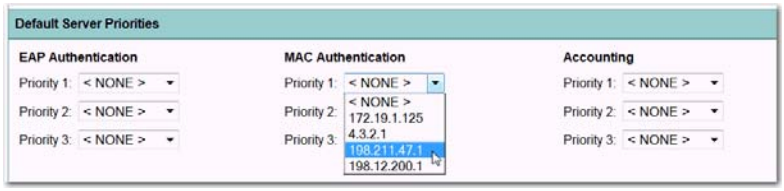
4. Select <NEW> from the Current Server List.
5. Use the pull-down menu to select RADIUS server as the server type.
6. Enter the server host name or IP address in the Server text field.



7. In the Shared Secret text field, enter the shared secret used by your specified server that matches the one on the device.
8. (Optional) Enter the port number your server uses for authentication in the Authentication Port parameter.

   For example, the port setting for the Cisco RADIUS server (Access Control Server [ACS]) is 1645, and the port setting for many RADIUS servers is 1812.

9. From Default Server Priorities, determine the level of priority you want to assign to each server.
10. Select Priority 1, 2, or 3 for this server.



11. Click Apply to add the server.

    Steps step 12 through step 16 are optional tasks and can be skipped to expedite setup.

12. Click the Global Properties tab.
13. In the Accounting Updates Interval field, specify the interval that you want the accounting updates to be performed.

14. In the TACACS+ Server Timeout field, specify the number of seconds an access point waits for a reply to a TACACS+ request before resending the request.
15. In the RADIUS Server Timeout field, specify the number of seconds an access point waits for a reply to a RADIUS request before resending the request.

16. In the RADIUS Server Retransmit Retries field, specify the number of times the access point sends each RADIUS request to the server before giving up.

    If more than one RADIUS server is configured for MAC authentication, enable the Dead Server List option.

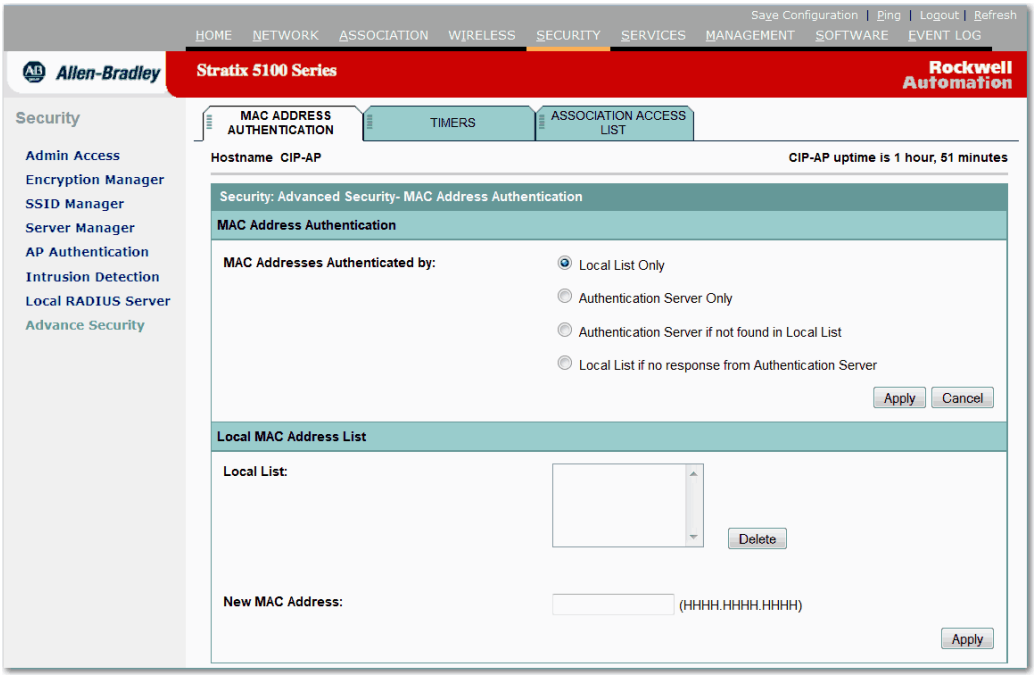
    a. Specify how long you want the unresponsive RADIUS servers to be skipped over when the access point is attempting RADIUS server authentication.
    b. Enter this amount in the Server remains on list for text field.

17. Click Apply.

Set the MAC Authentication Method

After the RADIUS server is added, you can set the MAC authentication method. Complete these steps to set the MAC authentication method.

1. Click Security.
2. From the Security menu, click Advanced Security.
3. Click the MAC Address Authentication tab.



4. Select Authentication Server if not found in Local List if you want to use the RADIUS server in conjunction with a local list.
5. Click Apply in the MAC Address Authentication section.

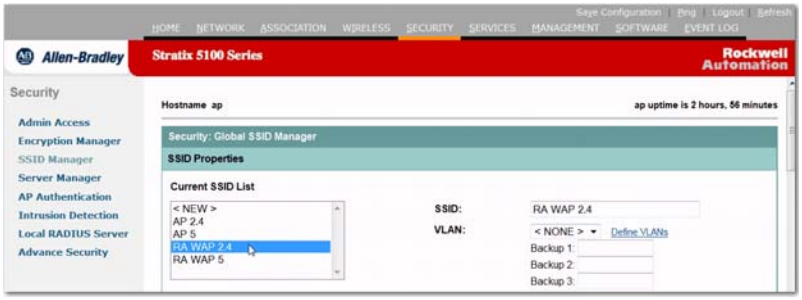
   Then complete Step 6 through Step 9. Otherwise, choose Authentication Server Only at the MAC Addresses authenticated by parameter and skip to Step 9.
6. In the Local MAC Address list section, enter the authorized MAC address in the New MAC Address parameter.
7. Click Apply on the Local MAC Address List portion of the page to add this MAC address to the local list.
8. If you need to add more than one MAC address to the local list, repeat Steps 4 and 5 until the list is complete.
9. Click Apply in the MAC Address Authentication section.

Configure Network EAP

A device uses the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server on your network to provide authentication for wireless client devices.

To configure Network EAP, you must first configure the SSID. Follow these steps to configure the SSID.

1. Click Security.
2. From the Security menu, click SSID Manager.
3. In the Current SSID list, select the SSID for the EAP authentication type.

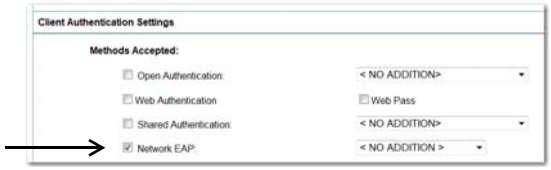


   If you need to create a new SSID, continue to Step 4. Otherwise, skip to Step 7.

4. Select <NEW> from the Current SSID List.
5. Provide the SSID name in the SSID text field.
6. From the VLAN pull-down list, select the VLAN to be used for this SSID.

   Select <NONE> if VLANs are not enabled. You can use the Define VLANs link to go to Services>VLAN and configure one.

7. Under Authentication Methods Accepted, check the Network EAP check box.



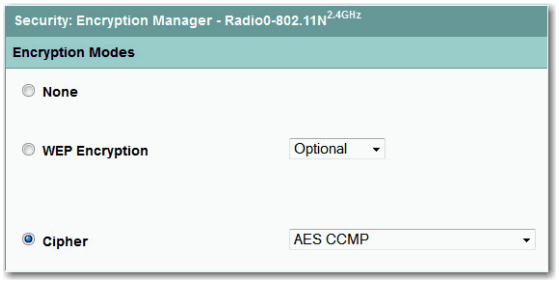
8. Click Apply to create the SSID.

Now that the SSID is configured, you must configure the encryption. Complete these steps to configure the encryption.

1. Click Security.
2. From the Security menu, click Encryption Manager.
3. From the Set Encryption Mode and Keys for VLAN pull-down menu, select the VLAN corresponding to the SSID you added above.

   This VLAN pull-down list appears when you have VLANs enabled. If no VLANs are present, the encryption settings apply to all SSIDs. Select <NONE> if VLANs are not enabled.

4. Under the Encryption Mode section, click Cipher to enable AES CCMP encryption.



Now that encryption is configured, you must add a RADIUS or TACACS+ server. Complete the following steps to add the RADIUS server.

1. Click Security.
2. From the Security menu, click Server Manager.
3. In the Current Server List, select the server to be used for EAP authentication.

   If you need to create a new server, continue to step 4. Otherwise, skip to step 10.
4. Select <NEW> from the Current Server List.
5. Enter the server host name or IP address in the Server text field.
6. Use the pull-down menu to select either a RADIUS or TACACS+ server.
7. In the Shared Secret text field, enter the shared secret used by your specified server that matches the one on the device.
8. Enter the port number your server uses for authentication in the Authentication Port parameter.

   The port setting for the Cisco RADIUS server (the Access Control Server [ACS]) is 1645, and the port setting for many RADIUS servers is 1812.
9. Enter the port number your RADIUS server uses for accounting.

   The port setting for Cisco's RADIUS server (the Access Control Server [ACS]) is 1646, and the port setting for many RADIUS servers is 1813. Check your server's product documentation to find the correct accounting port setting.
10. Use the pull-down menus to determine the level of priority you want to assign to each server.
11. Click Apply to add the server.

    Steps step 12 through step 17 are optional tasks and can be skipped to expedite setup.
12. Click the Global Properties tab.
13. Specify the interval that the accounting updates are performed in the Accounting Updates Interval field.

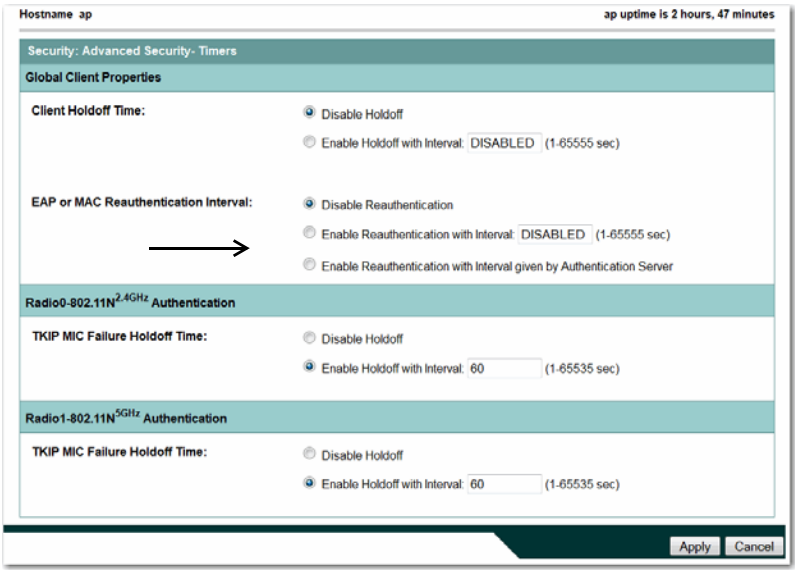
14. In the TACACS+ Server Timeout field, specify the number of seconds an access point waits for a reply to a TACACS+ request before resending the request.
15. In the RADIUS Server Timeout field, specify the number of seconds an access point waits for a reply to a RADIUS request before resending the request.
16. In the RADIUS Server Retransmit Retries field, specify the number of times the access point sends each RADIUS request to the server before it stops trying.

    If more than one RADIUS server is configured for EAP authentication, enable the Dead Server List option. Specify how long unresponsive RADIUS servers should be skipped over when the access point is attempting RADIUS server authentication. Enter this amount in the Server remains on list for text field.
17. Click Apply in the Global Server Properties section.

Configure Advanced EAP Parameters

Now that the RADIUS server is added, you can configure advanced EAP parameters. These steps are optional and can be skipped to expedite setup.

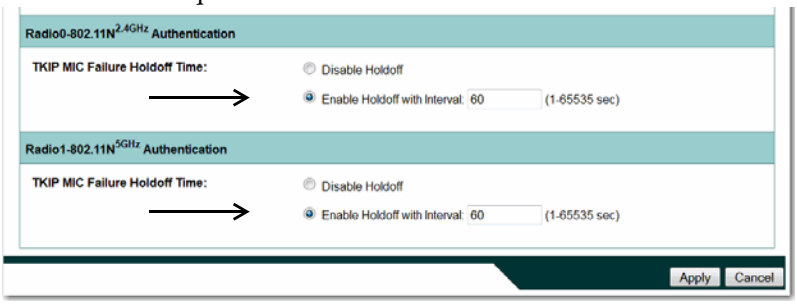
1. Click Security.
2. From the Security menu, click Advanced Security.
3. Click the Timers tab to go to the page where EAP authentication is specified.



4. Choose one of the options that enable reauthentication.

   These interval options set how often EAP authentication is reattempted. You can enter your own interval or use the one provided by the RADIUS server.

5. In the TKIP MIC Failure Holdoff Time text field, enter the amount of time the access point needs to wait for wireless clients to respond to EAP authentication requests.



6. Click Apply.

Configure the Local Authenticator Access Point by Using CLI

Beginning in Privileged Exec mode, follow these steps to configure the access point as a local authenticator.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable AAA.

   ```
   aaa new-model
   ```

3. Enable the access point as a local authenticator and enter configuration mode for the authenticator.

   ```
   radius-server local
   ```

4. Add an access point to the list of units that use the local authenticator.

   Enter the access point's IP address and the shared key used to authenticate communication between the local authenticator and other access points. You must enter this shared key on the access points that use the local authenticator. If your local authenticator also serves client devices, you must enter the local authenticator access point as a NAS.

   TIP Leading spaces in the key string are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, don't enclose the key in quotation marks unless the quotation marks are part of the key.

   Repeat this step to add each access point that uses the local authenticator.

   ```
   nas ip-address key shared-key
   ```

5. (Optional) Enter user group configuration mode and configure a user group that can be assigned shared settings.

   ```
   group group-name
   ```

6. (Optional) Specify a VLAN to be used by members of the user group.

   The access point moves group members into that VLAN, overriding other VLAN assignments. You can assign only one VLAN to the group.

   ```
   vlan vlan
   ```

7. (Optional) Enter up to 20 SSIDs to limit members of the user group to those SSIDs.

   The access point checks that the SSID that the client used to associate matches one of the SSIDs in the list. If the SSID does not match, the client is disassociated.

   ```
   ssid ssid
   ```

8. (Optional) Enter the number of seconds that you want to wait before the access points authenticate members of the group again.

The reauthentication provides users with a new encryption key. The default setting is 0, that means that group members are never required to reauthenticate.

```
reauthentication time seconds
```

9. (Optional) To help protect against password guessing attacks, you can lock out members of a user group for a length of time after a set number of incorrect passwords.
   - count—The number of failed passwords that triggers a lockout of the username.
   - time—The number of seconds the lockout can last. If you enter `infinite`, an administrator must manually unblock the locked username.

     See the Unblock Locked Usernames on page 323 for instructions on unblocking client devices.

   ```
   block count count
   time { seconds | infinite }
   ```

10. Exit group configuration mode and return to authenticator configuration mode.

    ```
    exit
    ```

11. Enter the LEAP and EAP-FAST users allowed to authenticate by using the local authenticator.

    You must enter a username and password for each user. If you only know the NT value of the password, where you can often find in the authentication server database, you can enter the NT hash as a string of hexadecimal digits.

    To add a client device for MAC-based authentication, enter the client's MAC address as both the username and password. Enter 12 hexadecimal digits without a dot or dash between the numbers as the username and the password. For example, for the MAC address 0009.5125.d02b, enter *00095125d02b* as both the username and the password.

    To limit only the user to MAC authentication, enter `mac-auth-only`.

    To add the user to a user group, enter the group name. If you don't specify a group, the user is not assigned to a specific VLAN and is never forced to reauthenticate.

    ```
    user username
    { password | nthash } password
    [ group group-name ]
    [mac-auth-only]
    ```

12. Return to privileged EXEC mode.

    ```
    end
    ```

13. (Optional) Save your entries in the configuration file.

    ```
    copy running-config startup-config
    ```

This example shows how to set up a local authenticator used by three access points with three user groups and several users:

```
AP# configure terminal
AP(config)# radius-server local
AP(config-radsrv)# nas 10.91.6.159 key 110337
AP(config-radsrv)# nas 10.91.6.162 key 110337
AP(config-radsrv)# nas 10.91.6.181 key 110337
AP(config-radsrv)# group clerks
AP(config-radsrv-group)# vlan 87
AP(config-radsrv-group)# ssid batman
AP(config-radsrv-group)# ssid robin
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group cashiers
AP(config-radsrv-group)# vlan 97
AP(config-radsrv-group)# ssid deer
AP(config-radsrv-group)# ssid antelope
AP(config-radsrv-group)# ssid elk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group managers
AP(config-radsrv-group)# vlan 77
AP(config-radsrv-group)# ssid mouse
AP(config-radsrv-group)# ssid chipmunk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# exit
AP(config-radsrv)# user jsmith password twain74
group clerks
AP(config-radsrv)# user stpatrick password snake100
group clerks
AP(config-radsrv)# user nick password uptown group
clerks
```

```
AP(config-radsrv)# user 00095125d02b password
00095125d02b group clerks mac-auth-only

AP(config-radsrv)# user 00095125d02b password
00095125d02b group cashiers

AP(config-radsrv)# user 00079431f04a password
00079431f04a group cashiers

AP(config-radsrv)# user carl password 272165 group
managers

AP(config-radsrv)# user vic password lid178 group
managers

AP(config-radsrv)# end
```

Configure Other Access Points to Use the Local Authenticator

You add the local authenticator to the list of servers on the access point the same way that you add other servers. For detailed instructions on setting up RADIUS servers on your access points, see Configure RADIUS and TACACS+ Servers on page 373

IMPORTANT	If your local authenticator access point also serves client devices, you must configure the local authenticator to use itself to authenticate client devices.

On the access points that use the local authenticator, use the `radius-server host` command to enter the local authenticator as a RADIUS server.

The order of access point attempts to use the servers matches the order that you entered the servers in the access point configuration.

If you are configuring the access point to use RADIUS for the first time, enter the main RADIUS servers first, and enter the local authenticator last.

IMPORTANT	You must enter 1812 as the authentication port and 1813 as the accounting port. The local authenticator listens on UDP port 1813 for RADIUS accounting packets. It discards the accounting packets but sends acknowledge packets back to RADIUS clients to prevent clients from assuming that the server is down.

Use the `radius-server deadtime` command to set an interval. During this interval, the access point does not attempt to use servers that don't respond. This avoids the wait for a request to time out before trying the next configured server. A server marked as dead is skipped by additional requests for the duration of minutes that you specify, up to 1440 (24 hours).

This example shows how to set up two main servers and a local authenticator with a server deadtime of 10 minutes:

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port
1000 acct-port 1001 key 77654
AP(config)# radius-server host 172.10.0.1 auth-port
1645 acct-port 1646 key 77654
AP(config)# radius-server host 10.91.6.151 auth-
port 1812 acct-port 1813 key 110337
AP(config)# radius-server deadtime 10
```

In this example, if the WAN link to the main servers fails, the access point completes these steps when a LEAP-enabled client device associates.

1. It tries the first server, times out multiple times, and marks the first server as dead.
2. It tries the second server, times out multiple times, and marks the second server as dead.
3. It tries and succeeds by using the local authenticator.

If another client device needs to authenticate during the 10-minute dead-time interval, the access point skips the first two servers and tries the local authenticator first. After the dead-time interval, the access point tries to use the main servers for authentication. When setting a dead time, you must balance the need to skip dead servers with the need to check the WAN link and begin by using the main servers again as soon as possible.

Each time the access point tries to use the main servers while they are down, the client device trying to authenticate can report an authentication timeout. The client device retries and succeeds when the main servers time out and the access point tries the local authenticator. You can extend the timeout value on Cisco client devices to accommodate expected server timeouts.

To remove the local authenticator from the access point configuration, use the `no radius-server host hostname | ip-address` global configuration command.

Configure EAP-FAST Settings

The default settings for EAP-FAST authentication are suitable for most wireless LANs. However, you can customize the credential timeout values, authority ID, and server keys to match your network requirements.

Configure PAC Settings

This section describes how to configure Protected Access Credential (PAC) settings. The first time that an EAP-FAST client device attempts to authenticate to the local authenticator, the local authenticator generates a PAC for the client. You can also generate PACs manually and use the Aironet Client Utility to import the PAC file.

PAC Expiration Times

You can limit the number of days that PACs are valid and a grace period where the PACs are valid after they have expired. By default, PACs are valid for 2 days (one day default period plus one day grace period). You can also apply the expiration of time and the grace period settings to a group of users.

Use this command to configure the expiration time and grace period for PACs:

```
AP(config-radsrv-group)# [no] eapfast pac expiry
days [grace days]
```

Enter a number of days from 2...4095. Enter the no form of the command to reset the expiration time or grace period to infinite days.

In this example, PACs for the user group expire in 100 days with a grace period of two days:

```
AP(config-radsrv-group)# eapfast pac expiry 100
grace 2
```

Generate PACs Manually

The local authenticator automatically generates PACs for EAP-FAST clients that request them. However, you can generate a PAC manually for some client devices. When you enter the command, the local authenticator generates a PAC file and writes it to the network location that you specify. The user imports the PAC file into the client profile.

Use this command to generate a PAC manually:

```
AP# radius local-server pac-generate filename
username [password password] [expiry days]
```

When you enter the PAC filename, enter the full path to where the local authenticator writes the PAC file (such as tftp://172.1.1.1/test/user.pac). The password is optional and, if not specified, a default password understood by the CCX client is used. Expiry is also optional and, if not specified, the default period is one day.

In this example, the local authenticator generates a PAC for the username *joe*, password-protects the file with the password `bingo`, sets the PAC to expire in 10 days, and writes the PAC file to the TFTP server at 10.0.0.5:

```
AP# radius local-server pac-generate tftp://
10.0.0.5 joe password bingo expiry 10
```

Configure an Authority ID

All EAP-FAST authenticators are identified by an authority identity (AID). The local authenticator sends its AID to an authenticating client, and the client checks its database for a matching AID. If the client does not recognize the AID, it requests a new PAC.

Use these commands to assign an AID to the local authenticator:

```
AP(config-radserv)# [no] eapfast authority id
identifier
```

```
AP(config-radserv)# [no] eapfast authority info
identifier
```

The eapfast authority id command assigns an AID that the client device uses during authentication.

Configure Server Keys

The local authenticator uses server keys to encrypt PACs that it generates and to decrypt PACs when authenticating clients. The server maintains two keys, a primary key and a secondary key, and uses the primary key to encrypt PACs. By default, the server uses a default value as the primary key but does not use a secondary key unless you configure one.

When the local authenticator receives a client PAC, it attempts to decrypt the PAC with the primary key. If decryption fails with the primary, the authenticator attempts to decrypt the PAC with the secondary key if one is configured. If decryption fails, the authenticator rejects the PAC as invalid.

Use these commands to configure server keys:

```
AP(config-radsrv)# [no] eapfast server-key primary
{[auto-generate] | [ [0 | 7] key]}

AP(config-radsrv)# [no] eapfast server-key
secondary [0 | 7] key
```

Keys can contain up to 32 hexadecimal digits.

- Enter `0` before the key to enter an unencrypted key.
- Enter **7** before the key to enter an encrypted key.

Use the `no` form of the commands to reset the local authenticator to the default setting, that is a default value as a primary key.

Possible PAC Failures Caused by Access Point Clock

The local authenticator uses the access point clock to both generate PACs and to determine whether PACs are valid. However, relying on the access point clock can lead to PAC failures.

If your local authenticator access point receives its time setting from an NTP server, there is an interval between starting up and synchronization with the NTP server. During this interval, the access point uses its default time setting.

If the local authenticator generates a PAC during that interval, the PAC can be expired when the access point receives a new time setting from the NTP server. If an EAP-FAST client attempts to authenticate during the interval between startup and NTP-synch, the local authenticator can reject the client's PAC as invalid.

If your local authenticator does not receive its time setting from an NTP server and it restarts frequently, PACs generated by the local authenticator can expire at the right time. The access point clock is reset when the access point restarts, so the elapsed time on the clock has not reached the PAC expiration time.

Limit the Local Authenticator to One Authentication Type

By default, a local authenticator access point performs LEAP, EAP-FAST, and MAC-based authentication for client devices. However, you can limit the local authenticator to perform only one or two authentication types. Use the no form of the authentication command to restrict the authenticator to an authentication type:

```
AP(config-radsrv)# [no] authentication [eapfast]
[leap] [mac]
```

Because all authentication types are enabled by default, you enter the **no** form of the command to disable authentication types. For example, if you want the authenticator to perform only LEAP authentication, you enter these commands:

```
AP(config-radsrv)# no authentication eapfast
AP(config-radsrv)# no authentication mac
```

Unblock Locked Usernames

You can unblock usernames before the lockout time expires, or when the lockout time is set to infinite. In Privileged Exec mode on the local authenticator, enter this command to unblock a locked username:

```
AP# clear radius local-server user username
```

View Local Authenticator Statistics

In privileged exec mode, enter this command to view statistics collected by the local authenticator:

```
AP# show radius local-server statistics
```

This example shows local authenticator statistics:

```
Successes               : 0           Unknown usernames : 0
Client blocks           : 0           Invalid passwords      : 0
Unknown NAS             : 0           Invalid packet from NAS: 0

NAS : 10.91.6.158
Successes               : 0           Unknown usernames      : 0
Client blocks           : 0           Invalid passwords      : 0
Corrupted packet        : 0           Unknown RADIUS message : 0
No username attribute   : 0           Missing auth attribute : 0
Shared key mismatch     : 0           Invalid state attribute: 0
Unknown EAP message     : 0           Unknown EAP auth type  : 0
Auto provision success  : 0           Auto provision failure : 0
```

```
PAC refresh           : 0          Invalid PAC received   : 0

Username                   Successes  Failures  Blocks
nicky                              0         0       0
jones                              0         0       0
jsmith                             0         0       0
Router#sh radius local-server statistics
Successes             : 1          Unknown usernames      : 0
Client blocks         : 0          Invalid passwords      : 0
Unknown NAS           : 0          Invalid packet from NAS: 0
```

The first section of statistics lists cumulative statistics from the local authenticator.

The second section lists stats for each access point (NAS) authorized to use the local authenticator. The EAP-FAST statistics in this section include these stats:

- Auto provision success—the number of PACs generated automatically
- Auto provision failure—the number of PACs not generated because of an invalid handshake packet or invalid username or password
- PAC refresh—the number of PACs renewed by clients
- Invalid PAC received—the number of PACs received that were expired, that the authenticator could not decrypt, or that were assigned to a client username not in the authenticator's database

The third section lists stats for individual users. If a user is blocked and the lockout time is set to infinite, *blocked* appears at the end of the stat line for that user. If the lockout time is not infinite, *Unblocked in x seconds* appears at the end of the stat line for that user.

Use this privileged exec mode command to reset local authenticator statistics to zero:

```
AP# clear radius local-server statistics
```

Debug Messages

In privileged exec mode, enter this command to control the display of debug messages for the local authenticator:

```
AP# debug radius local-server { client | eapfast |
error | packets}
```

Use the command options to display this debug information:

- Use the `client` option to display error messages related to failed client authentications.
- Use the `eapfast` option to display error messages related to EAP-FAST authentication. Use the sub-options to select specific debugging information:
  - `encryption` — information on the encryption and decryption of received and transmitted packets.
  - `events`— information on all EAP-FAST events.
  - `pac`—information on events related to PACs, such as PAC generation and verification.
  - `pkts`— The packets sent to and received from EAP-FAST clients.
- Use the `error` option to display error messages related to the local authenticator.
- Use the `packets` option to turn on display of the content of RADIUS packets sent and received.

Notes:

Configure Cipher Suites

This chapter describes how to configure the cipher suites required to use Wi-Fi Protected Access (WPA) and Cisco Centralized Key Management (CCKM) authenticated key management, including AES, Message Integrity Check (MIC), Temporal Key Integrity Protocol (TKIP), and broadcast key rotation.

Topic	Page
Cipher Suites	327
Configure Cipher Suites	328

Cipher Suites

Just as anyone within range of a radio station can tune to the station's frequency and listen to the signal, any wireless networking device within range of an access point can receive the access point's radio transmissions. We recommend that you use full encryption on your wireless network.

Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN. You must use a cipher suite to enable WPA or CCKM.

Cipher suites are enabled by using the "encryption mode cipher" command in CLI or by using the cipher pull-down menu in the web browser interface. Cipher suites that contain AES CCMP provide the best security for your wireless LAN, and cipher suites that contain only WEP are the least secure and not recommended.

- AES-CCMP—Based on the Advanced Encryption Standard (AES) defined in the National Institute of Standards and Technology's FIPS Publication 197, AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. AES-CCMP is superior to WEP encryption and is defined in the IEEE 802.11i standard.

- WEP (Wired Equivalent Privacy)

  WEP is an 802.11 standard encryption algorithm originally designed to provide your wireless LAN with the same level of privacy available on a wired LAN. However, the basic WEP construction is flawed, and an attacker can compromise the privacy with reasonable effort.

  TIP Cisco 802.11n radios require that either no encryption or AES-CCMP be configured for proper operation.

- TKIP (Temporal Key Integrity Protocol)

  TKIP is a suite of algorithms surrounding WEP that is designed to achieve the best possible security on legacy hardware built to run WEP. Broadcast key rotation (also known as Group Key Update) allows the access point to generate the best possible random group key and update all key-management capable clients periodically. Wi-Fi Protected Access (WPA) also provides additional options for group key updates.

  See WPA Key Management on page 336 for details on WPA.

IMPORTANT Client devices using static WEP cannot use the access point when you enable broadcast key rotation. Broadcast key rotation is supported when using only key management (such as dynamic WEP (802.1x), WPA with EAP, or preshared key).

Configure Cipher Suites

These sections describe how to configure cipher suites, and additional features such as MIC, TKIP, and broadcast key rotation.

Enable Cipher Suites

Beginning in privileged EXEC mode, follow these steps to enable a cipher suite.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface. The 2.4 GHz radio is radio 0, and the 5 GHz radio is radio 1.

   ```
   interface dot11radio { 0 | 1 }
   ```

3. Enable a cipher suite containing the protection you need.

   Table 101 on page 329 lists guidelines for selecting a cipher suite that matches the type of authenticated key management you configure.

4. (Optional) Select the VLAN that you want enabled for security features.
5. Set the cipher options.

You must configure WPA key management as optional to configure cipher modes `TKIP + WEP 128 or TKIP + WEP 40`.

```
encryption
[vlan vlan-id]
mode ciphers
{[aes | aes-ccm | ckip | tkip]} {[wep128 | wep40]}
```

6. Return to privileged EXEC mode.

   ```
   end
   ```

7. (Optional) Save your entries in the configuration file.

```
copy running-config startup-config
```

Use the `no` form of the encryption command to disable a cipher suite.

Match Cipher Suites with WPA or CCKM

If you configure your access point to use WPA or CCKM authenticated key management, you must select a cipher suite compatible with the authenticated key management type. This table lists the cipher suites that are compatible with WPA and CCKM.

Table 101 - Cipher Suites Compatible with WPA and CCKM

Authenticated Key Management Types	Compatible Cipher Suites
CCKM	encryption mode ciphers wep128 encryption mode ciphers wep40 encryption mode ciphers ckip encryption mode ciphers cmic encryption mode ciphers ckip-cmic encryption mode ciphers tkip encryption mode aes
WPA	encryption mode ciphers tkip encryption mode ciphers tkip wep128 encryption mode ciphers tkip wep40 encryption mode ciphers eas Encryption mode ciphers tkip wep128 and tkip wep-40 can only be used is WPA is configured as optional.

IMPORTANT If using WPA and CCKM as key management, only tkip and aes ciphers are supported. If using only CCKM as key management, ckip, cmic, ckip-cmic, tkip, wep, and aes ciphers are supported.

When you configure the cipher TKIP (not TKIP + WEP 128 or TKIP + WEP 40) for an SSID, the SSID must use WPA or CCKM key management. Client authentication fails on an SSID that uses the cipher TKIP without enabling WPA or CCKM key management.

For a complete description of WPA and instructions for configuring authenticated key management, see WPA Key Management on page 336.

Enable and Disable Broadcast Key Rotation

Broadcast key rotation is disabled by default. Client devices using static WEP cannot use the access point when you enable broadcast key rotation. Broadcast key rotation is supported only when using key management (such as dynamic WEP (802.1x), WPA with EAP, or preshared key).

Beginning in privileged EXEC mode, follow these steps to enable broadcast key rotation.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.
   - The 2.4 GHz 802.11n radio is 0.
   - The 5 GHz 802.11n radio is 1.

   ```
   interface dot11radio { 0 | 1 }
   ```

3. Enable broadcast key rotation.
4. Enter the number of seconds between each rotation of the broadcast key.
5. (Optional) Enter a VLAN that you want to enable for broadcast key rotation.

See Configure Authentication Types on page 331 for detailed instructions on enabling authenticated key management.

```
broadcast-key
change seconds
[ vlan vlan-id ]
[ membership-termination ]
[ capability-change ]
```

6. Return to privileged EXEC mode.

   ```
   end
   ```

7. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the no form of the encryption command to disable broadcast key rotation.

This example enables broadcast key rotation on VLAN 22 and sets the rotation interval to 300 seconds:

```
ap5100# configure terminal
ap5100(config)# interface dot11radio 0
ap5100(config-if)# broadcast-key vlan 22 change 300
ap5100(config-if)# end
```

Configure Authentication Types

This chapter describes how to configure authentication types on the access point.

Topic	Page
Authentication Types	331
WPA Key Management	336
Configure Authentication Types	337
Configure Additional WPA Settings	341
Configure Authentication Hold-off, Timeout, and Interval	345
Create and Apply EAP Method Profiles for the 802.1X Supplicant	347

Authentication Types

The authentication types are tied to the SSIDs that you configure for the access point. If you want to serve different types of client devices with the same access point, you can configure multiple SSIDs.

See Configure Multiple Service Set Identifiers (SSIDs) on page 285 for complete instructions on configuring multiple SSIDs.

Before a wireless client device can communicate on your network through the access point, it must authenticate to the access point. For maximum security, client devices must also authenticate to your network by using MAC-address or EAP authentication, authentication types that rely on an authentication server on your network.

IMPORTANT By default, the access point sends reauthentication requests to the authentication server with the service-type attribute set to authenticate-only. However, some Microsoft IAS servers don't support the authenticate-only service-type attribute. Depending on the user requirements, set the service-type attribute to: dot11 aaa authentication attributes service-type login-user or dot11 aaa authentication attributes service-type framed-user. By default the service type login is sent in the access request.

The access point uses several authentication mechanisms or types and can use more than one at the same time.

Open Authentication to the Access Point

Open authentication allows any device to authenticate and then attempt to communicate with the access point. By using open authentication, any wireless device can authenticate with the access point.

Shared Key Authentication to the Access Point

Cisco provides shared key authentication to comply with the IEEE 802.11b standard. However, because of shared key's security flaws, avoid using it.

During shared key authentication, the access point sends an unencrypted challenge text string to any device attempting to communicate with the access point. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate.

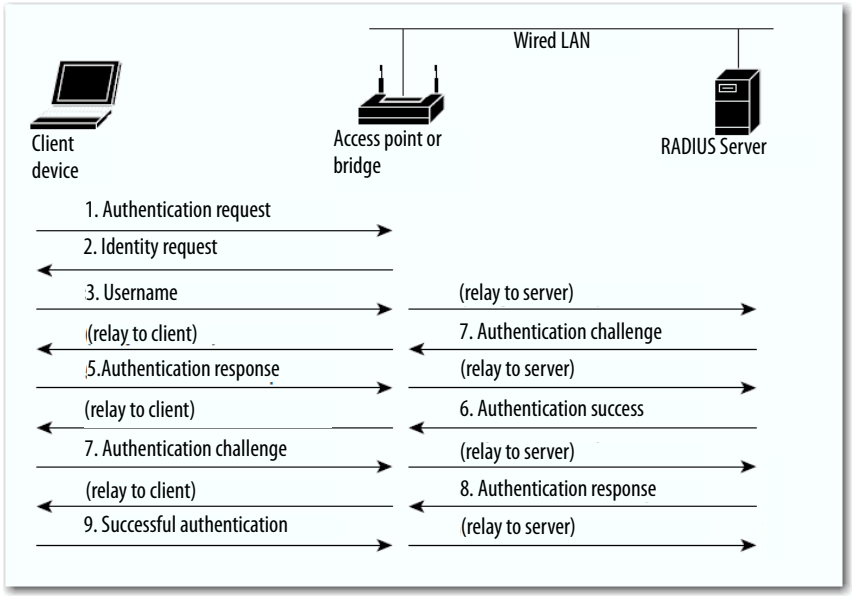
Both the unencrypted challenge and the encrypted challenge can be monitored, however, that leaves the access point open to attack from an intruder who calculates the WEP key by comparing the unencrypted and encrypted text strings. Because of this weakness, shared key authentication can be less secure than open authentication. Like open authentication, shared key authentication does not rely on a RADIUS server on your network.

EAP Authentication to the Network

This authentication type provides the highest level of security for your wireless network. By using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication.

When you enable EAP on your access points and client devices, authentication to the network occurs in the sequence shown in this figure.

Figure 86 - Sequence for EAP Authentication



In Steps 1...9, a wireless client device and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the access point. The RADIUS server sends an authentication challenge to the client.

The client uses a one-way encryption of the user-supplied password to generate a response to the challenge and sends that response to the RADIUS server. By using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, and the client authenticates the RADIUS server.

There is more than one type of EAP authentication, but the access point behaves the same way for each type: it relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device.

See Assigning Authentication Types to an SSID on page 337 for instructions on setting up EAP on the access point.

MAC Address Authentication to the Network

The access point relays the wireless client device's MAC address to a RADIUS server on your network, and the server checks the address against a list of allowed MAC addresses. Intruders can create counterfeit MAC addresses, so MAC-based authentication is less secure than EAP authentication.

However, MAC-based authentication provides an alternate authentication method for client devices that don't have EAP capability.

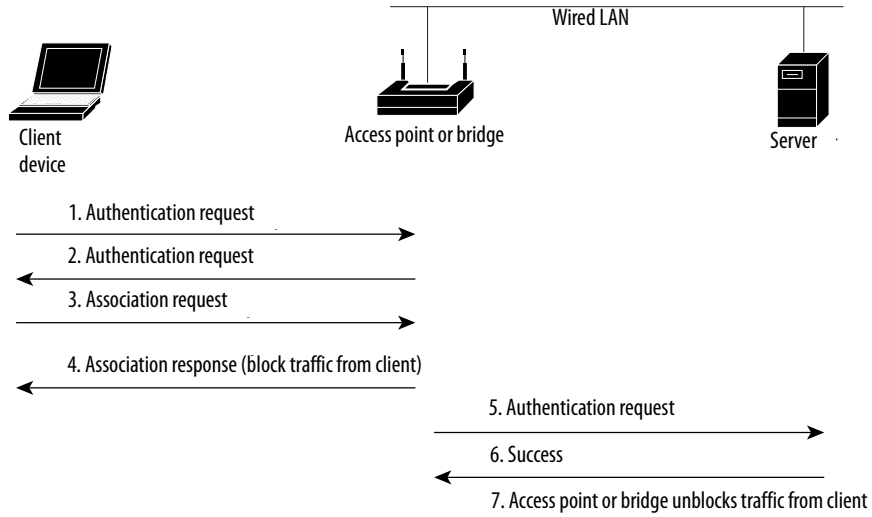
See the Assigning Authentication Types to an SSID on page 337 for instructions on enabling MAC-based authentication.

TIP If you don't have a RADIUS server on your network, you can create a list of allowed MAC addresses on the access point's Advanced Security: MAC Address Authentication page. Devices with MAC addresses not on the list are not allowed to authenticate.

TIP If MAC-authenticated clients on your wireless LAN roam frequently, you can enable a MAC authentication cache on your access points. MAC authentication caching reduces overhead because the access point authenticates devices in its MAC-address cache without sending the request to your authentication server. See Configure MAC Authentication Caching on page 343 for instructions on enabling this feature.

This figure shows the authentication sequence for MAC-based authentication.

Figure 87 - Sequence for MAC-Based Authentication



Combine MAC-Based, EAP, and Open Authentication

You can set up the access point to authenticate client devices by using a combination of MAC-based and EAP authentication. When you enable this feature, client devices that associate to the access point by using 802.11 open authentication first attempt MAC authentication; if MAC authentication succeeds, the client device joins the network. If MAC authentication fails, EAP authentication takes place.

See the Assigning Authentication Types to an SSID on page 337 for instructions on setting up this combination of authentications.

Using CCKM for Authenticated Clients

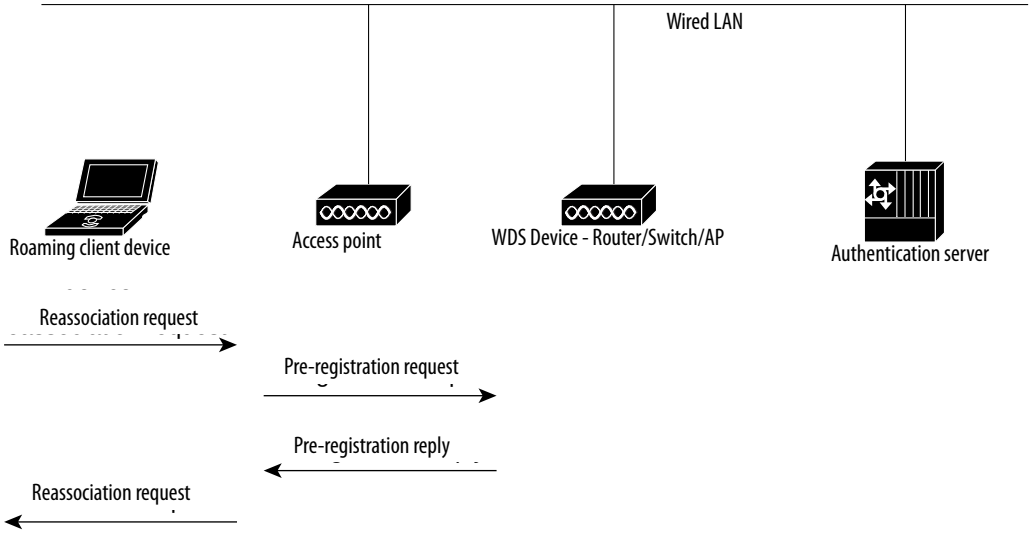
By using Cisco Centralized Key Management (CCKM), authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides Wireless Domain Services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. When a client device roams, the WDS access point forwards the client's security credentials to the new access point, and the reassociation process is reduced to a two-packet exchange between the roaming client and the new access point.

- See the Assigning Authentication Types to an SSID on page 337 for instructions on enabling CCKM on your access point.
- See the Configure Access Points to Use the WDS Device on page 361 for detailed instructions on setting up a WDS access point on your wireless LAN.

IMPORTANT The RADIUS-assigned VLAN feature is not supported for client devices that associate by using SSIDs with CCKM enabled.

This figure shows the reassociation process by using CCKM.

Figure 88 - Client Reassociation by Using CCKM



WPA Key Management

Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and can be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.

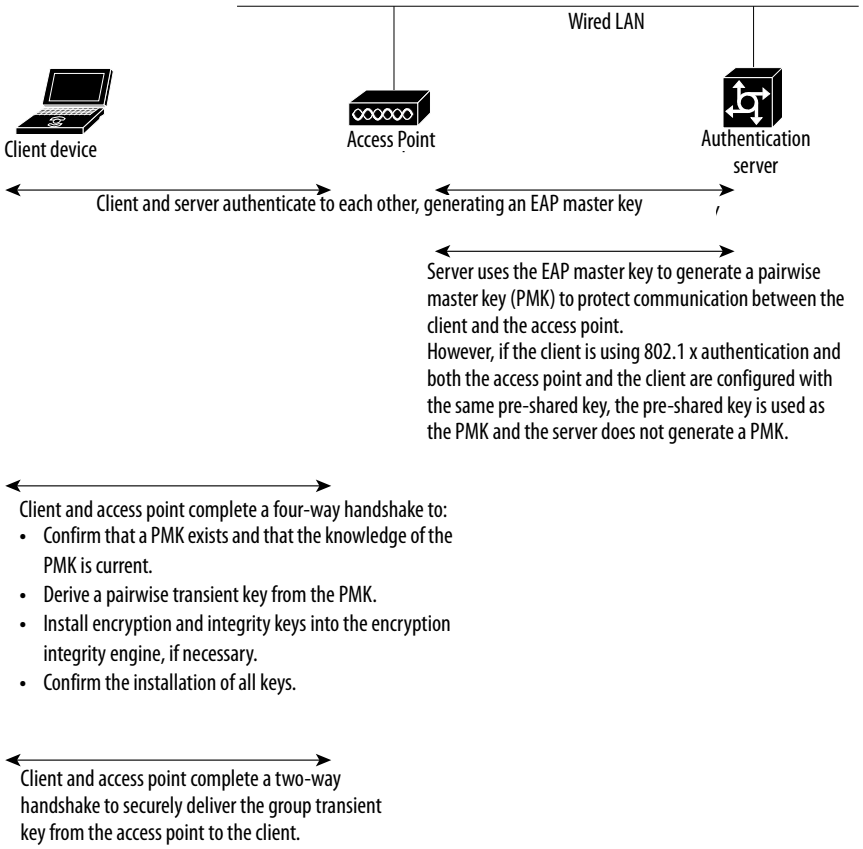
WPA key management supports two mutually exclusive management types: WPA and WPA-Pre-shared key (WPA-PSK). By using WPA key management, clients and the authentication server authenticate to each other by using an EAP authentication method, and the client and server generate a pair-wise master key (PMK). By using WPA, the server generates the PMK dynamically and passes it to the access point. When using WPA-PSK, however, you configure a pre-shared key on both the client and the access point, and that pre-shared key is used as the PMK.

IMPORTANT Unicast and multicast cipher suites advertised in WPA information element (and negotiated during 802.11 association) can be potentially mismatched with the cipher suite supported in an explicitly assigned VLAN. If the RADIUS server assigns a new vlan ID that uses a different cipher suite from the previously negotiated cipher suite, there is no way for the access point and client to switch back to the new cipher suite. Currently, the WPA and CCKM protocols does not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the client device is disassociated from the wireless LAN.

See Assigning Authentication Types to an SSID on page 337 for instructions on configuring WPA key management on your access point.

This figure shows the WPA key management process.

Figure 89 - WPA Key Management Process



Configure Authentication Types

This section describes how to configure authentication types. You attach configuration types to the access point's SSIDs. See Configure Multiple Service Set Identifiers (SSIDs) on page 285 for details on setting up multiple SSIDs.

TIP There are no default SSIDs for the wireless access point.

Assigning Authentication Types to an SSID

Beginning in privileged EXEC mode, follow these steps to configure authentication types for SSIDs.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Create an SSID and enter SSID configuration mode for the new SSID.

   The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.

```
dot11 ssid ssid-string
```

3. (Optional) Set the authentication type to open for this SSID.

   Open authentication allows any device to authenticate and then attempt to communicate with the access point.

   ```
   authentication open
   [mac-address list-name [alternate]]
   [[optional] eap list-name]
   ```

   a. (Optional) Set the SSID's authentication type to open with MAC address authentication.

      The access point forces all client devices to perform MAC-address authentication before they are allowed to join the network. For list-name, specify the authentication method list.

      Use the alternate keyword to allow client devices to join the network by using either MAC or EAP authentication; clients that successfully complete either authentication are allowed to join the network.

   b. (Optional) Set the SSID's authentication type to open with EAP authentication.

      The access point forces all client devices to perform EAP authentication before they are allowed to join the network. For list-name, specify the authentication method list.

Use the optional keyword to allow client devices by using either open or EAP authentication to associate and become authenticated. This setting is used mainly by service providers that require special client accessibility.

TIP An access point configured for EAP authentication forces all client devices that associate to perform EAP authentication. Client devices that don't use EAP cannot use the access point.

Because of shared key's security flaws, We recommend that you avoid using it. You can assign shared key authentication to only one SSID.

4. (Optional) Set the authentication type for the SSID to Network-EAP.

```
authentication network-eap list-name
[mac-address list-name]
```

When the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. However, the access point does not force all client devices to perform EAP authentication.

a. (Optional) Set the SSID's authentication type to Network-EAP with MAC address authentication.
b. For list-name, specify the authentication method list.

All client devices that associate to the access point are required to perform MAC-address authentication.

5. (Optional) Set the authentication type for the SSID to WPA, CCKM, or both.

```
authentication key-management { [wpa] [cckm] } [
optional ]
```

If you use the optional keyword, client devices other than WPA and CCKM clients can use this SSID. If you don't use the optional keyword, only WPA or CCKM client devices are allowed to use the SSID.

- To enable CCKM for an SSID, you must also enable Network-EAP authentication. When CCKM and Network EAP are enabled for an SSID, client devices using LEAP, EAP-FAST, PEAP/GTC, MSPEAP, EAP-TLS, and EAP-FAST can authenticate by using the SSID.
- To enable WPA for an SSID, you must also enable Open authentication or Network-EAP or both.

When you enable both WPA and CCKM for an SSID, you must enter wpa first and cckm second. Any WPA client can attempt to authenticate, but only CCKM voice clients can attempt to authenticate.

Before you can enable CCKM or WPA, you must set the encryption mode for the SSID's VLAN to one of the cipher suite options. To

enable both CCKM and WPA, you must set the encryption mode to a cipher suite that includes TKIP.

See the Configure Cipher Suites on page 327 for instructions on configuring the VLAN encryption mode.

If you enable WPA for an SSID without a pre-shared key, the key management type is WPA. If you enable WPA with a pre-shared key, the key management type is WPA-PSK.

- See the Configure Additional WPA Settings on page 341 for instructions on configuring a pre-shared key.
- See Configure Wireless Domain Services and Fast Secure Roaming on page 349 for detailed instructions on setting up your wireless LAN to use CCKM and a subnet context manager.

6. Return to privileged EXEC mode.

   ```
   end
   ```

7. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the no form of the SSID commands to disable the SSID or to disable SSID features.

This example sets the authentication type for the `SSID batman` to Network-EAP with CCKM authenticated key management. Client devices using the batman SSID authenticate by using the adam server list. After they are authenticated, CCKM-enabled clients can perform fast reassociations by using CCKM.

```
ap1200# configure terminal
ap1200(config)# dot11 ssid batman
ap1200(config-ssid)# authentication network-eap
adam
ap1200(config-ssid)# authentication key-management
cckm optional
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# end
```

Configure Additional WPA Settings

Use two optional settings to configure a pre-shared key on the access point and adjust the frequency of group key updates.

Set a Pre-shared Key

To support WPA on a wireless LAN where 802.1X-based authentication is not available, you must configure a pre-shared key on the access point. You can enter the pre-shared key as ASCII or hexadecimal characters. If you enter the key as ASCII characters, you enter between 8...63 characters, and the access point expands the key. If you enter the key as hexadecimal characters, you must enter 64 hexadecimal characters.

Configure Group Key Updates

In the last step in the WPA process, the access point distributes a group key to the authenticated client device. You can use these optional settings to configure the access point to change and distribute the group key based on client association and disassociation:

- Membership termination

  The access point generates and distributes a new group key when any authenticated device disassociates from the access point. This feature keeps the group key private for associated devices, but it can generate some overhead traffic if clients on your network roam frequently among access points.

- Capability change

  The access point generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static-WEP clients associated to the access point.

Beginning in privileged EXEC mode, follow these steps to configure a WPA pre-shared key and group key update options.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter SSID configuration mode for the SSID.

   ```
   dot11 ssid ssid-string
   ```

3. Enter a pre-shared key for client devices by using WPA that also use static WEP keys.

   ```
   wpa-psk { hex | ascii } [ 0 | 7 ] encryption-key
   ```

   Enter the key by using either hexadecimal or ASCII characters. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the access point expands the key for you. You can enter a maximum of 63 ASCII characters.

1. Enter interface configuration mode for the radio interface.

   ```
   interface dot11radio { 0 | 1 }
   ```

   - The 2.4 GHz 802.11n radio is 0.
   - The 5 GHz 802.11n radio is 1.

2. Enter the ssid defined in Step 2 to assign the ssid to the selected radio interface.

   ```
   ssid ssid-string
   ```

3. Return to privileged EXEC mode.

   ```
   exit
   ```

4. Use the broadcast key rotation command to configure additional updates of the WPA group key.

   ```
   broadcast-key [ vlan vlan-id ]
   { change seconds }
   [ membership-termination ]
   [ capability-change ]
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

This example shows how to configure a pre-shared key for clients by using WPA with group key update options:

```
ap# configure terminal
ap(config)# dot11 ssid batman
ap(config-ssid)# wpa-psk ascii batmobile65
ap(config)# interface dot11radio 0
ap(config-ssid)# ssid batman
ap(config-if)# exit
ap(config)# broadcast-key vlan 87 membership-
termination capability-change
```

Configure MAC Authentication Caching

If MAC-authenticated clients on your wireless LAN roam frequently, you can enable a MAC authentication cache on your access points. MAC authentication caching reduces overhead because the access point authenticates devices in its MAC-address cache without sending the request to your authentication server. When a client device completes MAC authentication to your authentication server, the access point adds the client's MAC address to the cache.

Beginning in privileged EXEC mode, follow these steps to enable MAC authentication caching.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable MAC authentication caching on the access point.

   ```
   dot11 aaa mac-authen filter-cache [timeout seconds]
   ```

Use the **timeout** option to configure a timeout value for MAC addresses in the cache. Enter a value from 30...65555 seconds. The default value is 1800 (30 minutes). When you enter a timeout value, MAC-authentication caching is enabled automatically.

3. Return to privileged EXEC mode.

   ```
   exit
   ```

4. Show entries in the MAC-authentication cache. Include client MAC addresses to show entries for specific clients.

   ```
   show dot11 aaa mac-authen filter-cache [address]
   ```

5. Clear all entries in the cache. Include client MAC addresses to clear specific clients from the cache.

   ```
   clear dot11 aaa mac-authen filter-cache [address]
   ```

6. Return to privileged EXEC mode.

   ```
   end
   ```

7. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

This example shows how to enable MAC authentication caching with a one-hour timeout:

```
ap# configure terminal
ap(config)# dot11 aaa mac-authen filter-cache
timeout 3600
ap(config)# end
```

Use the no form of the `dot11 aaa mac-authen filter-cache` command to disable MAC authentication caching. For example:

```
no dot11 aaa authentication mac-authen filter-cache
```

Configure Authentication Hold-off, Timeout, and Interval

Beginning in privileged EXEC mode, follow these steps to configure hold-off times, reauthentication periods, and authentication timeouts for client devices authenticating through your access point.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter the number of seconds a client device must wait before it can reattempt to authenticate following a failed authentication.

   ```
   dot11 holdoff-time seconds
   ```

   The hold-off time is invoked when a client fails three login attempts or fails to respond to three authentication requests from the access point. Enter a value from 1...65555 seconds.

3. Enter the number of seconds the access point must wait for a client to reply to an EAP/dot1x message before the authentication fails. Enter a value from 1...120 seconds.

   ```
   dot1x timeout supp-response seconds [local]
   ```

   The RADIUS server can be configured to send a different timeout value that overrides the one that is configured. Enter the `local` keyword to configure the access point to ignore the RADIUS server value and use the configured value.

   The optional `no` keyword resets the timeout to its default state, 30 seconds.

4. Enter interface configuration mode for the radio interface.

   ```
   interface dot11radio { 0 | 1 }
   ```

   - The 2.4 GHz 802.11n radio is 0.
   - The 5 GHz 802.11n radio is 1.

5. Enter the interval in seconds that the access point waits before forcing an authenticated client to reauthenticate.

   ```
   dot1x reauth-period { seconds | server }
   ```

   Enter the server keyword to configure the access point to use the reauthentication period specified by the authentication server. If you use this option, configure your authentication server with RADIUS attribute 27, Session-Timeout.

   This attribute sets the maximum number of seconds of service to be provided to the client before termination of the session or prompt. The server sends this attribute to the access point when a client device performs EAP authentication.

TIP If you configure both MAC address authentication and EAP authentication for an SSID, the server sends the Session-Timeout attribute for both MAC and EAP authentications for a client device. The access point uses the Session-Timeout attribute for the last authentication that the client performs.

For example, if a client performs MAC address authentication and then performs EAP authentication, the access point uses the server's Session-Timeout value for the EAP authentication.

To avoid confusion when using a Session-Timeout attribute, configure the same Session-Timeout value on your authentication server for both MAC and EAP authentication.

6. Configure a TKIP MIC failure holdtime.

   ```
   countermeasure tkip hold-time seconds
   ```

   If the access point detects two MIC failures within 60 seconds, it blocks all the TKIP clients on that interface for the holdtime period.

7. Return to privileged EXEC mode.

   ```
   end
   ```

8. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the no form of these commands to reset the values to default settings.

Create and Apply EAP Method Profiles for the 802.1X Supplicant

This section describes the optional configuration of an EAP method list for the 802.1X supplicant. Configuring EAP method profiles enables the supplicant not to acknowledge some EAP methods, even though they are available on the supplicant. For example, if a RADIUS server supports EAP-FAST and LEAP, under certain configurations, the server can initially employ LEAP instead of a more secure method. If no preferred EAP method list is defined, the supplicant supports LEAP, but it can be advantageous to force the supplicant to force a more secure method such as EAP-FAST.

- Use the `no` command to negate a command or set its defaults.
- Use the show eap registrations method command to view the currently available (registered) EAP methods.
- Use the show eap sessions command to view existing EAP sessions.

See Create a Credentials Profile on page 208 for additional information about the 802.1X supplicant.

Create an EAP Method Profile

Beginning in privileged exec mode, follow these steps to define a new EAP profile.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter a name for the profile.

   ```
   eap profile profile name
   ```

3. (Optional)—Enter a description for the EAP profile.

   ```
   description
   ```

4. Enter an allowed EAP method or methods.

   ```
   method fast
   ```

   TIP Although they appear as sub-parameters, EAP-GTC, EAP-MD5, and EAP-MSCHAPV2 are intended as inner methods for tunneled EAP authentication and must not be used as the primary authentication method.

5. Return to the privileged EXEC mode.

   ```
   end
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running config startup-config
   ```

Apply an EAP Profile to an Uplink SSID

This operation typically applies to workgroup bridges or access points. Beginning in the privileged exec mode, follow these steps to apply an EAP profile to the uplink SSID.

1. Enter the global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.

   ```
   interface dot11radio {0 | 1}
   ```

   - The 2.4 GHz 802.11n radio is 0.
   - The 5 GHz 802.11n radio is 1.

3. Assign the uplink SSID to the radio interface.

   ```
   ssid ssid
   ```

4. Return to the configure terminal mode.

   ```
   exit
   ```

5. Enter the profile preconfigured profile name.

   ```
   eap profile profile
   ```

6. Return to the privileged EXEC mode.

   ```
   end
   ```

7. (Optional) Save your entries in the configuration file.

   ```
   copy running config startup-config
   ```

Configure Wireless Domain Services and Fast Secure Roaming

This chapter describes how to configure your access points for wireless domain services (WDS) and fast secure roaming of client devices.

Topic	Page
WDS	349
Configure WDS	353
Configure Fast Secure Roaming	364
Management Frame Protection	367

WDS

When you configure Wireless Domain Services on your network, access points on your wireless LAN use the WDS device (either an access point, an Integrated Services Router, or a switch configured as the WDS device) to provide fast, secure roaming for client devices and to participate in radio management.

An access point configured as the WDS device supports up to 60 participating access points, an Integrated Services Router (ISR) configured as the WDS devices supports up to 100 participating access points.

TIP A single access point supports up to 16 mobility groups.

Fast, secure roaming provides rapid reauthentication when a client device roams from one access point to another, preventing delays in voice and other time-sensitive applications.

Role of the WDS Device

The WDS device performs several tasks on your wireless LAN:

- Advertises its WDS capability and participates in electing the best WDS device for your wireless LAN. When you configure your wireless LAN for WDS, you set up one device as the main WDS candidate and one or more additional devices as back-up WDS candidates. If the main WDS device goes off line, one of the back-up WDS devices takes its place.
- Authenticates all access points in the subnet and establishes a secure communication channel with each of them.

- Acts as a pass-through for all 802.1x-authenticated client devices associated to participating access points.
- Registers all client devices in the subnet that use dynamic keying, establishes session keys for them, and caches their security credentials. When a client roams to another access point, the WDS device forwards the client's security credentials to the new access point.

This table lists the number of participating access points supported by the platforms that can be configured as a WDS device.

Table 102 - Participating Access Points Supported by WDS Devices

Unit Configured as WDS Device	Participating Access Points Supported
Access point that also serves client devices	30
Access point with radio interfaces disabled	60

Role of Access Points by Using the WDS Device

The access points on your wireless LAN interact with the WDS device in these activities:

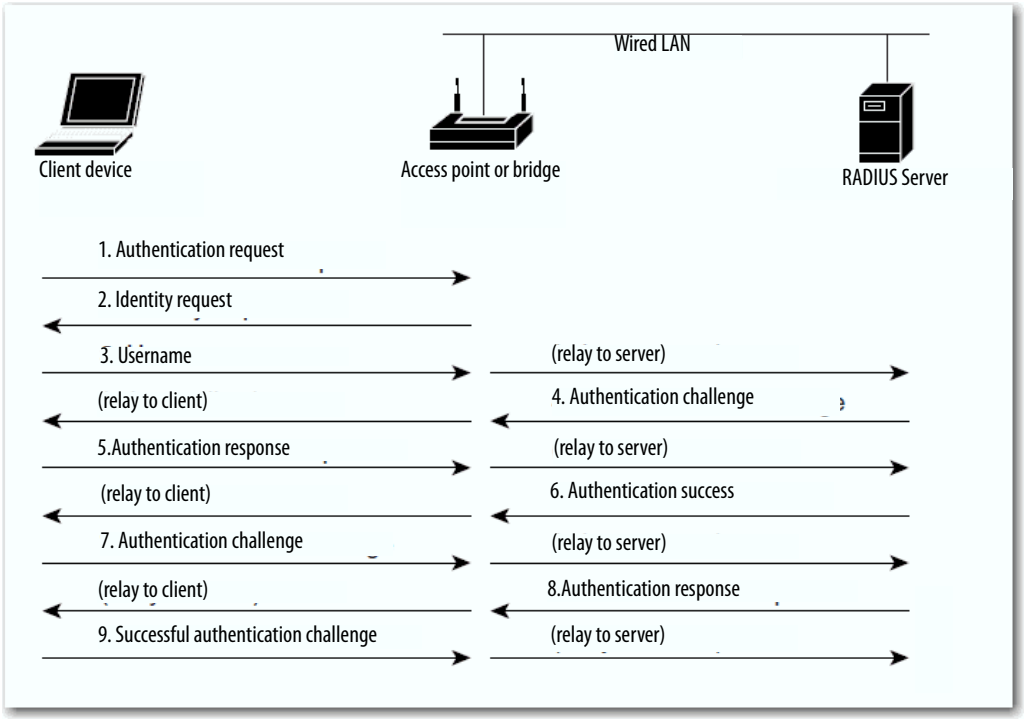
- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.
- Report radio data to the WDS device.

Fast Secure Roaming

Access points in many wireless LANs serve mobile client devices that roam from access point to access point throughout the installation. Some applications running on client devices require fast reassociation when they roam to a different access point. Voice applications, for example, require seamless roaming to prevent delays and gaps in conversation.

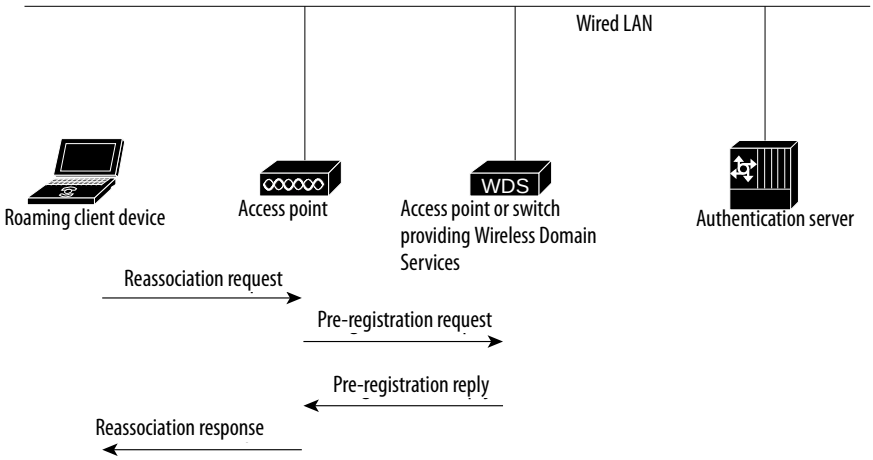
During normal operation, EAP-enabled client devices mutually authenticate with a new access point by performing a complete EAP authentication, including communication with the main RADIUS server.

Figure 90 - Client Authentication by Using a RADIUS Server



When you configure your wireless LAN for fast, secure roaming, however, EAP-enabled client devices roam from one access point to another without involving the main RADIUS server. Using Cisco Centralized Key Management (CCKM), a device configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client so quickly that there is no perceptible delay in voice or other time-sensitive applications. This figure shows client authentication by using CCKM.

Figure 91 - Client Reassociation by Using CCKM and a WDS Access Point



The WDS device maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the client sends a reassociation request to the new access point, and the new access point relays the request to the WDS device.

The WDS device forwards the client's credentials to the new access point, and the new access point sends the reassociation response to the client. Only two packets pass between the client and the new access point, greatly shortening the reassociation time. The client also uses the reassociation response to generate the unicast key.

See Configure Fast Secure Roaming on page 364 for instructions on configuring access points to support fast, secure roaming.

Configure WDS

This section describes how to configure WDS on your network.

Topic	Page
Guidelines for WDS	353
Requirements for WDS	353
Configuration Overview	353
Configure Access Points as Potential WDS Devices	355
Configure Access Points to Use the WDS Device	361
Configure WDS-Only Mode	362
Configure WDS-Only Mode	362
View WDS Information	363
Debug Messages	364

Guidelines for WDS

Follow these guidelines when configuring WDS:

- A WDS access point that also serves client devices supports up to 30 participating access points, but a WDS access point with radios disabled supports up to 60 participating access points.
- The WDS mode supports only up to 60 infrastructure access points and 1200 clients.
- Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to return (fall back) to repeater mode in case of Ethernet failure.

Requirements for WDS

To configure WDS, you must have these items on your wireless LAN:

- At least one access point that you can configure as the WDS device
- An authentication server (or an access point configured as a local authenticator)

Configuration Overview

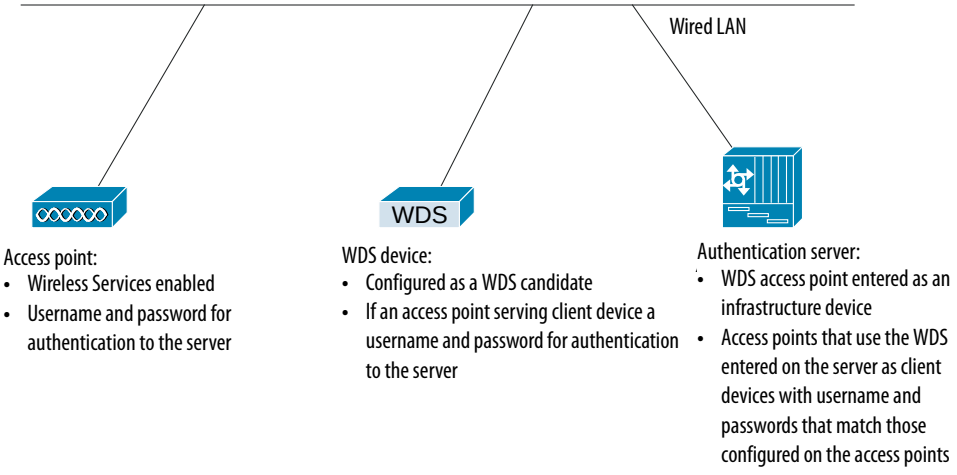
You must complete three major steps to set up WDS and fast, secure roaming.

1. Configure access points as potential WDS devices. This chapter provides instructions for configuring an access point as a WDS device.
2. Configure the rest of your access points to use the WDS device.

3. Configure the authentication server on your network to authenticate the WDS device and the access points that use the WDS device.

This figure shows the required configuration for each device that participates in WDS.

Figure 92 - Configurations on Devices Participating in WDS



Configure Access Points as Potential WDS Devices

For the main WDS candidate, configure an access point that does not serve a large number of client devices. If client devices associate to the WDS access point when it starts up, the clients can wait several minutes to be authenticated.

When WDS is enabled, the WDS access point performs and tracks all authentications. Therefore, you must configure EAP security settings on the WDS access point.

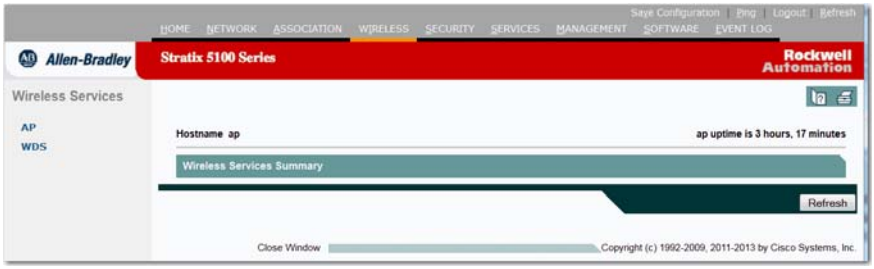
See Configure Authentication Types on page 337 for instructions on configuring EAP on the access point.

On the access point that you want to configure as your primary WDS access point, follow these steps to configure the access point as the main WDS candidate.

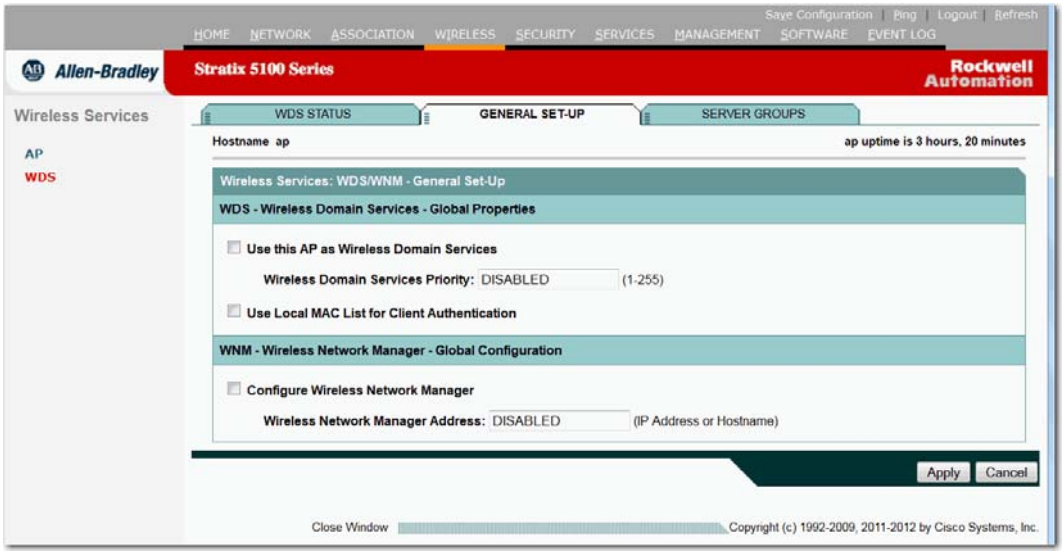
1. Go to the Wireless Services Summary page.

This figure shows the Wireless Services Summary page.

Figure 93 - Wireless Services Summary Page



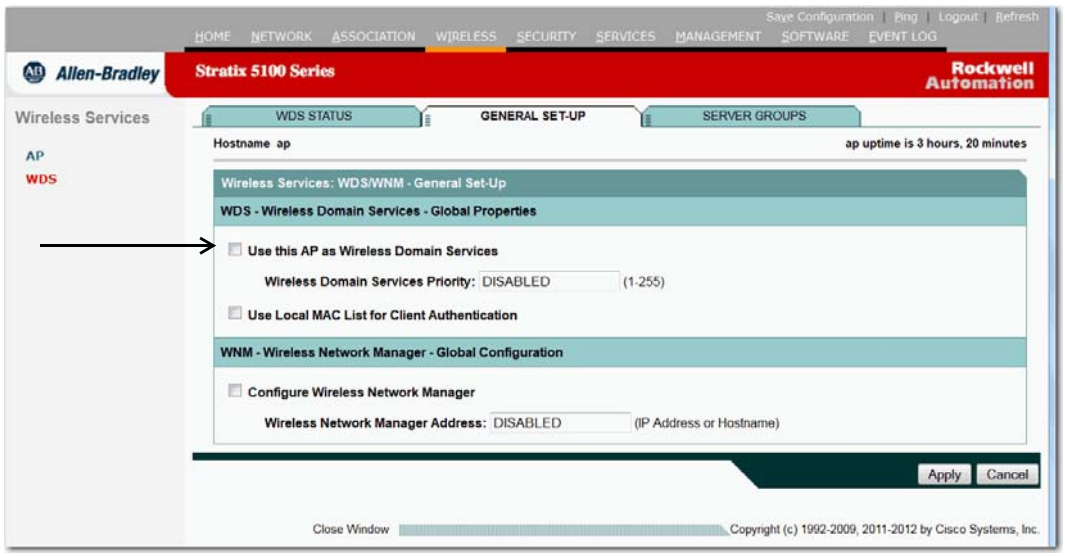
2. Click WDS to go to the WDS/WNM Summary page.



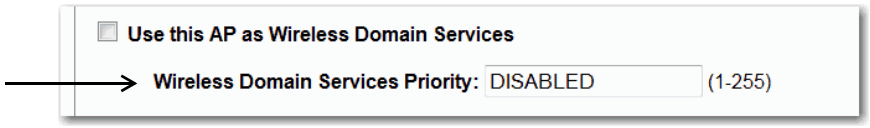
3. On the WDS/WNM Summary page, click General Setup to go to the WDS/WNM General Setup page.

   The WDS/WNM General Setup page appears.

Figure 94 - WDS/WNM General Setup Page



4. Check the Use this AP as Wireless Domain Services check box.
5. In the Wireless Domain Services Priority field, enter a priority number from 1...255 to set the priority of this WDS candidate.



The WDS access point candidate with the highest number in the priority field becomes the acting WDS access point. For example, if one WDS candidate is assigned priority 255 and one candidate is assigned priority 100, the candidate with priority 255 becomes the acting WDS access point.

6. (Optional) Check Use Local MAC List for Client Authentication.

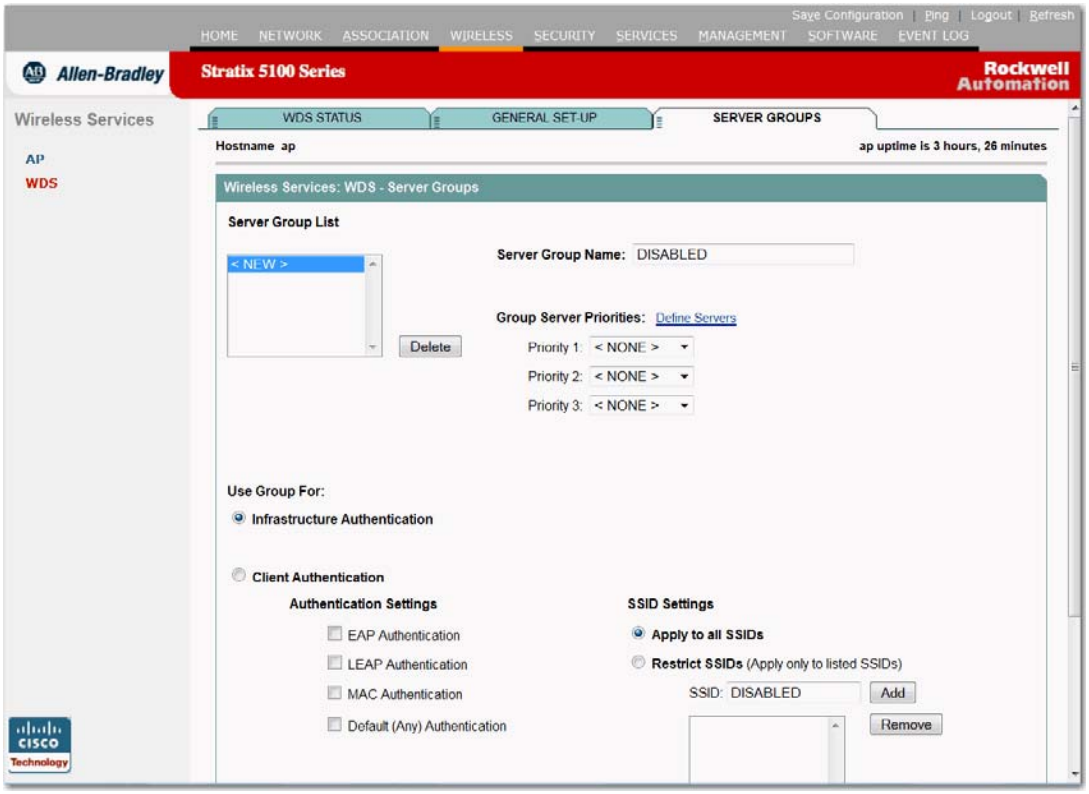
   This authenticates client devices by using MAC addresses in the local list of addresses configured on the WDS device. If you don't check this check box, the WDS device uses the server specified for MAC-address authentication on the Server Groups page to authenticate clients based on MAC addresses.

   TIP Selecting the Use Local MAC List for Client Authentication check box does not force client devices to perform MAC-based authentication. It provides a local alternative to server-based MAC-address authentication.

7. Click Apply.
8. Go to the WDS Server Groups page, click Server Groups.

The WDS Server Groups Page appears.

Figure 95 - WDS Server Groups Page



Configure a Group of Servers

Follow these instructions to create a group of servers to be used for 802.1x authentication for the infrastructure devices (access points) that use the WDS access point.

1. Enter a group name in the Server Group Name field.
2. From the Priority 1 pull-down menu, choose the primary server.

   If a server that you need to add to the group does not appear in the Priority pull-down menus, click Define Servers to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.

   TIP If you don't have an authentication server on your network, you can configure an access point or an ISR as a local authentication server. See Configure an Access Point as a Local Authenticator on page 303 for configuration instructions.

3. (Optional) Choose backup servers from the Priority 2 and 3 pull-down menus.
4. Click Apply.

5. Configure the list of servers to be used for 802.1x authentication for client devices.

   You can specify a separate list for clients by using a certain type of authentication, such as EAP, LEAP, PEAP, or MAC-based, or specify a list for client devices by using any type of authentication.

6. Enter a group name for the server or servers in the Server Group Name field.

7. Choose the primary server from the Priority 1 pull-down menu.

   If a server that you need to add to the group does not appear in the Priority pull-down menus, click Define Servers to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.

8. (Optional) Choose backup servers from the Priority 2 and 3 pull-down menus.

9. (Optional) Choose Restrict SSIDs to limit use of the server group to client devices by using specific SSIDs.

10. Enter an SSID in the SSID field and click Add.

    To remove an SSID, highlight it in the SSID list and click Remove.

11. Click Apply.

12. Configure the WDS access point for LEAP authentication.

    See Configure Authentication Types on page 331 for instructions on configuring LEAP.

TIP If your WDS access point serves client devices, follow the instructions in the Configure Access Points to Use the WDS Device on page 361 to configure the WDS access point to use the WDS.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the Configure Access Points as Potential WDS Devices on page 355:

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 200 interface bvi1
AP(config)# wlccp authentication-server
infrastructure infra_devices
AP(config)# wlccp authentication-server client any
client_devices
AP(config-wlccp-auth)# ssid fred
AP(config-wlccp-auth)# ssid ginger
AP(config)# end
```

In this example, infrastructure devices are authenticated by using server group infra_devices; client devices by using SSIDs fred or ginger are authenticated by using server group client_devices.

For complete descriptions of the commands used in this example, see the Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Guide.

Configure Access Points to Use the WDS Device

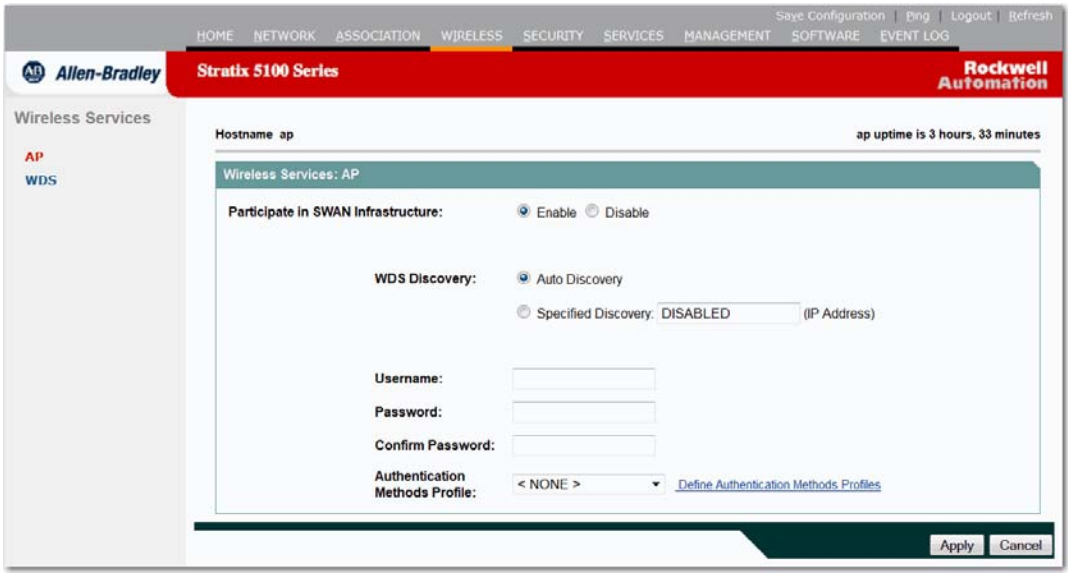
To participate in WDS, infrastructure access points run the same version of IOS as the one that WDS runs.

Follow these steps to configure an access point to authenticate through the WDS device and participate in WDS.

1. Browse to the Wireless Services Summary page.
2. Click AP to browse to the Wireless Services AP page.

This Wireless Services page appears.

Figure 96 - Wireless Services AP Page



3. Click Enable for the Participate in SWAN Infrastructure setting.
4. In the Username field, enter a username for the access point.

   This username must match the username that you create for the access point on your authentication server.
5. In the Password field, enter a password for the access point, and enter the password again in the Confirm Password field.

This password must match the password that you create for the access point on your authentication server.

6. Click Apply.

The access points that you configure to interact with the WDS automatically perform these steps:

- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the Configure Access Points to Use the WDS Device on page 361:

```
AP# configure terminal
AP(config)# wlccp ap username APWestWing password 7
wes7win8
AP(config)# end
```

In this example, the access point is enabled to interact with the WDS device, and it authenticates to your authentication server by using APWestWing as its username and wes7win8 as its password. You must configure the same username and password pair when you set up the access point as a client on your authentication server.

For complete descriptions of the commands used in this example, see the Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Guide.

Configure WDS-Only Mode

WDS access points can operate in WDS-only mode by using the `wlccp wds mode wds-only` command. After issuing this command and reloading, the access point starts working in the WDS-only mode.

- In WDS-only mode, the dot11 subsystems are not initialized and the dot11 interface related commands cannot be configured.
- In WDS-only mode, the WDS supports up to 60 infrastructure access points and up to 1200 clients. Use the `no` form of this command to turn off WDS-only mode. Use the `show wlccp wds` command to display the working mode of the WDS access point.

- To set the WDS access point to operate in both AP and WDS modes, use the `no wlccp wds mode wds-only` command and use the `write erase` command to reload the access point immediately.

After the access point reloads, the dot11 radio subsystems initialize. The access point and WDS associate directly to wireless clients. In this mode, the WDS supports 30 infrastructure access points and 600 clients in addition to 20 direct wireless client associations.

View WDS Information

On the web browser interface, browse to the Wireless Services Summary page to view a summary of WDS status.

On CLI in privileged exec mode, use these commands to view information about the current WDS device and other access points participating in CCKM:

Command	Description
`show wlccp ap`	Use this command on access points participating in CCKM to display the WDS device's MAC address, the WDS device's IP address, the access point's state (authenticating, authenticated, or registered), the IP address of the infrastructure authenticator, and the IP address of the client device (MN) authenticator.
`show wlccp wds { ap | mn } [ detail ] [ mac-addr` *`mac-address`* `]`	On the WDS device use only this command to display cached information about access points and client devices. • ap— access points participating in CCKM. – The command provides each access point's MAC address, IP address, state (authenticating, authenticated, or registered), and lifetime (seconds remaining before the access point must reauthenticate). – Use the `mac-addr` option for information about a specific access point. • mn— cached information about client devices, also called mobile nodes. – The command provides each client's MAC address, IP address, the client associated access point (cur-AP), and state (authenticating, authenticated, or registered). – The detail option provides the client's lifetime (seconds remaining before the client must reauthenticate), SSID, and VLAN ID. – Use the `mac-addr` option to display information about a specific client device. • If you enter only `show wlccp wds`, the access point's IP address, MAC address, priority, and interface state (administratively standalone, active, back-up, candidate, or WDS-only) appear. • If the state is backup, the `show wlccp wds` command provides the current WDS device's IP address, MAC address, and priority. • If the state is WDS-only, the `show wlccp wds` command provides the device's MAC address, IP address, interface state, access point count, and mobile node count.

Debug Messages

In privileged exec mode, use these debug commands to control the display of debug messages for devices interacting with the WDS device:

Table 103 - Debug Commands

Command	Description
`debug wlccp ap {mn | wds-discovery | state}`	Use this command to turn on display of debug messages related to client devices (mn), the WDS discovery process, and access point authentication to the WDS device (state).
`debug wlccp dump`	Use this command to perform a dump of WLCCP packets received and sent in binary format.
`debug wlccp packet`	Use this command to turn on display of packets to and from the WDS device.
`debug wlccp wds [aggregator | authenticator | nm | state | statistics]`	Use this command and its options to turn on display of WDS debug messages. Use the statistics option to turn on display of failure statistics.
`debug wlccp wds authenticator {all | dispatcher | mac-authen | process | rxdata | state-machine | txdata}`	Use this command and its options to turn on display of WDS debug messages related to authentication.

Configure Fast Secure Roaming

After you configure WDS, access points configured for CCKM can provide fast, secure roaming for associated client devices. This section describes how to configure fast, secure roaming on your wireless LAN.

Requirements for Fast Secure Roaming

To configure fast secure roaming, you must have these items on your wireless LAN:

- At least one access point, ISR, or switch (equipped with a WLSM) configured as the WDS device
- Access points configured to participate in WDS
- Access points configured for fast, secure roaming
- An authentication server (or an access point, ISR, or switch configured as a local authenticator)
- Cisco Aironet client devices, or Cisco-compatible client devices that comply with Cisco Compatible Extensions (CCX) version 2 or later

For instructions on configuring WDS, refer to the Configure WDS on page 353.

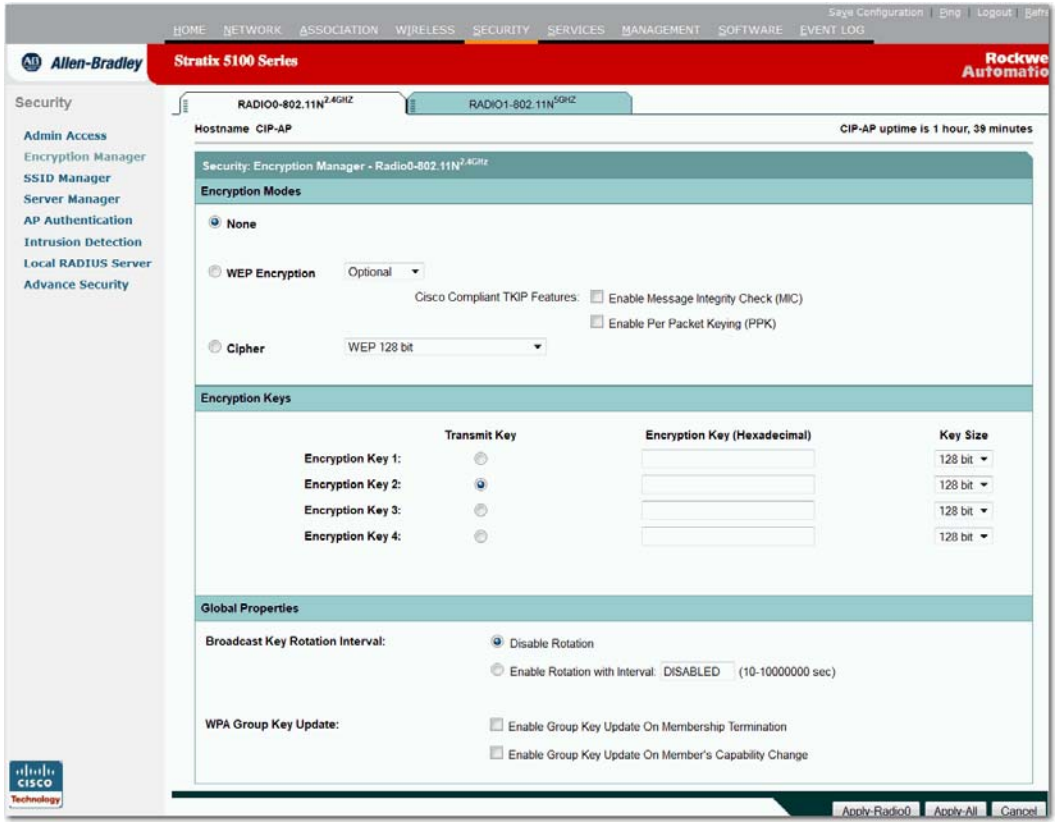
Configure Access Points to Support Fast Secure Roaming

To support fast, secure roaming, the access points on your wireless LAN must be configured to participate in WDS and they must allow CCKM authenticated key management for at least one SSID. Follow these steps to configure CCKM for an SSID.

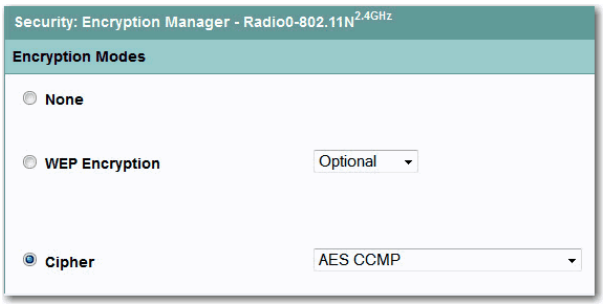
1. Browse to the Encryption Manager page on the access point GUI.

   This figure shows the top section of the Encryption Manager page.

Figure 97 - Encryption Manager Page



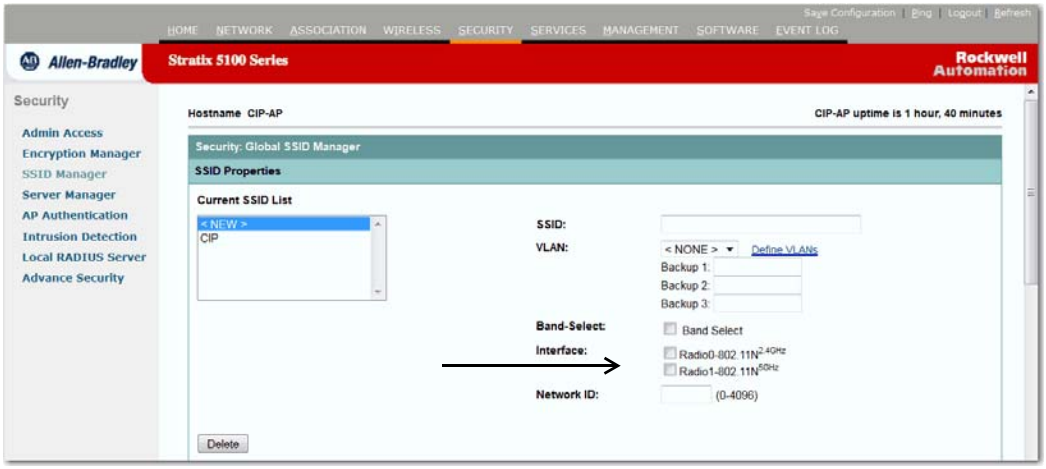
2. Click Cipher.
3. From the Cipher pull-down menu, choose AES-CCMP.



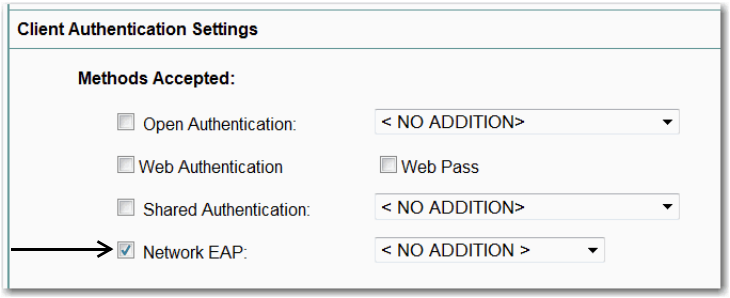
4. Click Apply.

5. Go to the SSID Manager page.

Figure 98 - SSID Manager Page

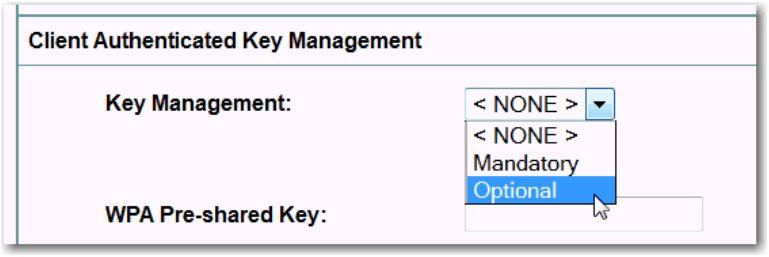


6. On the SSID that supports CCKM, choose these settings:
   a. If your access point contains multiple radio interfaces, select the interfaces that the SSID applies to.
   b. Under Authentication Settings, choose Network EAP.



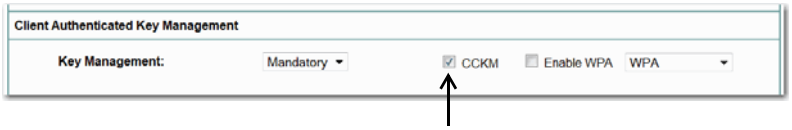
When you enable CCKM, you must enable Network EAP as the authentication type.

   c. Choose Mandatory or Optional under Authenticated Key Management.



- If you select Mandatory, clients that support only CCKM can associate by using the SSID.
- If you select Optional, both CCKM clients and clients that don't support CCKM can associate by using the SSID.

d. Check the CCKM check box.



7. Click Apply.

CLI Configuration Example

This example shows CLI commands that are equivalent to the steps listed in the Configure Access Points to Support Fast Secure Roaming on page 365:

```
AP# configure terminal
AP(config)# dot11 ssid fastroam
AP(config-ssid)# authentication network-eap
eap_methods
AP(config-ssid)# authentication key-management cckm
AP(config-ssid)# exit
AP(config)# interface dot11radio0
AP(config-if)# encryption mode ciphers aes-ccm
AP(config-if)# ssid fastroam
AP(config-if)# exit
AP(config)# end
```

In this example, the SSID fastroam is configured to support Network EAP and CCKM, the AES-CCM cipher suite is enabled on the 2.4 GHz radio interface, and the SSID fastroam is enabled on the 2.4 GHz radio interface.

Management Frame Protection

Management Frame Protection provides security features for the management messages passed between Access Point and Client stations. MFP consists of two functional components: Infrastructure MFP and Client MFP.

Infrastructure MFP provides Infrastructure support. Infrastructure MFP utilizes a message integrity check (MIC) across broadcast and directed management frames that can assist in detection of rogue devices and denial of service attacks. Client MFP provides client support. Client MFP protects authenticated clients from spoofed frames, by preventing many of the common attacks against WLANs from becoming effective. Management Frame Protection operation requires a WDS.

Overview

Client MFP encrypts class 3 management frames sent between access points and CCXv5-capable client stations, so that both AP and client can take preventative action by dropping spoofed class 3 management frames, for example, management frames passed between an AP and a client station that is authenticated and associated.

Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect class 3 Unicast management frames. The unicast cipher suite negotiated by the STA in the reassociation request's RSNIE is used to protect both unicast data and class 3 management frames. An access point in workgroup bridge, repeater, or non-root bridge mode must negotiate either TKIP or AES-CCMP to use Client MFP.

Protection of Unicast Management Frames

Unicast class 3 management frames are protected by applying either AES-CCMP or TKIP in a similar manner to that already used for data frames. Client MFP is enabled only for autonomous access points if the encryption is AES-CCMP or TKIP and key management WPA version 2.

Protection of Broadcast Management Frames

To prevent attacks by using broadcast frames, access points supporting CCXv5 don't emit any broadcast class 3 management frames. An access point in workgroup bridge, repeater, or non-root bridge mode discards broadcast class 3 management frames if Client MFP is enabled. Client MFP is enabled only for autonomous access points if the encryption is AES-CCMP or TKIP and key management WPA version 2.

Client MFP for Access Points in Root Mode

Autonomous access points in root mode support mixed mode clients. Clients capable of CCXv5 with negotiated cipher suite AES or TKIP with WPAv2 are Client MFP enabled. Client MFP is disabled for clients that are not CCXv5 capable. By default, Client MFP is optional for a particular SSID on the access point, and can be enabled or disabled by using CLI in SSID configuration mode.

Client MFP can be configured as either required or optional for a particular SSID. To configure Client MFP as required, you must configure the SSID with key management WPA version 2 mandatory. If the key management is not WPAv2 mandatory, an error message is displayed and your CLI command is rejected. If you attempt to change the key management with Client MFP configured as required and key management WPAv2, an error message appears and rejects your CLI command. When configured as optional, Client MFP is enabled if the SSID is capable of WPAv2, otherwise Client MFP is disabled.

Configure Client MFP

The following CLI commands are used to configure Client MFP for access points in root mode.

```
ids mfp client required
```

This SSID configuration command enables Client MFP as required on a particular SSID. The Dot11Radio interface is reset when the command is executed if the SSID is bound to the Dot11Radio interface. The command also expects that the SSID is configured with WPA version 2 mandatory. If the SSID is not configured with WPAv2 mandatory, an error message appears and the command is rejected.

```
no ids mfp client
```

This ssid configuration command disables Client MFP on a particular SSID. The Dot11Radio interface is reset when the command is executed if the SSID is bound to the Dot11Radio interface.

```
ids mfp client optional
```

This ssid configuration command enables Client MFP as optional on a particular SSID. The Dot11Radio interface is reset when the command is executed if the SSID is bound to the Dot11Radio interface. Client MFP is enabled for this particular SSID if the SSID is WPAv2 capable, otherwise Client MFP is disabled.

```
show dot11 ids mfp client statistics
```

Use this command to display Client MFP statistics on the access point console for a Dot11Radio interface.

```
clear dot11 ids mfp client statistics
```

Use this command to clear the Client MFP statistics.

```
authentication key management wpa version {1|2}
```

Use this command to explicitly specify the WPA version to use for WPA key management for a particular SSID.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Configures the access point as an MFP generator.

   When enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving access point that is configured to detect (validate) MFP frames to report the discrepancy. The access point must be a member of a WDS.

   ```
   dot11 ids mfp generator
   ```

3. Configures the access point as an MFP detector.

When enabled, the access point validates management frames it receives from other access points. If it receives any frame that does not contain a valid, and expected, MIC IE, it reports the discrepancy to the WDS. The access point must be a member of a WDS.

```
dot11 ids mfp detector
```

4. Enter the name or ip address of the SNTP server.

   ```
   sntp server server IP address
   ```

5. Return to the privileged EXEC mode.

   ```
   end
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Beginning in privileged EXEC mode, follow these steps to configure the WDS:

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Configures the WDS as an MFP distributor.

   When enabled, the WDS manages signature keys, used to create the MIC IEs, and securely transfers them between generators and detectors.

   ```
   dot11 ids mfp distributor
   ```

3. Return to the privileged EXEC mode.

   ```
   end
   ```

4. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Configure an Authentication Failure Limit

Setting an authentication failure limit protects your network against a denial-of-service attack called EAPOL flooding. The 802.1X authentication that takes place between a client and the access point triggers a series of messages between the access point, the authenticator, and an authentication server by using EAPOL messaging. The authentication server, typically a RADIUS server, can quickly become overwhelmed if there are too many authentication attempts. If not regulated, a single client can trigger enough authentication requests to impact your network.

In monitor mode, the access point tracks the rate that 802.1X clients attempt to authenticate through the access point. If your network is attacked through excessive authentication attempts, the access point generates an alert when the authentication threshold has been exceeded.

You can configure these limits on the access point:

- Number of 802.1X attempts through the access point
- EAPOL flood duration in seconds on the access point

When the access point detects excessive authentication attempts it sets MIB variables to indicate this information:

- An EAPOL flood was detected
- Number of authentication attempts
- MAC address of the client with the most authentication attempts

Beginning in privileged EXEC mode, follow these steps to set authentication limits that trigger a fault on the access point:

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Configure the number of authentication attempts and the number of seconds of EAPOL flooding that trigger a fault on the access point.

   ```
   dot11 ids eap attempts number period seconds
   ```

3. Return to privileged EXEC mode.

   ```
   end
   ```

Notes:

Configure RADIUS and TACACS+ Servers

This chapter describes how to enable and configure the Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) that provide detailed accounting information and flexible administrative controls over the authentication and authorization processes. RADIUS and TACACS+ are facilitated through AAA and can be enabled only through `AAA` commands.

Topic	Page
Configure and Enable RADIUS	373
Configure the Access Point to Use Vendor-specific RADIUS Attributes	389
Configure the Access Point for Vendor-proprietary RADIUS Server Communication	390
Configure and Enable TACACS+	395
Configure and Enable TACACS+	395

TIP You can configure your access point as a local authenticator to provide a back-up for your main server or to provide authentication service on a network without a RADIUS server. Configure Authentication Types on page 331 for detailed instructions on configuring your access point as a local authenticator.

Configure and Enable RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco devices and send authentication requests to a central RADIUS server, that contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software from Cisco Secure Access Control Server version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, refer to the RADIUS server documentation.

Use RADIUS in these network environments that require access security.

- Networks with multiple-vendor access servers, each supporting RADIUS.

  For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that is customized to work with the Kerberos security system.

- Turnkey network security environments that applications support the RADIUS protocol, such as an access environment that uses a smart card access control system.

- Networks already using RADIUS.

  You can add an access point containing a RADIUS client to the network.

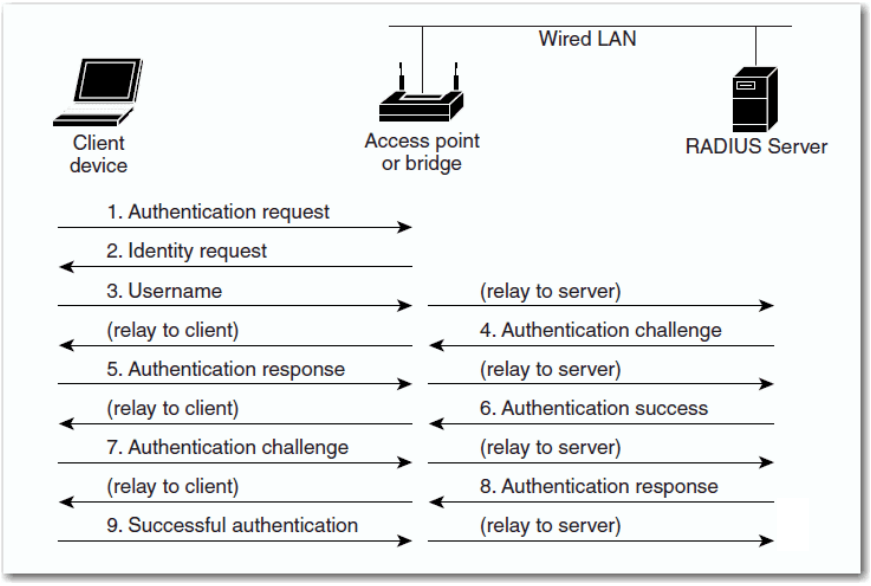
- Networks that require resource accounting.

  You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider can use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS Operation

When a wireless user attempts to log in and authenticate to an access point whose access is controlled by a RADIUS server, authentication to the network occurs in the steps shown in this figure.

Figure 99 - Sequence for EAP Authentication



In Steps 1...9, a wireless client device and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the access point. The RADIUS server sends an authentication challenge to the client. The client uses a one-way encryption of the user-supplied password to generate a response to the challenge and sends that response to the RADIUS server.

By using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, and the client authenticates the RADIUS server.

There is more than one type of EAP authentication, but the access point behaves the same way for each type: it relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device. See Assigning Authentication Types to an SSID on page 337 for instructions on setting up client authentication by using a RADIUS server.

Configure RADIUS

This section describes how to configure your access point to support RADIUS. At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a back-up system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

You can access and configure a RADIUS server before configuring RADIUS features on your access point.

TIP The RADIUS server CLI commands are disabled until you enter the `aaa new-model` command.

Default RADIUS Configuration

RADIUS and AAA are disabled by default. To prevent a lapse in security, you cannot configure RADIUS through a network management application using SNMP. When enabled, RADIUS can authenticate users accessing the access point through CLI or HTTP (Device Manager).

Identify the RADIUS Server Host

Access point-to-RADIUS-server communication involves several components:

- Host name or IP address
- Authentication destination port
- Accounting destination port
- Key string
- Timeout period
- Retransmission value

You identify RADIUS security servers by their host name or IP address, host name and specific UDP port numbers, or their IP address and specific UDP port numbers.

The combination of the IP address and the UDP port number creates a unique identifier allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

TIP The Stratix 5100 access point uses a randomly chosen UDP source port number in the range of 21645 to 21844 for communication with RADIUS servers.

If two different host entries on the same RADIUS server are configured for the same service—such as accounting—the second host entry configured acts as a fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the access point tries the second host entry

configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the access point use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the access point.

The timeout, retransmission, and encryption key values can be configured globally per server for all RADIUS servers or in some combination of global and per-server settings.

To apply these settings globally to all RADIUS servers communicating with the access point, use the three unique global configuration commands:

```
radius-server timeout
radius-server retransmit
radius-server key
```

To apply these values on a specific RADIUS server, use the `radius-server host` global configuration command.

TIP If you configure both global and per-server functions (timeout, retransmission, and key commands) on the access point, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands.

For information on configuring these setting on all RADIUS servers, see Configure All RADIUS Servers on page 387.

You can configure the access point to use AAA server groups to group existing server hosts for authentication. For more information, see Define AAA Server Groups on page 381.

Beginning in privileged EXEC mode, follow these steps to configure per-server RADIUS server communication. This procedure is required.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable AAA.

   ```
   aaa new-model
   ```

3. Specify the IP address or host name of the remote RADIUS server host.
   - (Optional) For `auth-port` *`port-number`*, specify the UDP destination port for authentication requests.
   - (Optional) For `acct-port` *`port-number`*, specify the UDP destination port for accounting requests.
   - (Optional) For `timeout` *`seconds`*, specify the time interval that the access point waits for the RADIUS server to reply before retransmitting. The range is 1...1000.

This setting overrides the `radius-server timeout` global configuration command setting. If no timeout is set with the `radius-server host` command, the setting of the `radius-server timeout` command is used.

- (Optional) For `retransmit` *`retries`*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1...1000.

  If no retransmit value is set with the `radius-server host` command, the setting of the `radius-server retransmit` global configuration command is used.
- (Optional) For `key` *`string`*, specify the authentication and encryption key used between the access point and the RADIUS daemon running on the RADIUS server.

TIP The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, don't enclose the key in quotation marks unless the quotation marks are part of the key.

To configure the access point to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The access point software searches for hosts in the order that you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.

```
radius-server host {hostname | ip-address} [auth-
port port-number] [acct-port port-number] [timeout
seconds] [retransmit retries] [key string]
```

4. Enter SSID configuration mode for an SSID when you need to enable accounting.

   The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.

   ```
   dot11 ssid ssid-string
   ```

5. Enable RADIUS accounting for this SSID. For list-name, specify the accounting method list.

   ```
   accounting list-name
   ```

6. Return to privileged EXEC mode.

   ```
   end
   ```

7. Verify your entries.

   ```
   show running-config
   ```

8. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

   To remove the specified RADIUS server, use the `no radius-server host` *`hostname | ip-address`* global configuration command.

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

```
AP(config)# radius-server host 172.29.36.49 auth-
port 1612 key rad1

AP(config)# radius-server host 172.20.36.50 acct-
port 1618 key rad2
```

This example shows how to configure an SSID for RADIUS accounting:

```
AP(config)# dot11 ssid batman

AP(config-ssid)# accounting accounting-method-list
```

This example shows how to configure *host1* as the RADIUS server and to use the default ports for both authentication and accounting:

```
AP(config)# radius-server host host1
```

You need to configure some settings also on the RADIUS server. These settings include the IP address of the access point and the key string to be shared by both the server and the access point.

Configure RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication and the sequence to be performed. This must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (by coincidence, is named default). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a back-up system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable AAA.

   ```
   aaa new-model
   ```

3. Create a login authentication method list.
   - To create a default list that is used when a named list is not specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.
   - For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

   Choose one of these methods:
   - Line

     Use the line password for authentication. You must define a line password before you can use this authentication method. Use the `password` *password* line configuration command.
   - Local

     Use the local username database for authentication. You must enter username information in the database. Use the `username` *password* global configuration command.
   - Radius

     Use RADIUS authentication. You must configure the RADIUS server before you can use this authentication method. For more information, see Identify the RADIUS Server Host on page 376.

   ```
   aaa authentication login {default | list-name}
   method1 [method2...]
   ```

4. Enter line configuration mode, and configure the lines that you want applied to the authentication list.

   ```
   line [console | tty | vty] line-number [ending-
   line-number]
   ```

5. Apply the authentication list to a line or set of lines.
   - If you specify default, use the default list created with the aaa authentication login command.
   - For list-name, specify the list created with the `aaa authentication login` command.

   ```
   login authentication {default | list-name}
   ```

6. Configure the access point to send its system name in the NAS_ID attribute for authentication.

   ```
   radius-server attribute 32 include-in-access-req
   format %h
   ```

7. Return to privileged EXEC mode.

```
end
```

8. Verify your entries.

   ```
   show running-config
   ```

9. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

- To disable AAA, use the `no aaa new-model` global configuration command.
- To disable AAA authentication, use the `no aaa authentication login {default | list-name} method1 [method2...]` global configuration command.

To either disable RADIUS authentication for login or to return to the default value, use the `no login authentication {default | list-name}` line configuration command.

Define AAA Server Groups

You can configure the access point to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list. The list contains the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service (such as accounting), the second configured host entry acts as a fail-over backup to the first one.

You use the server group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional authport and acct-port keywords.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable AAA.

   ```
   aaa new-model
   ```

3. Specify the IP address or host name of the remote RADIUS server host.
   - (Optional) `For auth-port` *port-number*, specify the UDP destination port for authentication requests.

- (Optional) For `acct-port` *port-number*, specify the UDP destination port for accounting requests.
- (Optional) For `timeout` *seconds*, specify the time interval that the access point waits for the RADIUS server to reply before retransmitting.

  The range is 1...1000. This setting overrides the `radius-server timeout` global configuration command setting. If no timeout is set with the `radius-server host` command, the setting of the `radius-server timeout` command is used.
- (Optional) For `retransmit` *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly.

  The range is 1...1000. If no retransmit value is set with the `radius-server hostp` command, the setting of the `radius-server retransmit` global configuration command is used.
- (Optional) For `key` *string*, specify the authentication and encryption key used between the access point and the RADIUS daemon running on the RADIUS server.

TIP The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, don't enclose the key in quotation marks unless the quotation marks are part of the key.

To configure the access point to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The access point software searches for hosts in the order that you specify. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.

`radius-server host {`*`hostname`* `|` *`ip-address`*`} [auth-port` *`port-number`*`] [acct-port` *`port-number`*`] [timeout` *`seconds`*`] [retransmit` *`retries`*`] [key` *`string`*`]`

4. Define the AAA server-group with a group name.

   This command puts the access point in a server group configuration mode.

   `aaa group server radius` *`group-name`*

5. Associate a particular RADIUS server with the defined server group.

   Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.

   `server` *`ip-address`*

6. Return to privileged EXEC mode.

   `end`

7. Verify your entries.

   `show running-config`

8. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

9. Enable RADIUS login authentication.

   See Configure RADIUS Login Authentication on page 379.

   - To remove the specified RADIUS server, use the `no radius-server host` *hostname* | *ip-address* global configuration command.
   - To remove a server group from the configuration list, use the `no aaa group server radius` *group-name* global configuration command.
   - To remove the IP address of a RADIUS server, use the `no server` *ip-address* server group configuration command.

In this example, the access point is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```
AP(config)# aaa new-model

AP(config)# radius-server host 172.20.0.1 auth-port
1000 acct-port 1001

AP(config)# radius-server host 172.10.0.1 auth-port
1645 acct-port 1646

AP(config)# aaa group server radius group1

AP(config-sg-radius)# server 172.20.0.1 auth-port
1000 acct-port 1001

AP(config-sg-radius)# exit

AP(config)# aaa group server radius group2

AP(config-sg-radius)# server 172.20.0.1 auth-port
2000 acct-port 2001

AP(config-sg-radius)# exit
```

Configure RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the access point uses information retrieved from the user's profile, that is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

TIP This section describes setting up authorization for access point administrators, not for wireless client devices.

You can use the `aaa authorization` global configuration command with the `radius` keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The `aaa authorization exec radius local` command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

TIP Authorization is bypassed for authenticated users who log in through CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Configure the access point for user RADIUS authorization for all network-related service requests.

   ```
   aaa authorization network radius
   ```

3. Configure the access point for user RADIUS authorization to determine if the user has privileged EXEC access.

   The `exec` keyword can return user profile information (such as `autocommand` information).

   ```
   aaa authorization exec radius
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. Verify your entries.

   ```
   show running-config
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

   To disable authorization, use the `no aaa authorization {network | exec}` *method1* global configuration command.

Start RADIUS Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the access point reports user activity to the RADIUS security server in the form of accounting records.

Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

See RADIUS Attributes Sent by the Access Point on page 392 for a complete list of attributes sent and honored by the access point.

Beginning in privileged EXEC mode, follow these steps to enable RADIUS accounting for each Cisco IOS privilege level and for network services:

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable RADIUS accounting for all network-related service requests.

   ```
   aaa accounting network start-stop radius
   ```

3. Configure the access point to send its BVI IP address in the NAS_IP_ADDRESS attribute for accounting records.

   ```
   ip radius source-interface bvi1
   ```

4. Enter an accounting update interval in minutes.

   ```
   aaa accounting update periodic minutes
   ```

5. Return to privileged EXEC mode.

   ```
   end
   ```

6. Verify your entries.

   ```
   show running-config
   ```

7. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

   To disable accounting, use the `no aaa accounting {network | exec} {start-stop}` *method1...* global configuration command.

Select the CSID Format

You can choose the format for MAC addresses in Called-Station-ID (CSID) and Calling-Station-ID attributes in RADIUS packets. Use the `dot11 aaa csid` global configuration command to select the CSID format.

This table lists the format options with corresponding MAC address examples.

Option	MAC Address Example
default	0007.85b3.5f4a
ietf	00-07-85-b3-5f-4a
unformatted	000785b35f4a

To return to the default CSID format, use the **no** form of the `dot11 aaa csid` command, or enter

```
dot11 aaa csid default
```

TIP You can also use the `wlccp wds aaa csid` command to select the CSID format.

Configure All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure global communication settings between the access point and all RADIUS servers.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Specify the shared secret text string used between the access point and all RADIUS servers.

   TIP The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, don't enclose the key in quotation marks unless the quotation marks are part of the key.

   ```
   radius-server key string
   ```

3. Specify the number of times the access point sends each RADIUS request to the server before giving up. The default is 3; the range 1...1000.

   ```
   radius-server retransmit retries
   ```

4. Specify the number of seconds an access point waits for a reply to a RADIUS request before resending the request.

   The default is 5 seconds; the range is 1...1000.

   ```
   radius-server timeout seconds
   ```

5. Use this command to cause the Cisco IOS software to mark as "dead" any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server.

   A RADIUS server marked as dead is skipped by additional requests for the duration of minutes that you specify, up to a maximum of 1440 (24 hours).

   TIP This command is required configuration when multiple RADIUS servers are defined. If not configured, client authentication does not occur. When one RADIUS server is defined, this command is optional.

   ```
   radius-server deadtime minutes
   ```

6. Configure the access point to send its system name in the NAS_ID attribute for authentication.

   ```
   radius-server attribute 32 include-in-access-req
   format %h
   ```

7. Return to privileged EXEC mode.

   ```
   end
   ```

8. Verify your settings.

   ```
   show running-config
   ```

9. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

This example shows how to set up two main servers and a local authenticator with a server deadtime of 10 minutes:

```
AP(config)# aaa new-model

AP(config)# radius-server host 172.20.0.1 auth-port
1000 acct-port 1001 key 77654

AP(config)# radius-server host 172.10.0.1 auth-port
1645 acct-port 1646 key 77654

AP(config)# radius-server host 10.91.6.151 auth-
port 1812 acct-port 1813 key 110337

AP(config)# radius-server deadtime 10
```

To return to the default setting for retransmit, timeout, and deadtime, use the no forms of these commands.

Configure the Access Point to Use Vendor-specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the access point and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use.

The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor ID is 9, and the supported option has vendor type 1, that is named cisco-avpair. The value is a string with this format:

```
protocol : attribute sep value *
```

Protocol is a value of the Cisco protocol attribute for a particular type of authorization. Attribute and value are an appropriate AV pair defined in the Cisco TACACS+ specification, and sep is = for mandatory attributes and the asterisk (*) for optional attributes. This lets a full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair activates Cisco's multiple named ip address pools feature during IP authorization (during PPP's IPCP address assignment):

```
cisco-avpair= ”ip:addr-pool=first“
```

The following example shows how to provide a user logging in from an access point with immediate access to privileged EXEC commands:

```
cisco-avpair= ”shell:priv-lvl=15“
```

Other vendors have their own unique vendor IDs, options, and associated VSAs. For more information about vendor IDs and VSAs, refer to RFC 2138, “Remote Authentication Dial-In User Service (RADIUS).”

Beginning in privileged EXEC mode, follow these steps to configure the access point to recognize and use VSAs.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable the access point to recognize and use VSAs as defined by RADIUS IETF attribute 26.
   - (Optional) Use the accounting keyword to limit the set of recognized vendor-specific attributes to only accounting attributes.
   - (Optional) Use the authentication keyword to limit the set of recognized vendor-specific attributes to only authentication attributes.

If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.

```
radius-server vsa send [accounting |
authentication]
```

3. Return to privileged EXEC mode.

   ```
   end
   ```

4. Verify your settings.

   ```
   show running-config
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

For a complete list of RADIUS attributes or more information about VSA 26, see publication Cisco IOS Security Configuration Guide for Release 12.2.

Configure the Access Point for Vendor-proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the access point and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the access point. You specify the RADIUS host and secret text string by using the `radius-server` global configuration commands.

Beginning in privileged EXEC mode, follow these steps to specify a vendor-proprietary RADIUS server host and a shared secret text string.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Specify the IP address or host name of the remote RADIUS server host and identify that it is using a vendor-proprietary implementation of RADIUS.

   ```
   radius-server host {hostname | ip-address} non-
   standard
   ```

3. Specify the shared secret text string used between the access point and the vendor-proprietary RADIUS server.

The access point and the RADIUS server use this text string to encrypt passwords and exchange responses.

TIP The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, don't enclose the key in quotation marks unless the quotation marks are part of the key.

```
radius-server key string
```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. Verify your settings.

   ```
   show running-config
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

   - To delete the vendor-proprietary RADIUS host, use the `no radius-server host {hostname | ip-address} non-standard` global configuration command.
   - To disable the key, use the `no radius-server key` global configuration command.

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of `rad124` between the access point and the server:

```
AP(config)# radius-server host 172.20.30.15
nonstandard
AP(config)# radius-server key rad124
```

Display the RADIUS Configuration

To display the RADIUS configuration, use the `show running-config` privileged EXEC command.

TIP When DNS is configured on the access point, the `show running-config` a server's IP address can appear instead of its name.

RADIUS Attributes Sent by the Access Point

Table 104 on page 392 through Table 106 on page 392 identify the attributes sent by an access point to a client in access-request, access-accept, and accounting-request packets.

Table 104 - Attributes Sent in Access-Request Packets

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
12	Framed-MTU
30	Called-Station-ID (MAC address)
31	Calling-Station-ID (MAC address)
32	NAS-Identifier(1)
61	NAS-Port-Type
79	EAP-Message
80	Message-Authenticator

(1) The access point sends the NAS-Identifier if attribute 32 (include-in-access-req) is configured.

Table 105 - Attributes Honored in Access-Accept Packets

Attribute ID	Description
25	Class
27	Session-Timeout
64	Tunnel-Type(1)
65	Tunnel-Medium-Type[1]
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID[1]
VSA (attribute 26)	LEAP session-key
VSA (attribute 26)	Auth-Algo-Type
VSA (attribute 26)	SSID

(1) RFC2868; defines a VLAN override number.

Table 106 - Attributes Sent in Accounting-Request (start) Packets

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class

Table 106 - Attributes Sent in Accounting-Request (start) Packets

Attribute ID	Description
41	Acct-Delay-Time
44	Acct-Session-Id
61	NAS-Port-Type
VSA (attribute 26)	SSID
VSA (attribute 26)	NAS-Location
VSA (attribute 26)	Cisco-NAS-Port
VSA (attribute 26)	Interface

Table 107 - Attributes Sent in Accounting-Request (update) Packets

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
61	NAS-Port-Type
VSA (attribute 26)	SSID
VSA (attribute 26)	NAS-Location
VSA (attribute 26)	VLAN-ID
VSA (attribute 26)	Connect-Progress
VSA (attribute 26)	Cisco-NAS-Port
VSA (attribute 26)	Interface

Table 108 - Attributes Sent in Accounting-Request (stop) Packets

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time

Table 108 - Attributes Sent in Accounting-Request (stop) Packets (Continued)

Attribute ID	Description
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
61	NAS-Port-Type
VSA (attribute 26)	SSID
VSA (attribute 26)	NAS-Location
VSA (attribute 26)	Disc-Cause-Ext
VSA (attribute 26)	VLAN-ID
VSA (attribute 26)	Connect-Progress
VSA (attribute 26)	Cisco-NAS-Port
VSA (attribute 26)	Interface
VSA (attribute 26)	Auth-Algo-Type

By default, the access point sends reauthentication requests to the authentication server with the service-type attribute set to authenticate-only. However, some Microsoft IAS servers don't support the authenticate-only service-type attribute. Depending on the user requirements, set the service-type attribute to.

```
dot11 aaa authentication attributes service-type
login-user
```

or

```
dot11 aaa authentication attributes service-type
framed-user.
```

By default the service type "login" is sent in the access request.

Configure and Enable TACACS+

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your access point. Unlike RADIUS, TACACS+ does not authenticate client devices associated to the access point.

TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or pages NT workstation. Access and configure a TACACS+ server before configuring TACACS+ features on your access point.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ lets a single access control server (the TACACS+ daemon) to provide each service; authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

TACACS+, administered through the AAA security services, can provide these services:

Authentication

Provides complete control of authentication of administrators through login and password dialog box, challenge and response, and messaging support.

The authentication facility can conduct a dialog with the administrator (for example, after a username and password are provided, to challenge a user with several questions, such as home address, mother's maiden name, service type, and social security number). The TACACS+ authentication service can also send messages to administrator screens. For example, a message could notify administrators that their passwords must be changed because of the company's password aging policy.

Authorization

Provides fine-grained control over administrator capabilities for the duration of the administrator's session, including but not limited to setting auto-commands, access control, session duration, or protocol support. You can also enforce restrictions on the commands that an administrator can execute with the TACACS+ authorization feature.

Accounting

Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track administrator activity for a security audit or to provide information for user billing. Accounting records include administrator identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the access point and the TACACS+ daemon, and it maintains confidentiality because all protocol exchanges between the access point and the TACACS+ daemon are encrypted.

You need a system running the TACACS+ daemon software to use TACACS+ on your access point.

TACACS+ Operation

When an administrator attempts a simple ASCII login by authenticating to an access point by using TACACS+, this process occurs:

1. When the connection is established, the access point contacts the TACACS+ daemon to obtain a username prompt, then it is displayed to the administrator.
2. The administrator enters a username, and the access point then contacts the TACACS+ daemon to obtain a password prompt.
3. The password prompt to the administrator appears, the administrator enters a password, and the password is sent to the TACACS+ daemon.

   TACACS+ lets a conversation to be held between the daemon and the administrator until the daemon receives enough information to authenticate the administrator. The daemon prompts for a username and password combination, but can include other items, such as the user's mother's maiden name.
4. The access point eventually receives one of these responses from the TACACS+ daemon.

Response	Description
ACCEPT	The administrator is authenticated and service can begin. If the access point is configured to require authorization, authorization begins at this time.
REJECT	The administrator is not authenticated. The administrator can be denied access or is prompted to retry the login sequence, depending on the TACACS+ daemon.
ERROR	An error occurred at some time during authentication with the daemon or in the network connection between the daemon and the access point. If an ERROR response is received, the access point typically tries to use an alternative method for authenticating the administrator.
CONTINUE	The administrator is prompted for additional authentication information.

   After authentication, the administrator undergoes an additional authorization phase if authorization has been enabled on the access point. Administrators must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
5. If TACACS+ authorization is required, the TACACS+ daemon is again contacted, and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes that direct the EXEC or NETWORK session for that administrator, determining the services that the administrator can access:
   - Telnet, rlogin, or privileged EXEC services
   - Connection parameters, including the host or client IP address, access list, and administrator timeouts

Configure TACACS+

To configure your access point to support TACACS+, you must identify the host or hosts maintaining the TACACS+ daemon and define the method lists for TACACS+ authentication. You can optionally define method lists for TACACS+ authorization and accounting.

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on an administrator. You can use method lists to designate one or more security protocols to be used, thus ensuring a back-up system if the initial method fails.

The software uses the first method listed to authenticate, to authorize, or to keep accounts on administrators; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate administrators accessing the access point through CLI.

Identify the TACACS+ Server Host and Setting the Authentication Key

You can configure the access point to use a single server or AAA server groups to group existing server hosts for authentication. You can group servers to select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list and contains the list of IP addresses of the selected server hosts.

Beginning in privileged EXEC mode, follow these steps to identify the IP host or host maintaining TACACS+ server and optionally set the encryption key.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Identify the IP host or hosts maintaining a TACACS+ server.

   Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order that you specify.

   - For *`hostname`*, specify the name or IP address of the host.
   - (Optional) For `port` *`integer`*, specify a server port number.

     The default is port 49. The range is 1...65535.

- (Optional) For `timeout` *`integer`*, specify a time in seconds the access point waits for a response from the daemon before it times out and declares an error.

  The default is 5 seconds. The range is 1...1000 seconds.
- (Optional) For `key` *`string`*, specify the encryption key for encrypting and decrypting all traffic between the access point and the TACACS+ daemon. You must configure the same key on the TACACS+ daemon for encryption to be successful.

`tacacs-server host` *`hostname`* `[port` *`integer`*`] [timeout` *`integer`*`] [key` *`string`*`]`

3. Enable AAA.

   `aaa new-model`

4. (Optional) Define the AAA server-group with a group name.

   This command puts the access point in a server group subconfiguration mode.

   `aaa group server tacacs+` *`group-name`*

5. (Optional) Associate a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group.

   Each server in the group must be previously defined in Step 2.

   `server` *`ip-address`*

6. Return to privileged EXEC mode.

   `end`

7. Verify your entries.

   `show tacacs`

8. (Optional) Save your entries in the configuration file.

   `copy running-config startup-config`

- To remove the specified TACACS+ server name or address, use the `no tacacs-server host hostname` global configuration command.
- To remove a server group from the configuration list, use the `no aaa group server tacacs+ group-name` global configuration command.
- To remove the IP address of a TACACS+ server, use the `no server ip-address` server group subconfiguration command.

Configure TACACS+ Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication and the sequence performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (by coincidence, is named default). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list describes the sequence and authentication methods to be queried to authenticate an administrator. You can designate one or more security protocols to be used for authentication, thus ensuring a back-up system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list.

This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the administrator access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable AAA.

   ```
   aaa new-model
   ```

3. Create a login authentication method list.
   - To create a default list that is used when a named list is **not** specified in the `login authentication` command, use the `default` keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.
   - For *`list-name`*, specify a character string to name the list you are creating.
   - For *`method1`*..., specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Choose one of these methods:

- `line`

  Use the line password for authentication. You must define a line password before you can use this authentication method. Use the `password` *`password`* line configuration command.

- `local`

  Use the local username database for authentication. You must enter username information into the database. Use the `username` *`password`* global configuration command.

- `tacacs+`

  Uses TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method.

  `aaa authentication login {default | list-name} method1 [method2...]`

4. Enter line configuration mode, and configure the lines that you want to apply the authentication list.
5. Enter line configuration mode.
6. Configure the lines.
7. Apply the authentication list.

   `line [console | tty | vty] line-number [ending-line-number]`

8. Apply the authentication list to a line or set of lines.
   - If you specify `default`, use the default list created with the `aaa authentication login` command.
   - For *list-name*, specify the list created with the `aaa authentication login` command.

   `login authentication {default | list-name}`

9. Return to privileged EXEC mode.

   `end`

10. Verify your entries.

    `show running-config`

11. (Optional) Save your entries in the configuration file.

    `copy running-config startup-config`

- To disable AAA, use the `no aaa new-model` global configuration command.

- To disable AAA authentication, use the `no aaa authentication login {default | list-name} method1 [method2...]` global configuration command.

- To either disable TACACS+ authentication for login or to return to the default value, use the `no login authentication {default | list-name}` line configuration command.

Configure TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to an administrator. When AAA authorization is enabled, the access point uses information retrieved from the administrator's profile, that is either in the local user database or on the security server, to configure the administrator's session. The administrator is granted access to a requested service only if the information in the administrator profile allows it.

You can use the `aaa authorization` global configuration command with the `tacacs+` keyword to set parameters that restrict an administrator's network access to privileged EXEC mode.

The `aaa authorization exec tacacs+ local` command sets these authorization parameters:

- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

TIP Authorization is bypassed for authenticated administrators who log in through CLI even if authorization has been configured.

```
Beginning in privileged EXEC mode, follow these
steps to specify TACACS+ authorization for
privileged EXEC access and network services:
```

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Configure the access point for administrator TACACS+ authorization for all network-related service requests.

   ```
   aaa authorization network tacacs+
   ```

3. Configure the access point for administrator TACACS+ authorization to determine if the administrator has privileged EXEC access.

   The `exec` keyword can return user profile information (such as `autocommand` information).

   ```
   aaa authorization exec tacacs+
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. Verify your entries.

   ```
   show running-config
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

To disable authorization, use the `no aaa authorization {network | exec} method1` global configuration command.

Start TACACS+ Accounting

The AAA accounting feature tracks the services that administrators are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the access point reports administrator activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Beginning in privileged EXEC mode, follow these steps to enable TACACS+ accounting for each Cisco IOS privilege level and for network services.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable TACACS+ accounting for all network-related service requests.

   ```
   aaa accounting network start-stop tacacs+
   ```

3. Enable TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.

   ```
   aaa accounting exec start-stop tacacs+
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. Verify your entries.

   ```
   show running-config
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

To disable accounting, use the `no aaa accounting {network | exec} {start-stop}` *method1...* global configuration command.

Display the TACACS+ Configuration

To display TACACS+ server statistics, use the `show tacacs` privileged EXEC command.

Configure Virtual Local Area Networks (VLAN)

This chapter describes how to configure your access point to operate with the VLANs set up on your wired LAN in the following sections.

Topic	Page
VLANs	403
Configure VLANs	406

VLANs

A VLAN is a switched network that is logically segmented, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they can be intermingled with other teams. You use VLANs to reconfigure the network through software rather than physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment such as LAN switches that operate bridging protocols between them with a separate group for each VLAN.

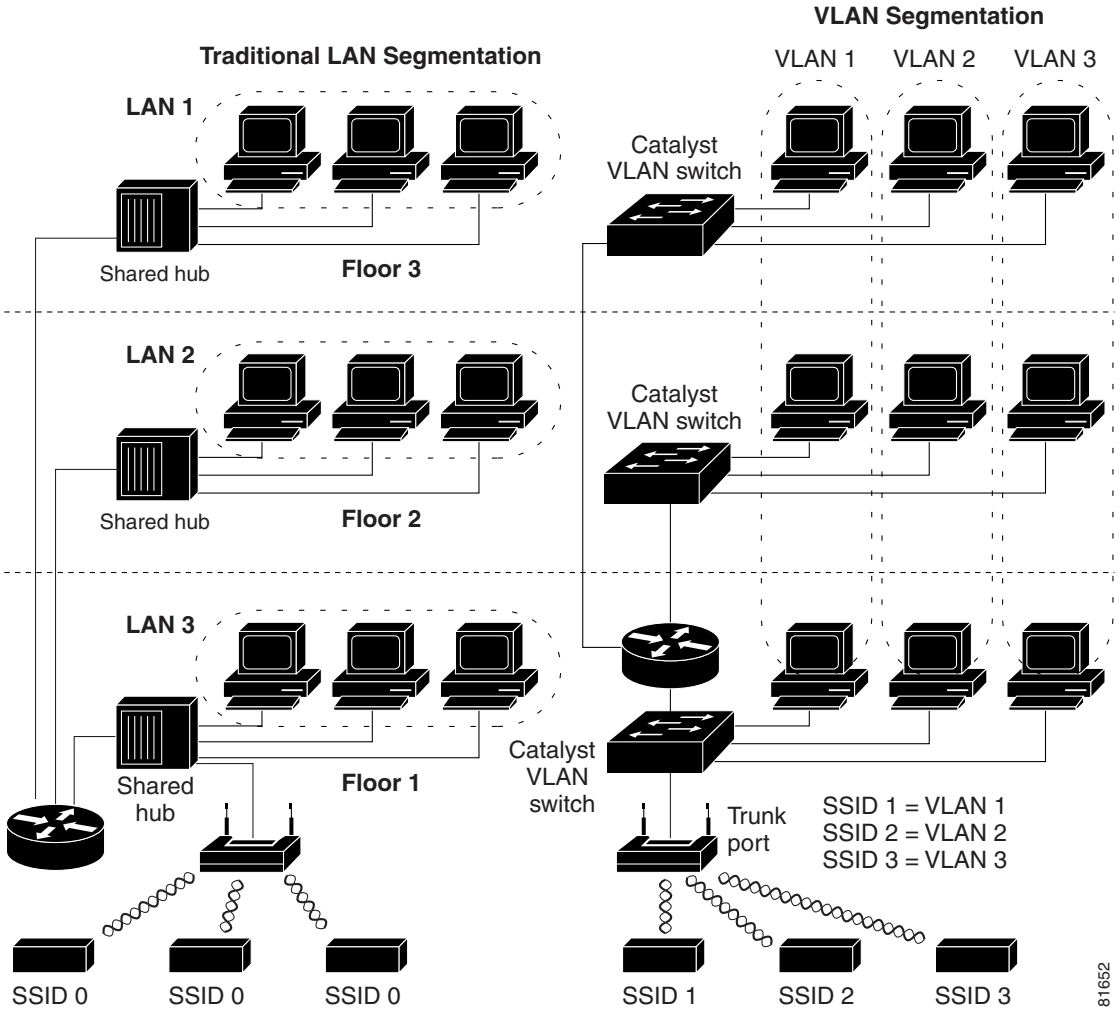
VLANs provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. Consider several key issues when you design and build switched LAN networks:

- LAN segmentation
- Security
- Broadcast control
- Performance
- Network management
- Communication between VLANs

You extend VLANs into a wireless LAN by adding IEEE 802.11Q tag awareness to the access point. Frames destined for different VLANs are transmitted by the wireless access point/workgroup bridge on different SSIDs with different encryption keys. Only the clients associated with that VLAN receive those packets. Conversely, packets coming from a client associated with a certain VLAN are 802.11Q tagged before they are forwarded onto the wired network.

This figure shows the difference between traditional physical LAN segmentation and logical VLAN segmentation with wireless devices connected.

Figure 100 - LAN and VLAN Segmentation with Wireless Devices



Incorporate Wireless Devices into VLANs

The basic wireless components of a VLAN consist of an access point and a client associated to it by using wireless technology. The access point is physically connected through a trunk port to the network VLAN switch where the VLAN is configured. The physical connection to the VLAN switch is through the access point's Ethernet port.

In fundamental terms, the key to configuring an access point to connect to a specific VLAN is to configure its SSID to recognize that VLAN. Because VLANs are identified by a VLAN ID or name, it follows that if the SSID on an access point is configured to recognize a specific VLAN ID or name, a connection to the VLAN is established. When this connection is made, associated wireless client devices having the same SSID can access the VLAN through the access point. The VLAN processes data to and from the clients the same way that it processes data to and from wired connections. You can configure up to 16 SSIDs on your access point, so you can support up to 16 VLANs. You can assign only one SSID to a VLAN.

You can use the VLAN feature to deploy wireless devices with greater efficiency and flexibility. For example, one access point can now handle the specific requirements of multiple users having widely varied network access and permissions. Without VLAN capability, multiple access points have to be employed to serve classes of users based on the access and permissions they were assigned.

These are two common strategies for deploying wireless VLANs:

- Segmentation by user groups: You can segment your wireless LAN user community and enforce a different security policy for each user group.

  For example, you can create three wired and wireless VLANs in an enterprise environment for full-time and part-time employees and also provide guest access.

- Segmentation by device types: You can segment your wireless LAN to allow different devices with different security capabilities to join the network.

  For example, some wireless users can have handheld devices that support only WPA2-PSK (pre-shared keys), and some wireless users can have more sophisticated devices by using 802.1x and EAP methods. You can group and isolate these devices into separate VLANs.

  TIP You cannot configure multiple VLANs on repeater access points. Repeater access points support only the native VLAN.

Configure VLANs

Configuring your access point to support VLANs is a three-step process.

1. Enable the VLAN on the radio and Ethernet ports.
2. Assign SSIDs to VLANs.
3. Assign authentication settings to SSIDs.

Assigning SSIDs to VLANs.

This section describes how to assign SSIDs to VLANs and how to enable a VLAN on the access point radio and Ethernet ports.

- For detailed instructions on assigning authentication types to SSIDs, see Configure Authentication Types on page 331
- For instructions on assigning other settings to SSIDs, see Configure Multiple Service Set Identifiers (SSIDs) on page 285

You can configure up to 16 SSIDs on the access point, so you can support up to 16 VLANs that are configured on your LAN. However, for most deployments, it is recommended not to create more than three SSID / VLANs to reduce overhead.

Beginning in privileged EXEC mode, follow these steps to assign an SSID to a VLAN and enable the VLAN on the access point radio and Ethernet ports.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Create an SSID and enter SSID configuration mode for the new SSID.

   The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.

   The SSID can consist of up to 32 alphanumeric, case-sensitive, characters. The first character can not contain the following characters:

   - Exclamation point (!)
   - Pound sign (#)
   - Semicolon (;)

   The following characters are invalid and cannot be used in an SSID:

   - Plus sign (+)
   - Right bracket (])
   - Front slash (/)
   - Quotation mark (")
   - Tab

- Trailing spaces

TIP You use the ssid command's authentication options to configure an authentication type for each SSID.

See Configure Authentication Types on page 331 for instructions on configuring authentication types.

```
dot11 ssid ssid-string
```

3. (Optional) Assign the SSID to a VLAN on your network.

   Client devices that associate by using the SSID are grouped into this VLAN. Enter a VLAN ID from 1...4095. You can assign only one SSID to a VLAN.

   TIP If your network uses VLAN names, you can also assign names to the VLANs on your access point.

   See Assign Names to VLANs on page 408 for instructions.

   ```
   vlan vlan-id
   ```

4. Return to interface configuration mode for the radio interface.

   ```
   exit
   ```

5. Enter interface configuration mode for the radio VLAN sub interface.

   ```
   interface dot11radio 0.x | 1.x
   ```

   where x is the VLAN number

6. Enable a VLAN on the radio interface.

   (Optional) Designate the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.

   ```
   encapsulation dot1q vlan-id [native]
   ```

7. Return to global configuration mode.

   ```
   exit
   ```

8. Enter interface configuration mode for the Ethernet VLAN subinterface.

   ```
   interface gigabitEthernet0.x
   ```

9. Enable a VLAN on the Ethernet interface.

   (Optional) Designate the VLAN as the native VLAN.

   ```
   encapsulation dot1q vlan-id [native]
   ```

10. Return to privileged EXEC mode.

    ```
    end
    ```

11. (Optional) Save your entries in the configuration file.

    ```
    copy running-config startup-config
    ```

This example shows how to:

a. Name an SSID.

b. Assign the SSID to a VLAN.

c. Enable the VLAN on the radio and Ethernet ports as the native VLAN.

```
ap1200Router# configure terminal
ap1200Router(config)# interface dot11radio0
ap1200Router(config-if)# ssid batman
ap1200Router(config-if)# exit
ap1200Router(config)# dot11 ssid batman
ap1200Router(config-ssid)# vlan 1
ap1200Router(config-ssid)# exit
ap1200Router(config)# interface dot11radio0.1
ap1200Router(config-subif)# encapsulation dot1q 1
native
ap1200Router(config-subif)# exit
ap1200Router(config)# interface gigabitEthernet0.1
ap1200Router(config-subif)# encapsulation dot1q 1
native
ap1200Router(config-subif)# exit
ap1200Router(config)# end
```

Assign Names to VLANs

You can assign a name to a VLAN in addition to its numerical ID. VLAN names can contain up to 32 ASCII characters. The access point stores each VLAN name and ID pair in a table.

Guidelines for Using VLAN Names

Keep these guidelines in mind when using VLAN names:

- The mapping of a VLAN name to a VLAN ID is local to each access point, so across your network, you can assign the same VLAN name to a different VLAN ID.

  TIP If clients on your wireless LAN require seamless roaming, We recommend that you assign the same VLAN name to the same VLAN ID across all access points, or that you use only VLAN IDs without names.

- Every VLAN configured on your access point must have an ID, but VLAN names are optional.

- VLAN names can contain up to 32 ASCII characters. However, a VLAN name cannot be a number between 1...4095. For example, *vlan4095* is a valid VLAN name, but *4095* is not. The access point reserves the numbers 1...4095 for VLAN IDs.

Creating a VLAN Name

Beginning in privileged EXEC mode, follow these steps to assign a name to a VLAN.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Assign a VLAN name to a VLAN ID. The name can contain up to 32 ASCII characters.

   ```
   dot11 vlan-name name vlan vlan-id
   ```

3. Return to privileged EXEC mode.

   ```
   end
   ```

4. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Use the `no` form of the command to remove the name from the VLAN. Use the `show dot11 vlan-name` privileged EXEC command to list all the VLAN name and ID pairs configured on the access point.

Assign Users to VLAN by Using a RADIUS Server

You can configure your RADIUS authentication server to assign users or groups of users to a specific VLAN when they authenticate to the network.

Unicast and multicast cipher suites advertised in WPA information element (and negotiated during 802.11 association) can potentially mismatch with the cipher suite supported in an explicitly assigned VLAN. If the RADIUS server assigns a new vlan ID that uses a different cipher suite from the previously negotiated cipher suite, there is no way for the access point and client to switch back to the new cipher suite. Currently, the WPA and CCKM protocols don't allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the client device is disassociated from the wireless LAN.

The VLAN-mapping process consists of these steps.

1. A client device associates to the access point by using any SSID configured on the access point.
2. The client begins RADIUS authentication.

3. When the client authenticates successfully, the RADIUS server maps the client to a specific VLAN, regardless of the VLAN mapping defined for the SSID the client is using on the access point. If the server does not return any VLAN attribute for the client, the client is assigned to the VLAN specified by the SSID mapped locally on the access point.

These are the RADIUS user attributes used for vlan-id assignment. Each attribute must have a common tag value between 1...31 to identify the grouped relationship.

- IETF 64 (Tunnel Type): Set this attribute to VLAN.
- IETF 65 (Tunnel Medium Type): Set this attribute to 802.
- IETF 81 (Tunnel Private Group ID): Set this attribute to vlan-id.

View VLANs Configured on the Access Point

In privileged EXEC mode, use the `show vlan` command to view the VLANs that the access point supports. This is sample output from a `show vlan` command:

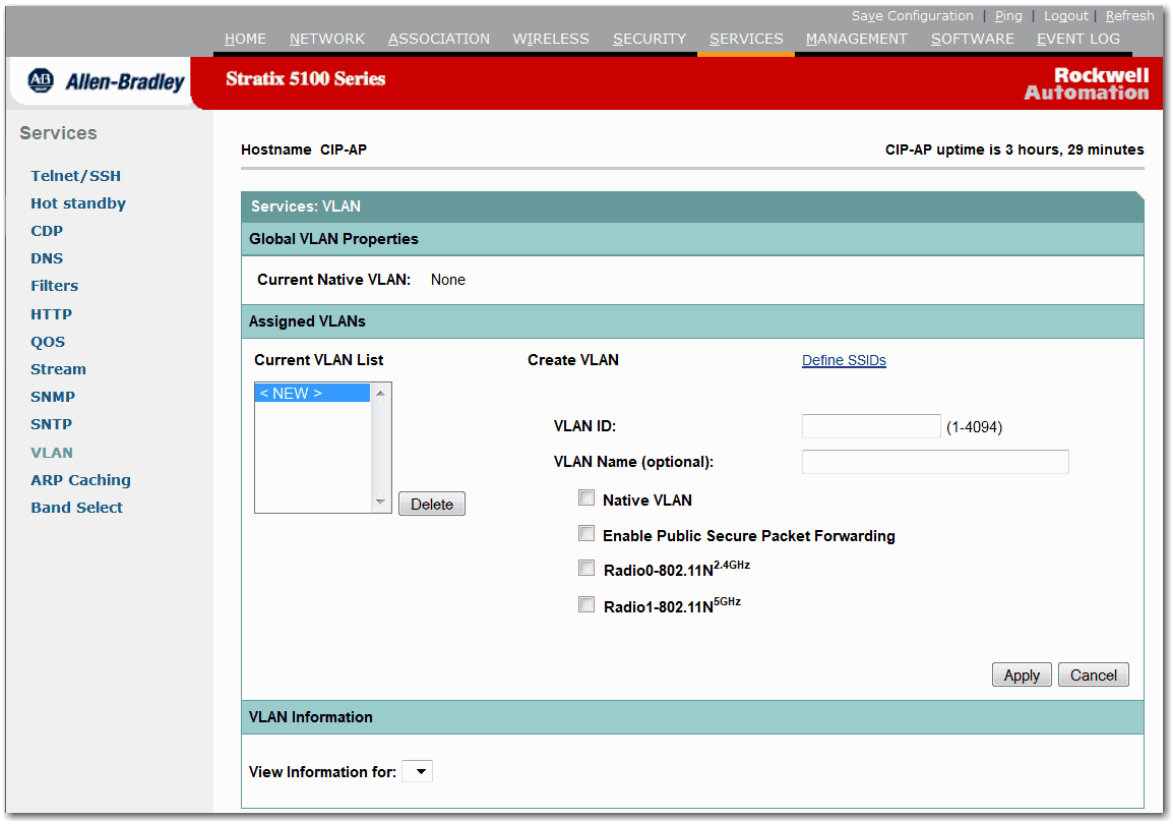
```
Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)


   vLAN Trunk Interfaces:  Dot11Radio0
GigabitEthernet0
Virtual-Dot11Radio0


 This is configured as native Vlan for the
following interface(s) :
Dot11Radio0
GigabitEthernet0
Virtual-Dot11Radio0
Protocols Configured:   Address:            Received:       Transmitted:
       Bridging       Bridge Group 1           201688                 0
       Bridging       Bridge Group 1           201688                 0
       Bridging       Bridge Group 1           201688                 0


Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)


   vLAN Trunk Interfaces:  Dot11Radio0.2
GigabitEthernet0.2
Virtual-Dot11Radio0.2
Protocols Configured:   Address:            Received:       Transmitted:
```

Configure and Enable a VLAN with SSID by Using Stratix 5100 Device Manager

The default VLAN is the management VLAN, and all untagged frames are implicitly associated with this default VLAN ID. Configure one of your VLANs to be configured as the native.

Complete these steps to configure the VLAN.

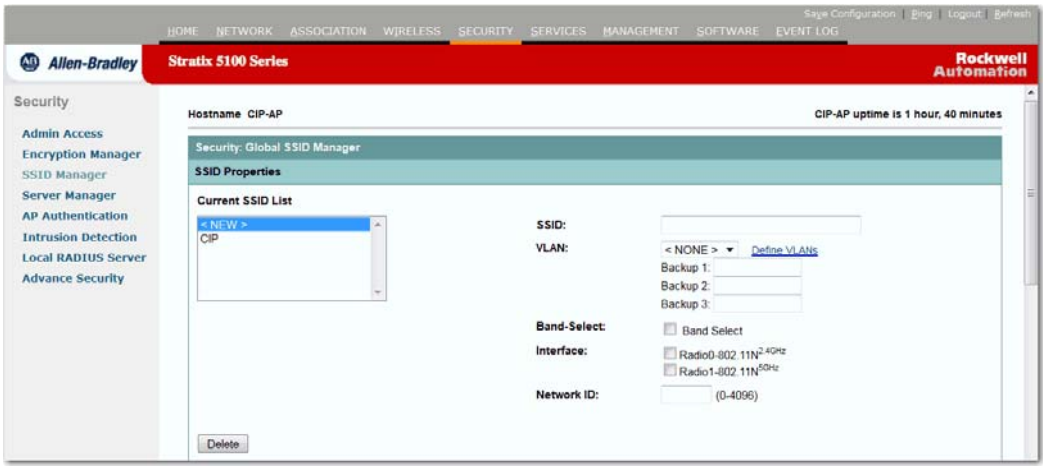
1. From the Services menu, choose Services.
2. Click VLAN.



3. Enter a unique VLAN ID number between 1...4095.
4. Determine if you want this VLAN ID to be the native VLAN.
5. Click on the radio you are associating with this VLAN ID.
6. Click Apply.

   If you do not click Apply, the new VLAN won't be saved and not seen on the SSID page.

7. Click the Define SSID link to go to the SSID Manager page.



8. Choose a unique SSID to be mapped with this VLAN.

   If no unique SSIDs are available, choose the NEW setting and create a new SSID.

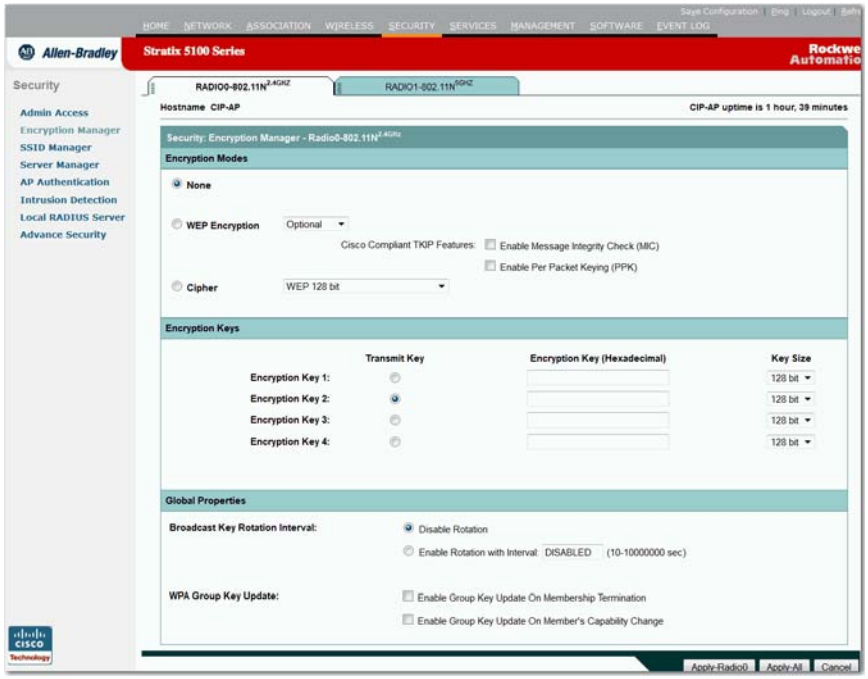
9. Select VLAN number from the list to associate with the unique SSID.
10. Click Apply to save the configuration.

Set the Encryption for the VLAN

Now that you have completed the configuration of the VLAN, you must set the encryption for the VLAN. Complete these steps to set the encryption for the VLAN.

1. Click Security to go to the Security Summary page.
2. From the Security menu, choose Encryption Manager.

   The Encryption Manager page appears.



3. Choose the VLAN you are configuring from the Set Encryption Mode and Keys for VLAN pull-down list.

   TIP This VLAN pull-down list appears only when you have VLANs enabled. If no VLANs are present, the encryption settings apply to all SSIDs.

4. In the Encryption Mode section, determine what encryption, if any, wireless clients need to use when communicating with the access point.

IMPORTANT AES CCMP is recommended for highest level of security.

5. Click Apply.

Notes:

Configure Quality of Service (QoS)

This chapter describes how to configure quality of service (QoS) on your access point. With this feature, you can provide preferential treatment to certain traffic at the expense of others. Without QoS, the access point offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.

IMPORTANT For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Guide.

Topic	Page
QoS for Wireless LANs	415
Configure QoS by Using Stratix 5100 Device Manager	418

QoS for Wireless LANs

Typically, networks operate on a best-effort delivery basis, meaning that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure QoS on the access point, you can select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your wireless LAN makes network performance more predictable and bandwidth utilization more effective.

When you configure QoS, you create QoS policies and apply the policies to the VLANs configured on your access point. If you don't use VLANs on your network, you can apply your QoS policies to the access point's Ethernet and radio ports.

IMPORTANT When you enable QoS, the access point uses Wi-Fi Multimedia (WMM) mode by default. See Wi-Fi Multimedia Mode on page 423 for information on WMM.

QoS for Wireless LANs Versus QoS on Wired LANs

The QoS implementation for wireless LANs differs from QoS implementations on other Cisco devices. With QoS enabled, access points perform the following:

- They prioritize packets based on DSCP value, IP address or TCP/UDP port value based on the ACL match, client type (such as a wireless phone), or the priority value in the 802.1q or 802.1p tag.
- Don't construct internal DSCP values; they support only mapping by assigning IP DSCP, Precedence, or Protocol values to Layer 2 COS values.
- Carry out EDCF like queuing on the radio egress port only.
- Do FIFO queueing only on the Ethernet egress port.
- Support only MQC policy-map set cos action.
- Prioritize the traffic from voice clients over traffic from other clients when the QoS Element for Wireless Phones feature is enabled.
- Support Spectralink phones by using the class-map IP protocol clause with the protocol value set to 119.

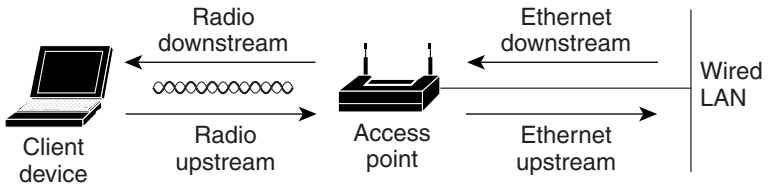
Impact of QoS on a Wireless LAN

Wireless LAN QoS features are a subset of the 802.11e standard. QoS on wireless LANs provides prioritization of traffic from the access point over the WLAN based on traffic classification.

Just as in other media, you can not notice the effects of QoS on a lightly loaded wireless LAN. The benefits of QoS become more obvious as the load on the wireless LAN increases, keeping the latency, jitter, and loss for selected traffic types within an acceptable range.

QoS on the wireless LAN focuses on downstream prioritization from the access point. This figure shows the upstream and downstream traffic flow.

Figure 101 - Upstream and Downstream Traffic Flow



- The radio downstream flow is traffic transmitted out the access point radio to a wireless client device. This traffic is the main focus for QoS on a wireless LAN.

- The radio upstream flow is traffic transmitted out the wireless client device to the access point. QoS for wireless LANs does not affect this traffic.

- The Ethernet downstream flow is traffic sent from a switch or a router to the Ethernet port on the access point. If QoS is enabled on the switch or router, the switch or router can prioritize and rate-limit traffic to the access point.

- The Ethernet upstream flow is traffic sent from the access point Ethernet port to a switch or router on the wired LAN. The access point does not prioritize traffic that it sends to the wired LAN based on traffic classification.

Precedence of QoS Settings

When you enable QoS, the access point queues packets based on the Layer 2 class of service value for each packet. The access point applies QoS policies in this order.

Packets already classified

When the access point receives packets from a QoS-enabled switch or router that has already classified the packets with non-zero 802.1Q/P user_priority values, the access point uses that classification and does not apply other QoS policy rules to the packets. An existing classification takes precedence over all other policies on the access point.

IMPORTANT Even if you have not configured a QoS policy, the access point always honors tagged 802.1P packets that it receives over the radio interface.

QoS Element for Wireless Phones setting

If you enable the QoS Element for Wireless Phones setting, dynamic voice classifiers are created for some of the wireless phone vendor clients, that lets the wireless phone traffic to be a higher priority than other clients' traffic. Additionally, the QoS Basic Service Set (QBSS) is enabled to advertise channel load information in the beacon and probe response frames. Some IP phones use QBSS elements to determine the access point to associate to, based on the traffic load.

Configure QoS by Using Stratix 5100 Device Manager

These steps describe how to configure quality of service (QoS) on your access point. With this feature, you can provide preferential treatment to certain traffic at the expense of others. Without QoS, the access point offers best-effort service to each packet, regardless of the packet contents or size.

Typically, networks operate on a best-effort delivery basis, that means all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure QoS on the access point, you can choose specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your wireless LAN makes network performance more predictable and bandwidth utilization more effective.

When you configure QoS, you create QoS policies and apply the policies to the VLANs configured on your access point. If you do not use VLANs on your network, you can apply your QoS policies to the access point's Ethernet and radio ports.

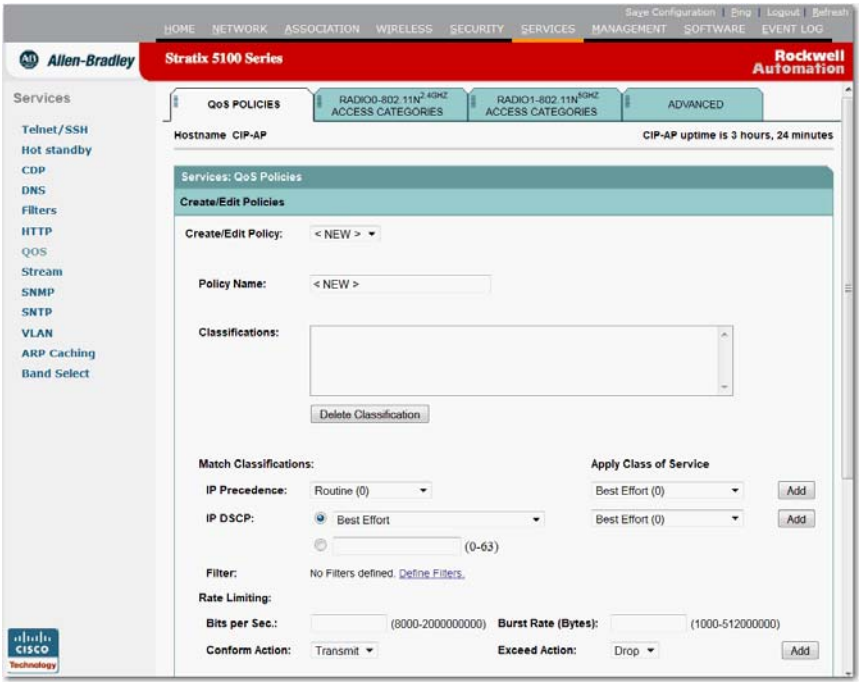
QoS is enabled in the default Stratix 5100 configuration. Before configuring or modifying QoS on your access point, keep this information in mind:

- The most important guideline in QoS deployment is to be familiar with the traffic on your wireless LAN. If you know the applications used by wireless client devices, the sensitivity of the applications to delay, and the amount of traffic associated with the applications, you can configure QoS to improve performance.
- QoS does not create additional bandwidth for your wireless LAN; it helps control the allocation of bandwidth. If you have plenty of bandwidth on your wireless LAN, you might not need to configure QoS.

IMPORTANT If you use VLANs on your wireless LAN, make sure the necessary VLANs are configured on your access point before configuring QoS.

Follow these steps to configure QoS on your access point.

1. From the top menu, click Services.
2. From the Services menu, click QoS.



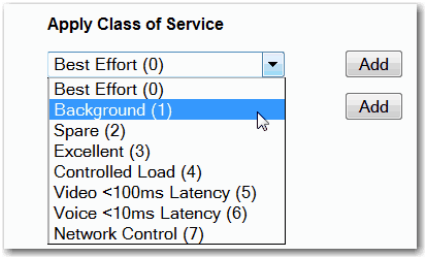
3. Select <NEW> Create/Edit Policy field or select an existing policy.
4. Type a name for the QoS policy in the Policy Name entry field.

   The name can contain up to 25 alphanumeric characters. Do not include spaces in the policy name.

   If the packets you need to prioritize contain IP precedence information in the IP header TOS field, select an IP precedence classification from the IP Precedence pull-down menu. Menu selections include these items:

   - Routine (0)
   - Priority (1)
   - Immediate (2)
   - Flash (3)
   - Flash Override (4)
   - Critic/CCP (5)
   - Internet Control (6)
   - Network Control (7)

5. From the Apply Class of Service pull-down menu, select the class of service that you want the access point to apply packets to the type that you selected from the IP Precedence menu.



6. The access point matches your IP Precedence selection with your class of service selection.

These are the settings in the Apply Class of Service menu:

- Best Effort (0)
- Background (1)
- Spare (2)
- Excellent (3)
- Control Lead (4)
- Video <100 ms Latency (5)
- Voice <100 ms Latency (6)
- Network Control (7)

7. Click Add beside the Class of Service menu for IP Precedence.

The classification appears in the Classifications field. To delete a classification, select it and click Delete beside the Classifications field.

If the packets that you need to prioritize contain IP DSCP precedence information in the IP header TOS field, select an IP DSCP classification from the IP DSCP pull-down menu. These are the menu choices:

- Best Effort
- Assured Forwarding - Class 1 Low
- Assured Forwarding - Class 1 Medium
- Assured Forwarding - Class 1 High
- Assured Forwarding - Class 2 Low
- Assured Forwarding - Class 2 Medium
- Assured Forwarding - Class 2 High
- Assured Forwarding - Class 3 Low
- Assured Forwarding - Class 3 Medium
- Assured Forwarding - Class 3 High
- Assured Forwarding - Class 4 Low

- Assured Forwarding - Class 4 Medium
- Assured Forwarding - Class 4 High
- Class Selector 1
- Class Selector 2
- Class Selector 3
- Class Selector 4
- Class Selector 5
- Class Selector 6
- Class Selector 7
- Expedited Forwarding

8. From the Apply Class of Service pull-down menu, select the class of service that you want the access point to apply to packets of the type that you selected from the IP DSCP menu.

   The access point matches your IP DSCP selection with your class of service selection.

9. Click Add beside the Class of Service menu for IP DSCP.

   The classification appears in the Classifications field.

   If you need to prioritize the packets from Spectralink phones (IP Protocol 119) on your wireless LAN, use Apply Class of Service. Select the class of service that you want the access point to apply to Spectralink phone packets. The access point matches Spectralink phone packets with your class of service selection.

10. Click Add beside the Class of Service menu for IP Protocol 119.

    The classification appears in the Classifications field.

    If you want to set a default classification for all packets on a VLAN, use Apply Class of Service to select the class of service that you want the access point to apply all packets on a VLAN. The access point matches all packets with your class of service selection.

11. Click Add beside the Class of Service menu for Default classification for packets on the VLAN.

    The classification appears in the Classifications field.

12. When you finish adding classifications to the policy, click Apply under the Apply Class of Service pull-down menu.
    - To cancel the policy and reset all fields to defaults, click Cancel below the Apply Class of Service pull-down menus.
    - To delete the entire policy, click Delete below the Apply Class of Service pull-down menus.

13. Use the Apply Policies to Interface/VLANs pull-down menus to apply policies to the access point Ethernet and radio ports.
    - If VLANs are configured on the access point, pull-down menus for each VLAN's virtual ports appear in this section.
    - If VLANs are not configured on the access point, pull-down menus for each interface appear.
14. Click Apply at the bottom of the page to apply the policies to the access point ports.

    If you want the access point to give priority to all voice packets regardless of VLAN, click the Advanced tab.

You can use the Cisco IOS command `dot11 phone dot11e` to enable support for the standard QBSS Load IE.

This example shows how to enable IEEE 802.11 phone support with the legacy QBSS Load element:

```
AP(config)# dot11 phone
```

This example shows how to enable IEEE 802.11 phone support with the standard (IEEE 802.11e) QBSS Load element:

```
AP(config)# dot11 phone dot11e
```

This example shows how to stop or disable the IEEE 802.11 phone support:

```
AP(config)# no dot11 phone
```

15. Policies you create on the access point—QoS Policies that you create and apply to VLANs or to the access point interfaces are third in precedence after previously classified packets and the QoS Element for Wireless Phones setting.
16. Default classification for all packets on VLAN—If you set a default classification for all packets on a VLAN, that policy is fourth in the precedence list.

Wi-Fi Multimedia Mode

When you enable QoS, the access point uses Wi-Fi Multimedia (WMM) mode by default. WMM provides these enhancements over basic QoS mode:

- The access point adds each packet's class of service to the packet's 802.11 header to be passed to the receiving station.
- Each access class has its own 802.11 sequence number. The sequence number allows a high-priority packet to interrupt the retries of a lower-priority packet without overflowing the duplicate checking buffer on the receiving side.
- WPA replay detection is done per access class on the receiver. Like 802.11 sequence numbering, WPA replay detection allows high-priority packets to interrupt lower priority retries without signalling a replay on the receiving station.
- For access classes that are configured to allow it, transmitters that are qualified to transmit through the normal backoff procedure are allowed to send a set of pending packets during the configured transmit opportunity (a specific number of microseconds). Sending a set of pending packets improves throughput because each packet does not have to wait for a backoff to gain access; instead, the packets can be transmitted immediately one after the other.
- U-APSD Power Save is enabled.

The access point uses WMM enhancements in packets sent to client devices that support WMM. The access point applies basic QoS policies to packets sent to clients that don't support WMM.

Use the no dot11 qos mode wmm configuration interface command to disable WMM by using CLI. To disable WMM by using the web browser interface, unselect the check boxes for the radio interfaces on the QoS Advanced page.

IGMP Snooping

When Internet Group Membership Protocol (IGMP) snooping is enabled on a switch and a client roams from one access point to another, the clients' multicast session is dropped. When the access points' IGMP snooping helper is enabled, the access point sends a general query to the wireless LAN, prompting the client to send in an IGMP membership report. When the network infrastructure receives the host's IGMP membership report, it makes sure that the delivery of that host's multicast data stream.

The IGMP snooping helper is enabled by default. To disable it, browse to the QoS Policies - Advanced page, check Disable, and click Apply.

IMPORTANT If there is no multicast router for processing IGMP query and response from the host, it is mandatory that no igmp snooping be configured on the access point. when IGMP snooping is enabled, all multicast group traffic must send IGMP query and response packets. If IGMP query or response packets are not detected, all multicast traffic for the group is dropped.

AVVID Priority Mapping

AVVID priority mapping maps Ethernet packets tagged as class of service 5 to class of service 6. This feature enables the access point to apply the correct priority to voice packets for compatibility with Cisco AVVID networks.

AVVID priority mapping is enabled by default. To disable it, browse to the QoS Policies - Advanced page, select No for Map Ethernet Packets with CoS 5 to CoS 6, and click Apply.

WiFi Multimedia (WMM)

By using the Admission Control check boxes, you can enable WMM on the access point's radio interface. When you enable admission control, clients associated to the access point must complete the WMM admission control procedure before they can use that access category.

Rate Limiting

Rate limiting provides control over the data traffic transmitted or received on an interface.The Class-Based Policing feature performs the following functions:

- Limits the input or output transmission rate of a class of traffic based on user-defined criteria.
- Marks packets by setting the IP precedence value, IP differentiated services code point (DSCP) value and Quality of Service (QoS) group.

This is used to rate-limit the upstream traffic originating from each of the non-roots to root bridge incase of P2MP setup. To do rate-limiting on downstream traffic, class-maps are applied at the root-side router/switch.

IMPORTANT Rate-limiting can be applied only to ethernet ingress.

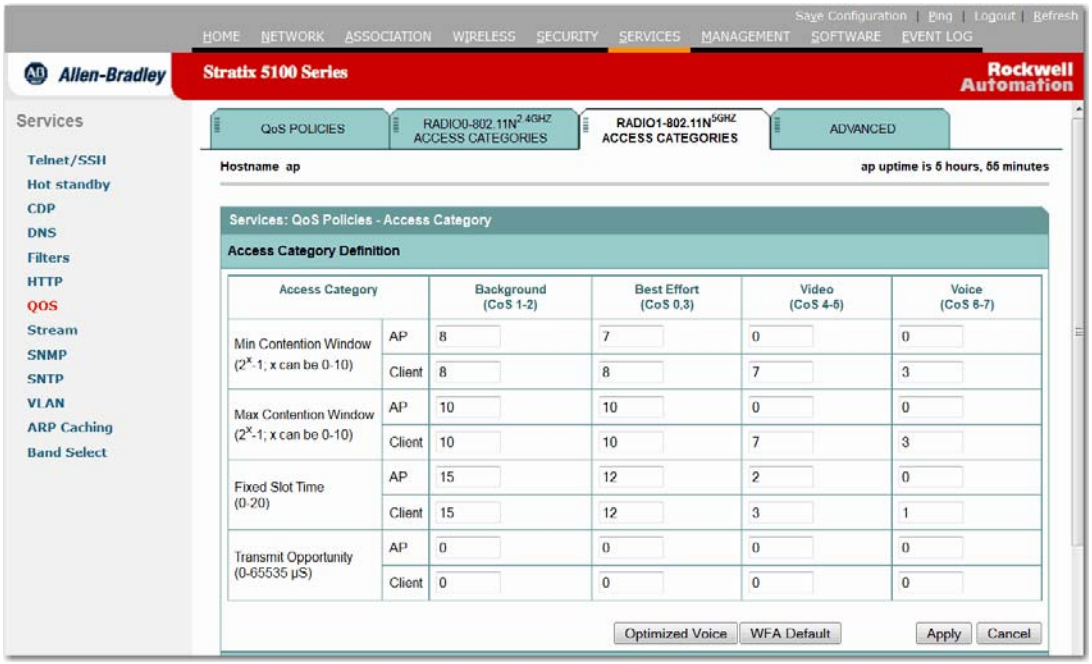
Adjust Radio Access Categories

The access point uses the radio access categories to calculate backoff times for each packet. As a rule, high-priority packets have short backoff times.

The default values in the Min and Max Contention page fields and in the Slot Time fields are based on settings recommended in IEEE Standard 802.11e. For detailed information on these values, consult that standard. The Stratix 5100 access point is preconfigured with values that are optimized for industrial control traffic.

This figure shows the Radio Access Categories page. Dual-radio access points have a Radio Access Categories page for each radio.

Figure 102 - Radio Access Categories Page



Configure Nominal Rates

When an access point receives an ADDTS (add traffic stream) request from a WMM client, it checks the nominal rate or minimum PHY rate in the ADDTS request against the nominal rates defined by the CLI command traffic-stream. If they don't match, the access point rejects the ADDTS request.

If you choose Optimized Voice Settings (see Figure 102 on page 425), the following nominal rates are configured:

- 5.5 Mbps, 6.0 Mbps, 11.0 Mbps, 12.0 Mbps, and 24.0 Mbps

IMPORTANT The above rates work fine for Cisco phones. Third parties wireless phones can have a different nominal rate or minimum PHY rate. You need to enable additional nominal rates for these phones.

Optimized Voice Settings

By using the Admission Control check boxes, you can control client use of the access categories. When you enable admission control for an access category, clients associated to the access point must complete the WMM admission control procedure before they can use that access category.

Configure Call Admission Control

Configuring Call Admission Control (CAC) on an access point involves these steps.

1. Configuring the radio.
2. Enabling admission control on an SSID.

Follow these steps to configure admission control on an access point's radio.

For a list of Cisco IOS commands for configuring admission control by using CLI, see the Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Guide.

1. Click the Access Categories page of the radio you want to configure.

Figure 102 on page 425 shows an example of an Access Categories page.

2. Check Admission Control under Voice (CoS 6-7).
3. Enter the maximum percentage of the channel to be used for voice in the Max Channel Capacity (%) field.
4. Enter the maximum percentage of the channel to use for roaming calls in the Roam Channel Capacity (%) field.

The percentage of the channel used by roaming calls up to the value specified in this field is deducted from the value you specified in the Max Channel Capacity (%) field.

For example, suppose you have entered 75% in the Max Channel Capacity (%) field and 6% in the Roam Channel Capacity (%). If roaming calls are using 5% of the channel, a maximum of 70% of the channel can be used for voice.

5. To use video access category (AC = 2) for signaling, check Admission Control under Video(CoS 4-5).

IMPORTANT The admission control settings you have configured does not take effect until you enable admission control on an SSID.

Enabling Admission Control

Follow these steps to enable admission control on an SSID.

1. Open the SSID Manager page.
2. Select an SSID.
3. Under General Settings, select Enable in the Call Admission Control field.

Troubleshoot Admission Control

You can use two CLI commands to display information to help you troubleshoot admission control problems:

- To display current admission control settings on radio 0, enter the following command:

  ```
  # show dot11 cac int dot11Radio 0
  ```

- To display current admission control settings on radio 1, enter the following command:

  ```
  # show dot11 cac int dot11Radio 1
  ```

- To display information about admitted streams with admission control and MT, enter the following command:

  ```
  # show dot11 traffic-streams
  ```

Notes:

Configure Filters

This chapter describes how to configure and manage MAC address, IP, and Ethertype filters on the access point by using the web browser interface.

Topic	Page
Filters	429
Configure Filters by Using CLI Commands	430
Configure Filters by Using Stratix 5100 Device Manager	432

Filters

Protocol filters (IP protocol, IP port, and Ethertype) prevent or allow the use of specific protocols through the access point's Ethernet and radio ports. You can set up individual protocol filters or sets of filters. You can filter protocols for wireless client devices, users on the wired LAN, or both. For example, an SNMP filter on the access point's radio port prevents wireless client devices from using SNMP with the access point but does not block SNMP access from the wired LAN.

IP address and MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific IP or MAC addresses. You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify.

You can configure filters by using the web browser interface or by entering commands in CLI.

TIP You can include filters in the access point's QoS policies. See Configure Quality of Service (QoS) on page 415 for detailed instructions on setting up QoS policies.

By using CLI, you can configure up to 2,048 MAC addresses for filtering. By using the web browser interface, however, you can configure only up to 43 MAC addresses for filtering.

Configure Filters by Using CLI Commands

To configure filters by using CLI commands, you use access control lists (ACLs) and bridge groups.

IMPORTANT Avoid using both CLI and the web browser interfaces to configure the wireless device. If you configure the wireless device by using CLI, the web browser interface can display an inaccurate interpretation of the configuration. However, the inaccuracy does not necessarily mean that the wireless device is misconfigured. For example, if you configure ACLs by using CLI, the web browser interface can display this message:

> Filter 700 was configured on interface `Dot11Radio0` by using CLI commands. It must be cleared via CLI for proper operation of the web interface.

If you see this message, use CLI to delete the ACLs and use the web browser interface to reconfigure them.

Create a Time-base ACL

Time-based ACLs are ACLs that can be enabled or disabled for a specific period of time. This capability provides robustness and the flexibility to define access control policies that either permit or deny certain kinds of traffic.

This example illustrates how to configure a time-based ACL through CLI, where Telnet connection is permitted from the inside to the outside network on weekdays during business hours:

IMPORTANT A time-based ACL can be defined either on the Gigabit Ethernet port or on the Radio port of the Stratix 5100 access point, based on your requirements. It is never applied on the Bridge Group Virtual Interface (BVI).

Follow these steps to create a time-based ACL.

1. Log in to the AP through CLI.
2. Use the console port or Telnet to access the ACL through the Ethernet interface or the wireless interface.
3. Enter global configuration mode.
4. Create a Time Range. For this example, Test:

   ```
   AP<config>#time-range Test
   ```

5. Create a time-range:

   ```
   AP<config>#time-range periodic weekdays 7:00 to
   19:00
   ```

   This lets users have access during weekdays from 7:00...19:00 hours.

6. Create an ACL. For this example, 101:

   ```
   AP<config># ip access-list extended 101
   ```

```
AP<config-ext-nacl>#permit tcp 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255 eq telnet time-range Test
```

IMPORTANT This ACL permits Telnet traffic to and from the network for the specified time-range Test. It also permits a Telnet session to the AP on weekdays.

7. Apply the time-based ACL to the Ethernet interface:

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
```

ACL Logging

ACL logging is not supported on the bridging interfaces of AP platforms. When applied on bridging interface, it works as if configured without the log option and logging does not take effect. However, ACL logging works well for the BVI interfaces as long as a separate ACL is used for the BVI interface.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the Block or Allow Client Association to the Access Point by Using MAC Address ACLs on page 436.

```
AP# configure terminal
AP(config)# dot11 association access-list 777
AP(config)# end
```

In this example, only client devices with MAC addresses listed in access list 777 are allowed to associate to the access point. The access point blocks associations from all other MAC addresses.

For complete descriptions of the commands used in this example, Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges.

Configure Filters by Using Stratix 5100 Device Manager

This section describes how to configure and manage MAC address, IP, and Ethertype filters on the access point by using the web-browser interface, Stratix 5100 Device Manager.

You complete these two steps to configure and enable a filter.

1. Name and configure the filter by using the filter setup pages.
2. Enable the filter.

For detailed instructions, see these sections:

- Configure and Enable MAC Address Filters on page 433
- Configure and Enable IP Filters on page 438
- Configure and Enable Ethertype Filters on page 444

Configure and Enable MAC Address Filters

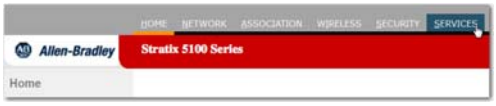
MAC address filters allow or disallow the forwarding of unicast and multicast packets addressed to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

IMPORTANT	By using CLI commands, you can configure MAC addresses for filtering, but because of a NVRAM limitation, you need FTP or TFTP for more than 600 MAC filters. By using the web browser interface, however, you can configure only up to 43 MAC addresses for filtering.

IMPORTANT	MAC address filters are powerful, and you can lock yourself out of the access point if you make a mistake setting up the filters. If you accidentally lock yourself out of your access point, use CLI to disable the filters.

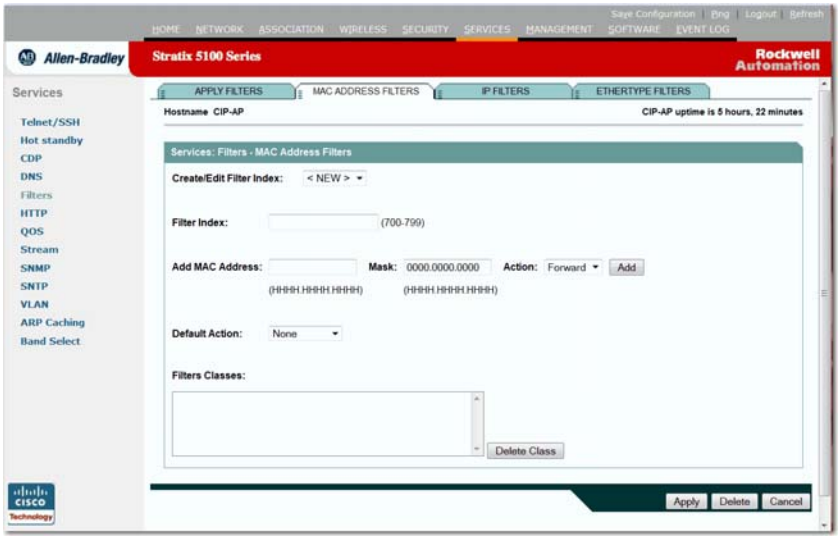
Use the MAC Address Filters page to create MAC address filters for the access point. Follow these steps to create a MAC address filter.

1. From the top navigation menu, click Services.



2. From the Services menu, click Filters to move to the Services: Filters - Apply Filters page.

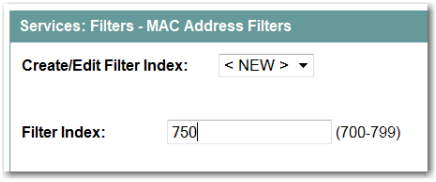
3. On the Apply Filters page, click the MAC Address Filters tab at the top of the page.



If you are creating a new MAC address filter, make sure <NEW> (the default) is selected in the Create/Edit Filter Index menu.

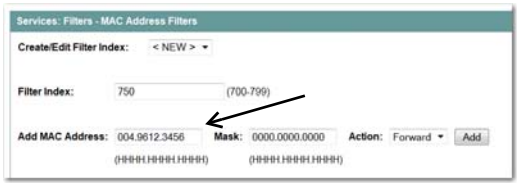
To edit a filter, select the filter number from the Create/Edit Filter Index menu.

4. In the Filter Index field, name the filter with a number from 700...799.



The number you assign creates an access control list (ACL) for the filter.

5. Enter a MAC address in the Add MAC Address field.



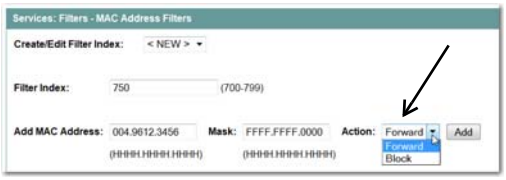
Enter the address with periods separating the three groups of four characters, for example, 0040.9612.3456.

TIP If you plan to block traffic to all MAC addresses except those you specify as allowed, put your own MAC address in the list of allowed MAC addresses.

6. Use the Mask entry field to indicate how many bits, from left to right, the filter checks against the MAC address.

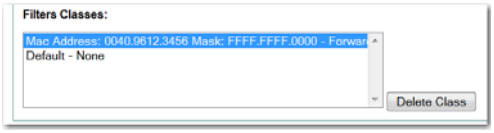
   For example, to require an exact match with the MAC address (to check all bits) enter FFFF.FFFF.FFFF. To check only the first 4 bytes, enter FFFF.FFFF.0000.

7. From the Action pull-down menu, choose Forward or Block.



8. Click Add.

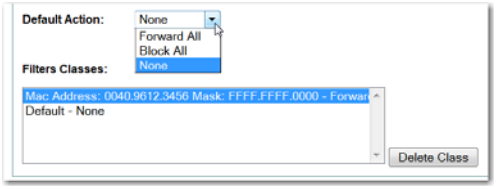
   The MAC address appears in the Filters Classes field.



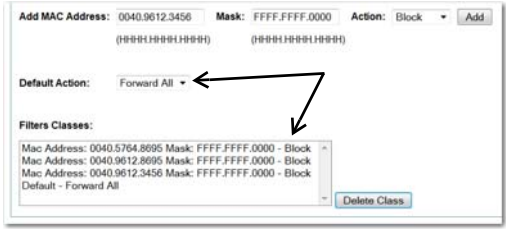
   To remove the MAC address from the Filters Classes list, select it and click Delete Class.

9. Repeat step 5 through step 8 to add addresses to the filter.

10. From the Default Action menu, choose Forward All or Block All.



   The default action of the filter must be the opposite of the action for at least one of the addresses in the filter.



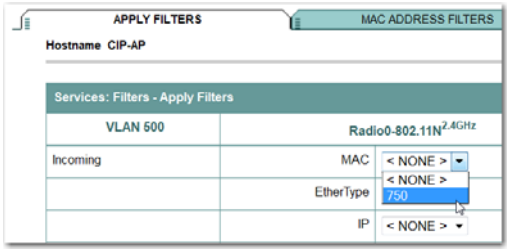
For example, if you enter several addresses and you choose Block as the action for all of them, you must choose Forward All as the filter's default action.

11. Click Apply.

    The filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.

12. Return to the Apply Filters page.

13. From one of the MAC pull-down menus, select the filter number.



    You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.

14. Click Apply.

    The filter is enabled on the selected ports.

If clients are not filtered immediately, click Reload on the System Configuration page to restart the access point. To reach the System Configuration page, click System Software on the task menu and then click System Configuration.

IMPORTANT Client devices with blocked MAC addresses cannot send or receive data through the access point, but they can remain in the Association Table as unauthenticated client devices. Client devices with blocked MAC addresses disappear from the Association Table when the access point stops monitoring them, when the access point restarts, or when the clients associate to another access point.

Block or Allow Client Association to the Access Point by Using MAC Address ACLs

You can use MAC address ACLs to block or allow association to the access point. Instead of filtering traffic across an interface, you use the ACL to filter associations to the access point radio.

Follow these steps to use an ACL to filter associations to the access point radio.

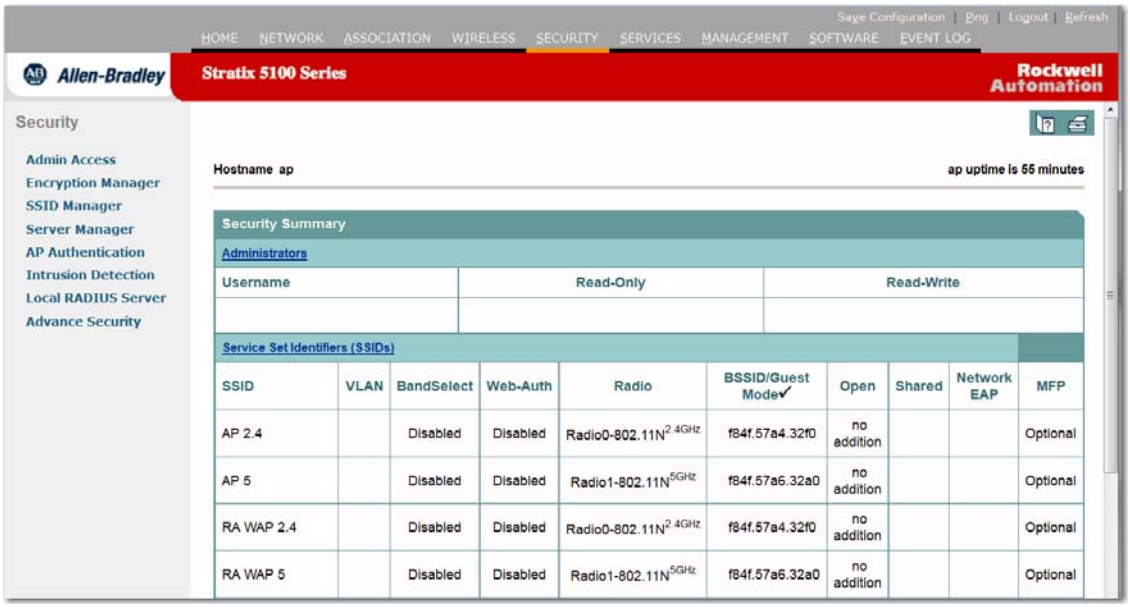
1. Follow Steps 1 through 10 in the Configure and Enable MAC Address Filters on page 433 to create an ACL.

   For MAC addresses that you want to allow to associate, choose Forward from the Action menu. Select Block for addresses that you want to prevent from associating. Select Block All from the Default Action menu.

2. From the main menu, click Security.

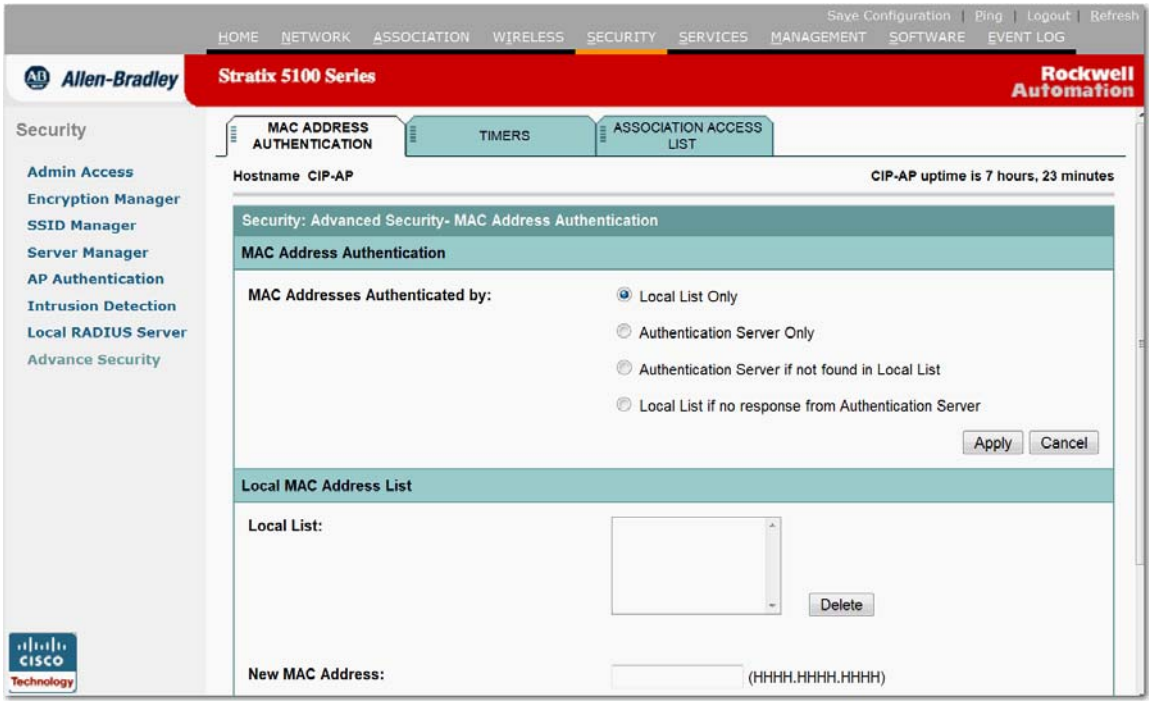
This figure shows the Security Summary page.

Figure 103 - Security Summary Page



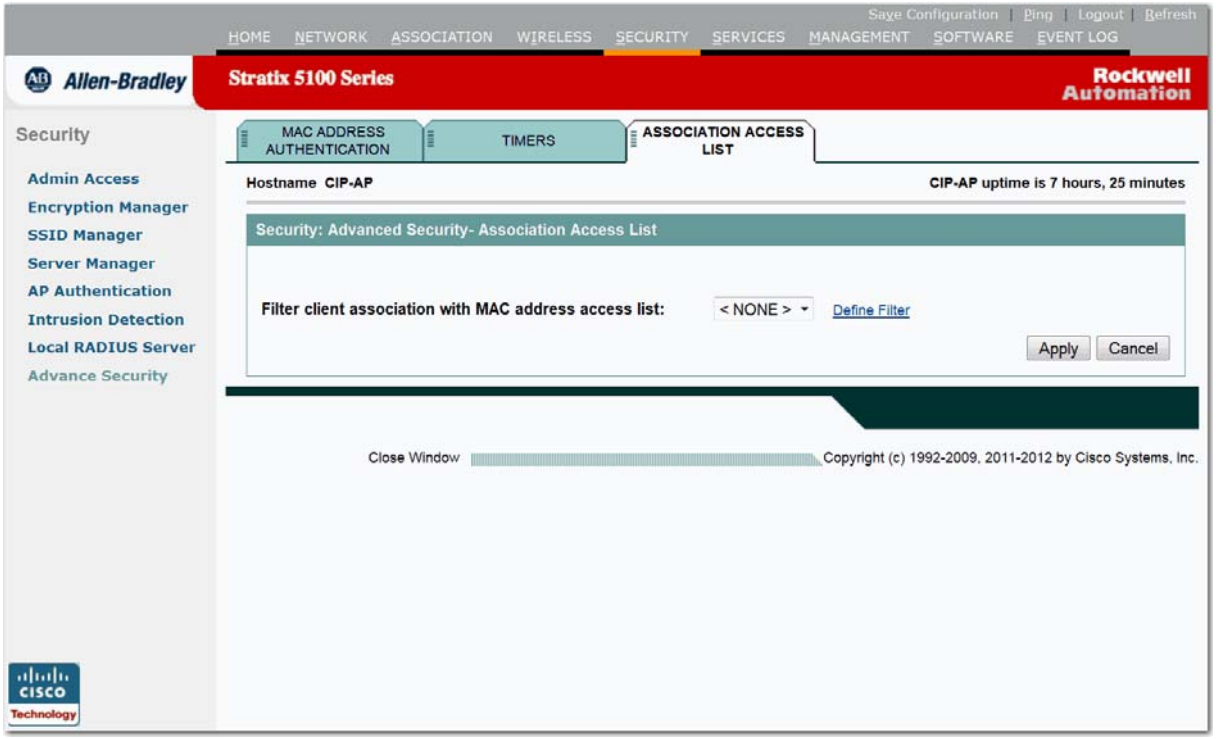
3. Click Advanced Security.

Figure 104 - Advanced Security: MAC Address Authentication Page



4. Click Association Access List tab.

Figure 105 - Association Access List Page



5. Select your MAC address ACL from the pull-down menu.
6. Click Apply.

Configure and Enable IP Filters

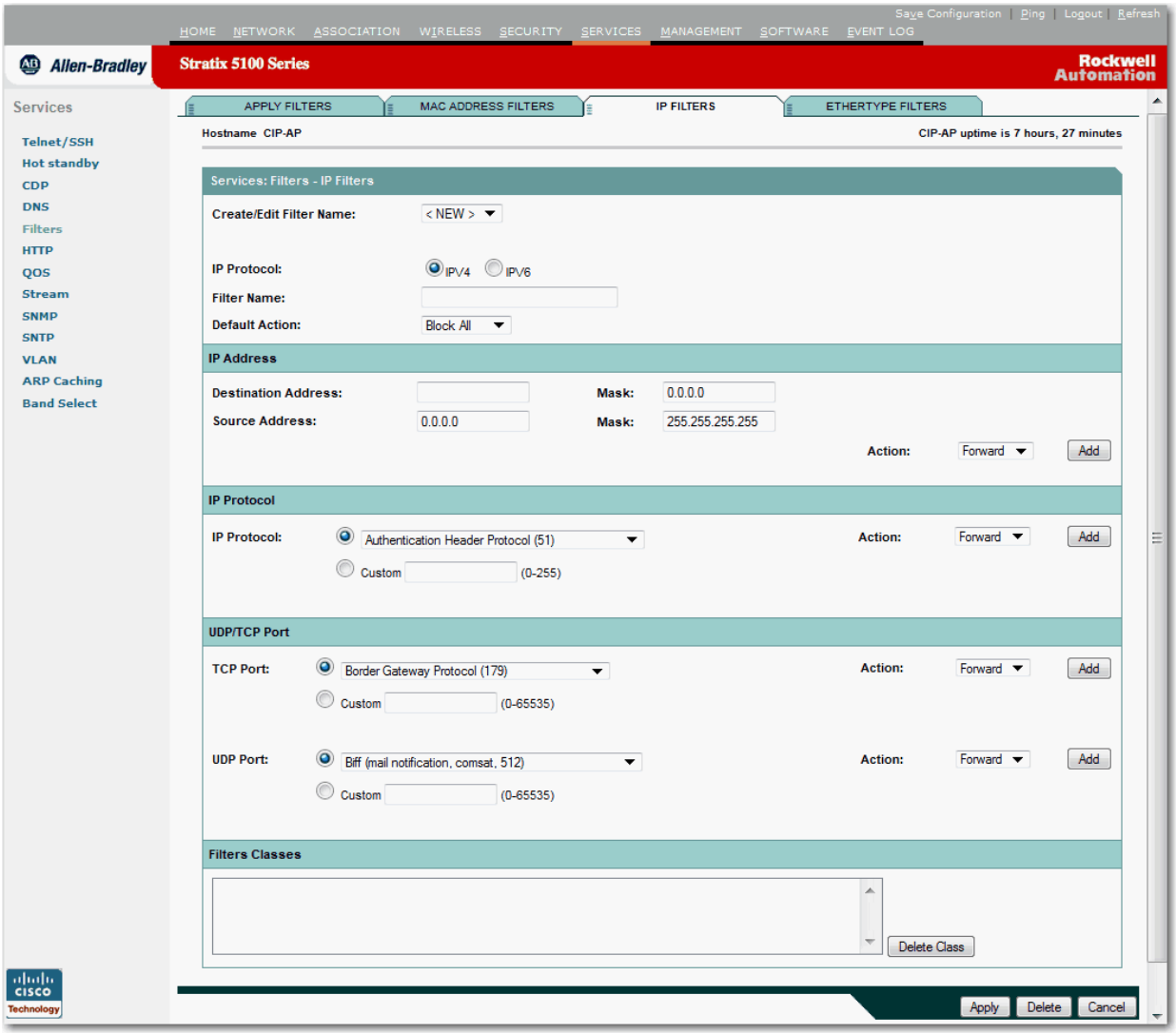
IP filters (IP address, IP protocol, and IP port) prevent or allow the use of specific protocols through the access point's Ethernet and radio ports, and IP address filters allow or prevent the forwarding of unicast and multicast packets either sent from or addressed to specific IP addresses.

You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify. You can create filters that contain elements of one, two, or all three IP filtering methods. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Use the IP Filters page to create IP filters for the access point.

1. rom the main menu, click Services.
2. In the Services page list, click Filters.
3. On the Apply Filters page, click the IP Filters tab.

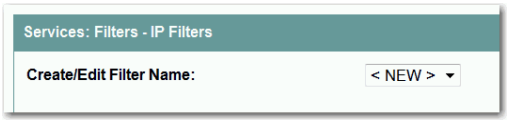
Figure 106 - IP Filters Page



Create an IP Filter

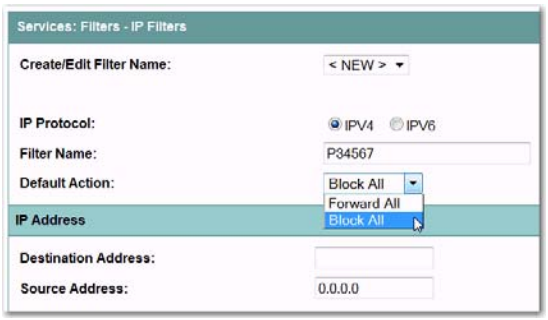
Follow these steps to create an IP filter.

1. If you are creating a new filter, make sure <NEW> (the default) is selected in the Create/Edit Filter Name menu.



   To edit an existing filter, select the filter name.

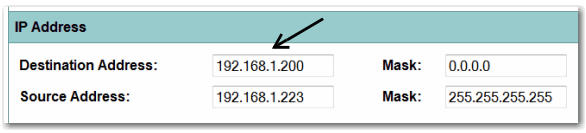
2. Enter a descriptive name for the new filter in the Filter Name field.
3. From the Default Action pull-down, select Forward all or Block all.



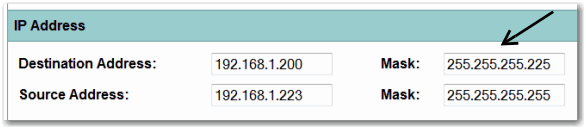
   The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you create a filter containing an IP address, an IP protocol, and an IP port and you select Block as the action for all of them, you must choose Forward All as the filter's default action.

4. To filter an IP address, enter an address in the IP Address field.

IMPORTANT If you plan to block traffic to all IP addresses except those you specify as allowed, put the address of your computer in the list of allowed addresses to avoid losing connectivity to the access point.



5. Type the mask for the IP address in the Mask field.



Enter the mask with periods separating the groups of characters, for example, 112.334.556.778.

If you enter 255.255.255.255 as the mask, the access point accepts any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered in the IP Address field. The mask you enter in this field behaves the same way that a mask behaves when you enter it in CLI.

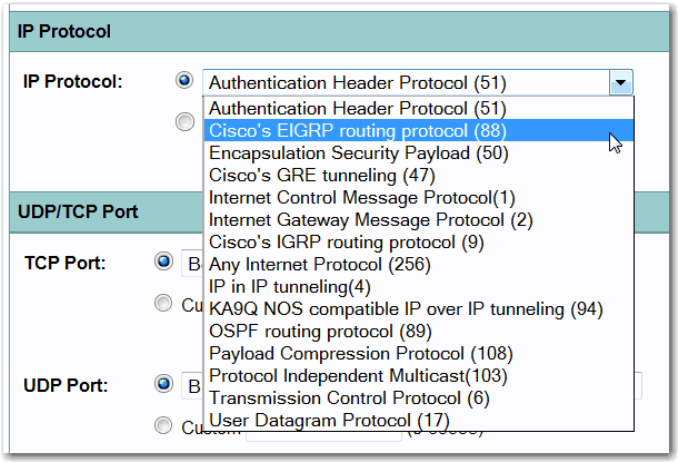
6. From the Action menu, select Forward or Block.

7. Click Add.

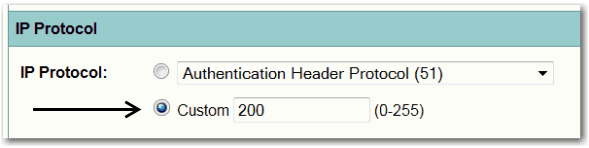
The address appears in the Filters Classes field. To remove the address from the Filters Classes list, select it and click Delete Class.

If you don't need to add IP protocol or IP port elements to the filter, skip to step 15 to save the filter on the access point.

8. To filter an IP protocol, select one of the common protocols from the IP Protocol pull-down menu, or select the Custom radio button and enter the number of an existing ACL in the Custom field.



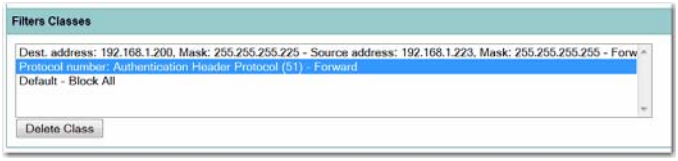
Enter an ACL number from 0...255. See Protocol Filters on page 527 for a list of IP protocols and their numeric designators.



9. From the Action menu, select Forward or Block.

10. Click Add.

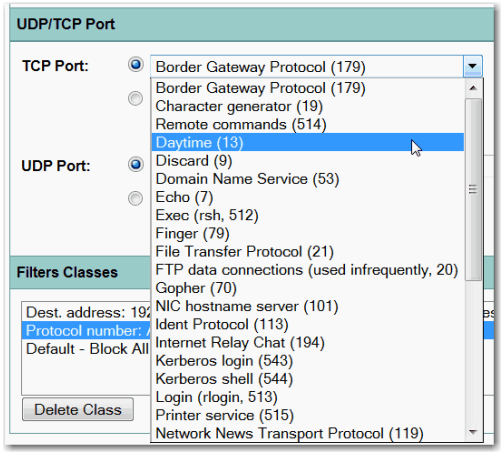
The protocol appears in the Filters Classes field.



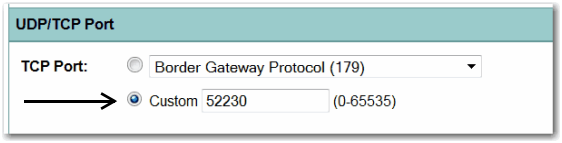
To remove the protocol from the Filters Classes list, select it and click Delete Class.

If you don't need to add IP port elements to the filter, skip to step 15 to save the filter on the access point.

11. To filter a TCP or UDP port protocol, select one of the common port protocols from the TCP Port or UDP Port pull-down menus, or select the Custom radio button and enter the number of an existing protocol in one of the Custom fields.



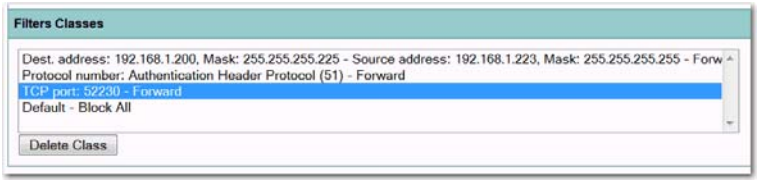
12. Enter a protocol number from 0...65535.



13. From the Action menu, select Forward or Block.

14. Click Add.

    The protocol appears in the Filters Classes field.



    To remove the protocol from the Filters Classes list, select it and click Delete Class.

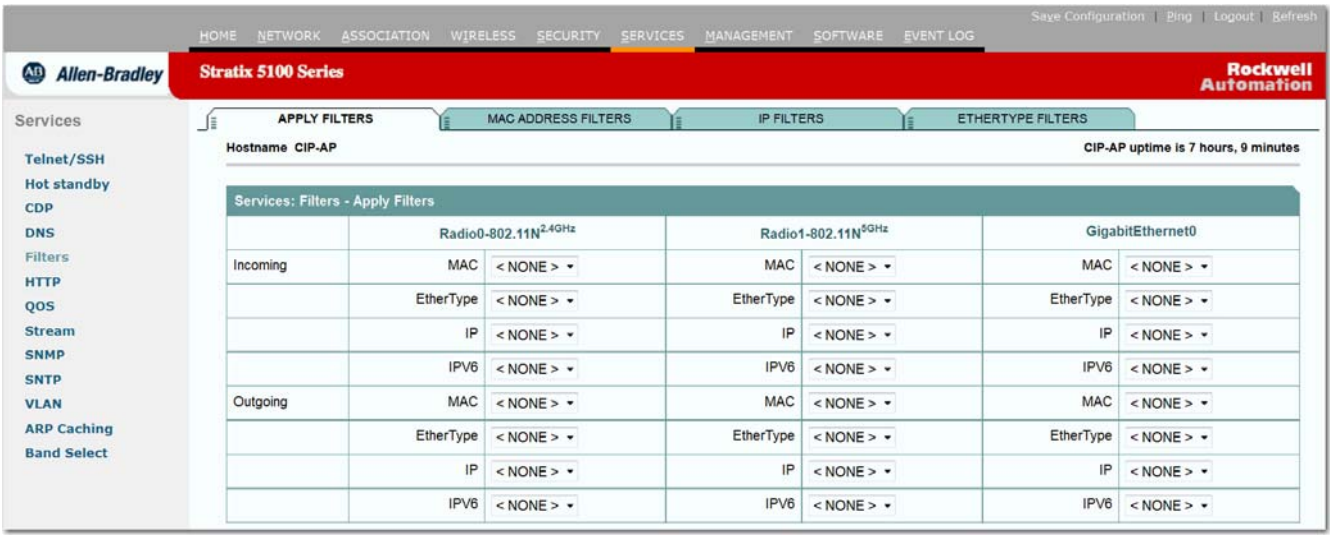
15. When the filter is complete, click Apply.

    The filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.

16. Click the Apply Filters tab to return to the Apply Filters page.

    Figure 107 on page 443 shows the Apply Filters page.

Figure 107 - Apply Filters Page



17. From one of the IP pull-down menu, select the filter name.

    You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.

18. Click Apply.

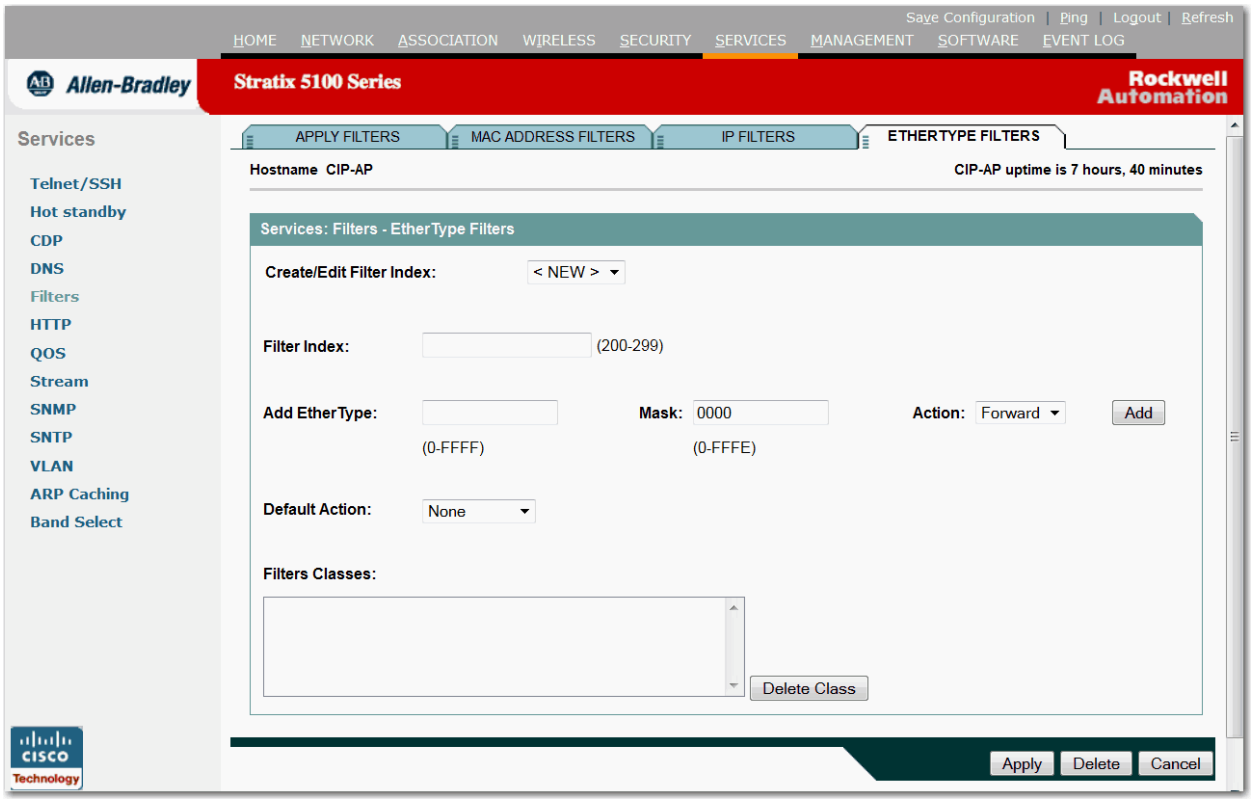
    The filter is enabled on the selected ports.

Configure and Enable Ethertype Filters

Ethertype filters prevent or allow the use of specific protocols through the access point's Ethernet and radio ports. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Use the Ethertype Filters page to create Ethertype filters for the access point. This figure shows the Ethertype Filters page.

Figure 108 - Ethertype Filters Page



Follow these steps to go to the Ethertype Filters page.

1. From the main menu, click Services.
2. In the Services page list, click Filters.
3. On the Apply Filters page, click the Ethertype Filters tab.

Create an Ethertype Filter

Follow these steps to create an Ethertype filter:

1. Follow the link path to the Ethertype Filters page.
2. If you are creating a new filter, make sure <NEW> (the default) is selected in the Create/Edit Filter Index menu.

To edit an existing filter, select the filter number from the Create/Edit Filter Index menu.

3. In the Filter Index field, name the filter with a number from 200...299.

   The number you assign creates an access control list (ACL) for the filter.

4. Enter an Ethertype number in the Add Ethertype field.

   See Protocol Filters on page 527 for a list of protocols and their numeric designators.

5. Enter the mask for the Ethertype in the Mask field.

   If you enter 0, the mask requires an exact match of the Ethertype.

6. From the Action menu, select Forward or Block.

7. Click Add.

   The Ethertype appears in the Filters Classes field. To remove the Ethertype from the Filters Classes list, select it and click Delete Class. Repeat step 4 through step 7 to add Ethertypes to the filter.

8. From the Default Action menu, select Forward All or Block All

   The filter's default action must be the opposite of the action for at least one of the Ethertypes in the filter. For example, if you enter several Ethertypes and you choose Block as the action for all of them, you must choose Forward All as the filter's default action.

9. Click Apply.

   The filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.

10. Click the Apply Filters tab to return to the Apply Filters page.

11. From one of the Ethertype pull-down menus, select the filter number.

    You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.

12. Click Apply.

    The filter is enabled on the selected ports.

Notes:

Configure Cisco Discovery Protocol (CDP)

This chapter describes how to configure Cisco Discovery Protocol (CDP) on your access point. If you are not going to use CDP, we recommend that you turn the feature off.

IMPORTANT For complete syntax and usage information for the commands used in this chapter, see these publications:

- Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges
- Cisco IOS Configuration Fundamentals Command Reference for Release 12.2

For information about configuring CDP in Device Manager, see CDP Page on page 134.

Topic	Page
CDP	447
Configure CDP	448
Monitor and Maintain CDP	451
Default CDP Configuration	448
Configure the CDP Characteristics	448
Disable and Enable CDP	449
Disable and Enable CDP on an Interface	450

CDP

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices. Information in CDP packets is used in network management software.

CDP is enabled on the access point Ethernet port by default. However, CDP is enabled only on the access point radio port when the radio is associated to another wireless infrastructure device, such as an access point or a bridge. CDP is sent on the lowest VLAN number configured on the access point. When more than one VLAN is used in a wireless network, We recommend that the lowest VLAN number configured be used as the native VLAN

IMPORTANT For best performance on your wireless LAN, disable CDP on all radio interfaces and on sub-interfaces if VLANs are enabled on the access point.

Configure CDP

This section contains CDP configuration information and procedures.

Default CDP Configuration

This table lists the default CDP settings.

Table 109 - Default CDP Configuration

Feature	Default Setting
CDP global state	Enabled
CDP interface state	Enabled
CDP holdtime (packet holdtime in seconds)	180
CDP timer (packets sent every x seconds)	60

Configure the CDP Characteristics

You can configure the CDP holdtime (the number of seconds before the access point discards CDP packets) and the CDP timer (the number of seconds between each CDP packets the access point sends).

Beginning in Privileged Exec mode, follow these steps to configure the CDP holdtime and CDP timer.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. (Optional) Specify the amount of time you want a receiving device to hold the information sent by the device before discarding it.

   The range is from 10...255 s; the default is 180 s.

   ```
   cdp holdtime seconds
   ```

3. (Optional) Set the transmission frequency of CDP updates in seconds.

   The range is from 5...254 s; the default is 60 s.

   ```
   cdp timer seconds
   ```

4. Return to Privileged Exec mode.

   ```
   end
   ```

Use the `no` form of the CDP commands to return to the default settings.

This example shows how to configure and verify CDP characteristics:

```
AP# configure terminal
AP(config)# cdp holdtime 120
AP(config)# cdp timer 50
AP(config)# end
```

```
AP# show cdp

Global CDP information:
        Sending a holdtime value of 120 seconds
        Sending CDP packets every 50 seconds
```

For additional CDP `show` commands, see the Monitor and Maintain CDP on page 451.

Disable and Enable CDP

CDP is enabled by default. Beginning in Privileged EXEC mode, follow these steps to disable the CDP device discovery capability.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Disable CDP.

   ```
   no cdp run
   ```

3. Return to Privileged EXEC mode.

   ```
   end
   ```

Beginning in privileged EXEC mode, follow these steps to enable CDP:

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter CDP after disabling it.

   ```
   cdp run
   ```

3. Return to Privileged EXEC mode.

   ```
   end
   ```

This example shows how to enable CDP.

```
AP# configure terminal
AP(config)# cdp run
AP(config)# end
```

Disable and Enable CDP on an Interface

CDP is enabled by default on all supported interfaces to send and receive CDP information.

Beginning in privileged EXEC mode, follow these steps to disable CDP on an interface.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode, and enter the interface that you are disabling CDP.

   interface *interface-id*

3. Disable CDP on an interface.

   ```
   no cdp enable
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Beginning in privileged EXEC mode, follow these steps to enable CDP on an interface:

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode, and enter the interface that you are enabling CDP.

   `interface` *`interface-id`*

3. Enable CDP on an interface after disabling it.

   ```
   cdp enable
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

This example shows how to enable CDP on an interface.

```
AP# configure terminal
AP(config)# interface x
AP(config-if)# cdp enable
AP(config-if)# end
```

Monitor and Maintain CDP

To monitor and maintain CDP on your device, perform one or more of these tasks, beginning in privileged EXEC mode.

Command	Description
`clear cdp counters`	Reset the traffic counters to zero.
`clear cdp table`	Delete the CDP table of information about neighbors.
`show cdp`	Display global information, such as frequency of transmissions and the holdtime for packets being sent.
`show cdp entry` *`entry-name`* `[protocol | version]`	Display information about a specific neighbor. You can enter an asterisk (*) to display all CDP neighbors, or you can enter the name of the neighbor to get the information. You can also limit the display to information about the protocols enabled on the specified neighbor or information about the version of software running on the device.
`show cdp interface [`*`type number`*`]`	Display information about interfaces where CDP is enabled. You can limit the display to the type of interface or the number of the interface tho get the information, for example, entering `gigabitethernet 0/1`, only the information about Gigabit Ethernet port 1 appears.
`show cdp neighbors [`*`type number`*`] [detail]`	Display information about neighbors, including device type, interface type and number, holdtime settings, capabilities, platform, and port ID. You can limit the display to neighbors on a specific type or number of interface or expand the display to provide more detailed information.
`show cdp traffic`	Display CDP counters, including the number of packets sent and received and checksum errors.

Notes:

Configure Simple Network Management Protocol (SNMP)

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on your access point.

For complete syntax and usage information for the commands used in this chapter, see these publications:

- Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges
- Cisco IOS Configuration Fundamentals Command Reference for Release 12.3.

Topic	Page
SNMP	453
Configure SNMP	457
Display SNMP Status	465

SNMP

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. The SNMP manager can be part of a network management system (NMS). The agent and management information base (MIB) reside on the access point. To configure SNMP on the access point, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

SNMP Versions

This software release supports these SNMP versions:

- SNMPv1—The Simple Network Management Protocol, a full Internet standard, defined in RFC 1157.
- SNMPv2C, has these features:
  - SNMPv2—Version 2 of the Simple Network Management Protocol, a draft Internet standard, defined in RFCs 1902...1907.
  - SNMPv2C—The Community-based Administrative Framework for SNMPv2, an experimental Internet protocol defined in RFC 1901.
- SNMPv3, has these features:
  - Support for SHA and MD5 authentication protocols and DES56 encryption.
  - Three security levels: no authentication and no privacy (NoAuthNoPriv), authentication and no privacy (AuthNoPriv), and authentication and privacy (AuthPriv).

SNMPv3 supports the highest available levels of security for SNMP communication. Community strings for SNMPv1 and SNMPv2 are stored and transferred as plain text without encryption. In the SNMPv3 security model, SNMP users authenticate and join a user group. Access to system data is restricted based on the group.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; therefore, you can configure the software to support communication with one management station by using the SNMPv3 protocol and another by using the SNMPv2 or SNMPv1 protocol.

This table lists the SNMP versions and security levels supported on access points:

Table 110 - SNMP Versions and Security Levels

SNMP Version	Security Level	Authentication	Encryption
v1	NoAuthNoPriv	Community string match	None
v2C	NoAuthNoPriv	Community string match	None
v3	NoAuthNoPriv	Username match	None
v3	AuthNoPriv	HMAC-MD5 or HMAC-SHA algorithms	None
v3	AuthPriv	HMAC-MD5 or HMAC-SHA algorithms	DES 56-bit encryption

For detailed information on SNMPv3, see the publication Configuring Simple Network Management Protocol.

SNMP Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in this table.

Table 111 - SNMP Operations

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table.(2)
get-bulk-request(1)	Retrieves large blocks of data that otherwise requires that the transmission of many small blocks of data, such as multiple rows in a table.
get-response	Replies to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Stores a value in a specific variable.
trap	An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.

(1) The get-bulk command works only with SNMPv2.
(2) With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.

SNMP Agent Functions

The SNMP agent responds to SNMP manager requests as follows:

- Get a MIB variable - The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Set a MIB variable - The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. For the NMS to access the access point, the community string definitions on the NMS must match at least one of the three community string definitions on the access point.

A community string can have one of these attributes:

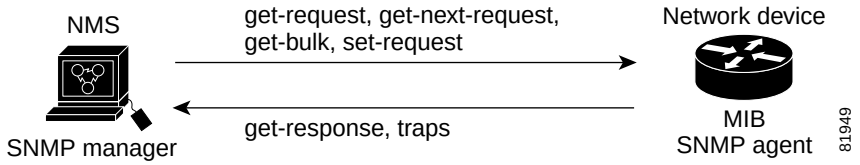
- Read-only - Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- Read-write - Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings

Access MIB Variables by Using SNMP

A Network Management Software (NMS) uses the access point MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can be displayed as a graph and analyzed to troubleshoot internet working problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown below, the SNMP agent gathers data from the MIB. The agent can send traps (notification of certain events) to the SNMP manager, that receives and processes the traps. Traps are messages alerting the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in `get-request`, `get-next-request`, and `set-request` format.

Figure 109 - SNMP Network



For information on supported MIBs and how to access them, see Supported Management Information Bases (MIBs) on page 517.

Configure SNMP

This section describes how to configure SNMP on your access point.

Default SNMP Configuration

This table shows the default SNMP configuration.

Feature	Default Setting
SNMP agent	Disabled
SNMP community strings	No strings are configured by default. However, when you enable SNMP by using the web browser interface, the access point automatically creates the public community with read-only access to the IEEE802dot11 MIB.
SNMP trap receiver	None configured
SNMP traps	None enabled

Enable the SNMP Agent

No specific CLI command exists to enable SNMP. The first `snmp-server` global configuration command that you enter enables the supported versions of SNMP.

You can also enable SNMP on the SNMP Properties page on the web browser interface. When you enable SNMP on the web browser interface, the access point automatically creates a community string called public with read-only access to the IEEE802dot11 MIB.

Configure Community Strings

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the access point.

Optionally, you can specify one or more of these characteristics associated with the string:

- An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent
- A MIB view, that defines the subset of all MIB objects accessible to the given community

- Read and write or read-only permission for the MIB objects accessible to the community

TIP In the current Cisco IOS MIB agent implementation, the default community string is for the Internet MIB object sub-tree. Because IEEE802dot11 is under another branch of the MIB object tree, you must enable either a separate community string and view on the IEEE802dot11 MIB or a common view and community string on the ISO object in the MIB object tree.

ISO is the common parent node of IEEE (IEEE802dot11) and Internet. This MIB agent behavior is different from the MIB agent behavior on access points not running Cisco IOS software.

Beginning in privileged EXEC mode, follow these steps to configure a community string on the access point.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Configure the community string.
   - For string, specify a string that acts like a password and permits access to the SNMP protocol. You can configure one or more community strings of any length.
   - (Optional) For access-list-number, enter an IP standard access list numbered from 1...99 and 1300...1999.
   - (Optional) For view mib-view, specify a MIB view where the community has access, such as ieee802dot11.

     See the snmp-server view Command on page 462 for instructions on using the snmp-server view command to access Standard IEEE 802.11 MIB objects through IEEE view.
   - (Optional) Specify either read-only (ro) if you want authorized management stations to retrieve MIB objects, or specify read/write (rw) if you want authorized management stations to retrieve and modify MIB objects. By default, the community string permits read-only access to all objects.

   TIP To access the IEEE802dot11 MIB, you must enable either a separate community string and view on the IEEE802dot11 MIB or a common view and community string on the ISO object in the MIB object tree.

   ```
   snmp-server community string
   [ access-list-number ]
   [ view mib-view ]
   [ro | rw]
   ```

3. (Optional) If you specified an IP standard access list number in Step 2, then create the list, repeating the command as many times as necessary.
   - For access-list-number, enter the access list number specified in Step 2.
   - The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched.

- For source, enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent.
- (Optional) For source-wildcard, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.

4. Recall that the access list is always terminated by an implicit deny statement for everything.

   `access-list` *`access-list-number`* `{deny | permit}` *`source`* `[`*`source-wildcard`*`]`

5. Return to privileged EXEC mode.

   `end`

6. Verify your entries.

   `show running-config`

7. (Optional) Save your entries in the configuration file.

   `copy running-config startup-config`

To disable access for an SNMP community, set the community string for that community to the null string (don't enter a value for the community string). To remove a specific community string, use the `no snmp-server community` string global configuration command.

This example shows how to assign the strings `open` and `ieee` to SNMP, to allow read-write access for both, and to specify that open is the community string for queries on non-IEEE802dot11-MIB objects and `ieee` is the community string for queries on IEEE802dot11-mib objects:

```
ap(config)# snmp-server view dot11view ieee802dot11
included
ap(config)# snmp-server community open rw
ap(config)# snmp-server community ieee view
ieee802dot11 rw
```

Specify SNMP-Server Group Names

To configure a new SNMP group, or a table that maps SNMP users to SNMP views, use the following command in global configuration mode:

Configures a new SNMP group, or a table that maps SNMP users to SNMP views.

```
snmp-server group [groupname  {v1 | v2c | v3 [auth |
noauth | priv]}][read readview] [write writeview]
[notify notifyview] [access  access-list]
```

Configure SNMP-Server Hosts

To configure the recipient of an SNMP trap operation, use the following command in global configuration mode:

```
snmp-server host host [traps | informs][version {1
| 2c | 3 [auth | noauth | priv]} ] community-string
[udp-port port] [notification-type]
```

Configure SNMP-Server Users

To configure a new user to an SNMP group, use the following command in global configuration mode:

```
snmp-server user username [groupname remote ip-
address

[udp-port port] {v1 | v2c | v3 [encrypted] [auth
{md5 | sha}  auth-password [priv des56 priv
password]] [access access-list]
```

Configure Trap Managers and Enabling Traps

A trap manager is a management station that receives and processes traps. Traps are system alerts that the access point generates when certain events occur. By default, no trap manager is defined, and no traps are issued.

Access points running this Cisco IOS release can have an unlimited number of trap managers. Community strings can be any length.

This table describes the supported access point traps (notification types). You can enable any or all of these traps and configure a trap manager to receive them.

Table 112 - Supported Access Point Traps

Notification Type	Description
authenticate-fail	Enable traps for authentication failures.
config	Enable traps for SNMP configuration changes.
deauthenticate	Enable traps for client device deauthentications.
disassociate	Enable traps for client device disassociations.
dot11-qos	Enable traps for QoS changes.
entity	Enable traps for SNMP entity changes.
rogue-ap	Enable traps for rogue access point detections.
snmp	Enable traps for SNMP events.
switch-over	Enable traps for switch-overs.
syslog	Enable syslog traps.
wlan-wep	Enable WEP traps.

Some notification types cannot be controlled with the `snmp-server enable` global configuration command, such as `udp-port`. These notification types are always enabled. You can use the `snmp-server host` global configuration command to a specific host to receive the notification types listed in Table 112 on page 460.

Beginning in privileged EXEC mode, follow these steps to configure the access point to send traps to a host.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Specify the recipient of the trap message.

- For `host-addr`, specify the name or address of the host (the targeted recipient).
- Specify traps (the default) to send SNMP traps to the host. Specify informs to send SNMP informs to the host.
- Specify the SNMP version to support. Version 1, the default, is not available with informs. Version 3 has three security levels:
  - `auth`—Specifies authentication of packets without encryption
  - `noauth`—Specifies no authentication and no encryption for packets
  - `priv`—Specifies authentication and encryption for packets
- For community-string, specify the string to send with the notification operation. Though you can set this string by using the snmp-server host command, We recommend that you define this string by using the snmp-server community command before using the `snmp-server host` command.
- For notification-type, use the keywords listed in Table 112 on page 460.

```
snmp-server host host-addr {traps | informs}
{version {1 | 2c | 3 {auth | noauth | priv}}}
community-string [udp-port port]
notification-type
```

3. Enable the access point to send specific traps.

   For a list of traps, see Table 112 on page 460.

   To enable multiple types of traps, you must issue a separate `snmp-server enable traps` command for each trap type.

   ```
   snmp-server enable traps notification-types
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. Verify your entries.

   ```
   show running-config
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

   To remove the specified host from receiving traps, use the `no snmp-server host` host global configuration command. To disable a specific trap type, use the `no snmp-server enable traps` notification-types global configuration command.

Set the Agent Contact and Location Information

Beginning in privileged EXEC mode, follow these steps to set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Set the system contact string.

   For example:

   ```
   snmp-server contact Dial System Operator at beeper
   21555.
   ```

3. Set the system location string.

   For example:

   ```
   snmp-server location Building 3/Room 222
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. Verify your entries.

   ```
   show running-config
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

`snmp-server view` Command

In global configuration mode, use the `snmp-server view` command to access Standard IEEE 802.11 MIB objects through IEEE view and the dot11 read-write community string.

This example shows how to enable IEEE view and dot11 read-write community string:

```
AP(config)# snmp-server view ieee ieee802dot11
included

AP(config)# snmp-server community dot11 view ieee
RW
```

SNMP Examples

This example shows how to enable SNMPv1, SNMPv2C, and SNMPv3. The configuration permits any SNMP manager to access all objects with read-only permissions by using the community string public. This configuration does not cause the access point to send any traps.

```
AP(config)# snmp-server community public
```

This example shows how to assign the strings open and ieee to SNMP, to allow read-write access for both, and to specify that open is the community string for queries on non-IEEE802dot11-MIB objects and ieee is the community string for queries on IEEE802dot11-mib objects:

```
bridge(config)# snmp-server view dot11view
ieee802dot11 included

bridge(config)# snmp-server community open rw

bridge(config)# snmp-server community ieee view
ieee802dot11 rw
```

This example shows how to permit any SNMP manager to access all objects with read-only permission by using the community string public. The access point also sends config traps to the hosts 192.180.1.111 and 192.180.1.33 by using SNMPv1 and to the host 192.180.1.27 by using SNMPv2C. The community string public is sent with the traps.

```
AP(config)# snmp-server community public

AP(config)# snmp-server enable traps config

AP(config)# snmp-server host 192.180.1.27 version
2c public

AP(config)# snmp-server host 192.180.1.111 version
1 public

AP(config)# snmp-server host 192.180.1.33 public
```

This example shows how to allow read-only access for all objects to members of access list 4 that use the comaccess community string. No other SNMP managers have access to any objects. SNMP Authentication Failure traps are sent by SNMPv2C to the host cisco.com by using the community string public.

```
AP(config)# snmp-server community comaccess ro 4
```

```
AP(config)# snmp-server enable traps snmp
authentication
AP(config)# snmp-server host cisco.com version 2c
public
```

This example shows how to send Entity MIB traps to the host cisco.com. The community string is restricted. The first line enables the access point to send Entity MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous `snmp-server host` commands for the host cisco.com.

```
AP(config)# snmp-server enable traps entity
AP(config)# snmp-server host cisco.com restricted
entity
```

This example shows how to enable the access point to send all traps to the host myhost.cisco.com by using the community string public:

```
AP(config)# snmp-server enable traps
AP(config)# snmp-server host myhost.cisco.com
public
```

This example shows how to configure these SNMPv3 settings:

- a view name (iso)
- an SNMP engine ID (1234567890) that this agent uses to identify itself to the remote host at IP address 1.4.74.10
- an SNMPv3 group (admin) that supports privacy encryption, and all users of the group have read and write access to all objects defined in the iso view
- an SNMP user (joe) that belongs to the admin group, uses MD5 authentication for queries, uses xyz123 as a password for MD5, uses DES56 data query encryption, and uses key007 as an encryption key
- an SNMP user (fred) that belongs to the admin group, uses MD5 authentication for queries, uses abc789 as an encrypted password for MD5, uses DES56 data query encryption, and uses key99 as an encryption key

```
AP(config)# snmp-server view iso iso included
AP(config)# snmp-server engineID remote 1.4.74.10
1234567890
AP(config)# snmp-server group admin v3 priv
AP(config)# snmp-server group admin v3 priv read iso
write iso
AP(config)# snmp-server user joe admin v3 auth md5
xyz123 priv des56 key007
AP(config)# snmp-server user fred admin v3 encrypted
auth md5 abc789 priv des56 key99
```

TIP After you enter the last command in this example, the show running-config and show startup-config commands display only a partial SNMP configuration.

Display SNMP Status

To display SNMP input and output statistics, including the number of illegal community string entries, errors, and requested variables, use the `show snmp` privileged EXEC command.

For information about the fields in this display, see the Cisco IOS Configuration Fundamentals Command Reference.

Notes:

Configure Workgroup Bridge Mode, Repeater Mode, and Standby Access Points

This chapter describes how to configure your access point as a workgroup bridge, a repeater, or as a hot standby unit.

Topic	Page
Workgroup Bridge Mode	467
Configuring Workgroup Bridge Mode	472
Use Workgroup Bridges in a Lightweight Environment	474
Repeater Access Points	478
Configure a Repeater Access Point	480
Hot Standby	484
Configure a Hot Standby Access Point by Using CLI	486

Workgroup Bridge Mode

You can configure the Stratix 5100 access point as workgroup bridges. In workgroup bridge mode, the unit associates to another access point as a client and provides a network connection for the devices connected to its Ethernet port.

For example, if you need to provide wireless connectivity for a group of network printers, you can connect the printers to a hub or to a switch, connect the hub or switch to the access point Ethernet port, and configure the access point as a workgroup bridge. The workgroup bridge associates to an access point on your network.

If your access point has two radios, either the 2.4 GHz radio or the 5 GHz radio can function in workgroup bridge mode. When you configure one radio interface as a workgroup bridge, the other radio interface remains up.

IMPORTANT An access point in workgroup bridge mode can introduce a bridge loop if you connect its Ethernet port to your wired LAN. To avoid a bridge loop on your network, disconnect the workgroup bridge from your wired LAN before or soon after you configure it as a workgroup bridge.

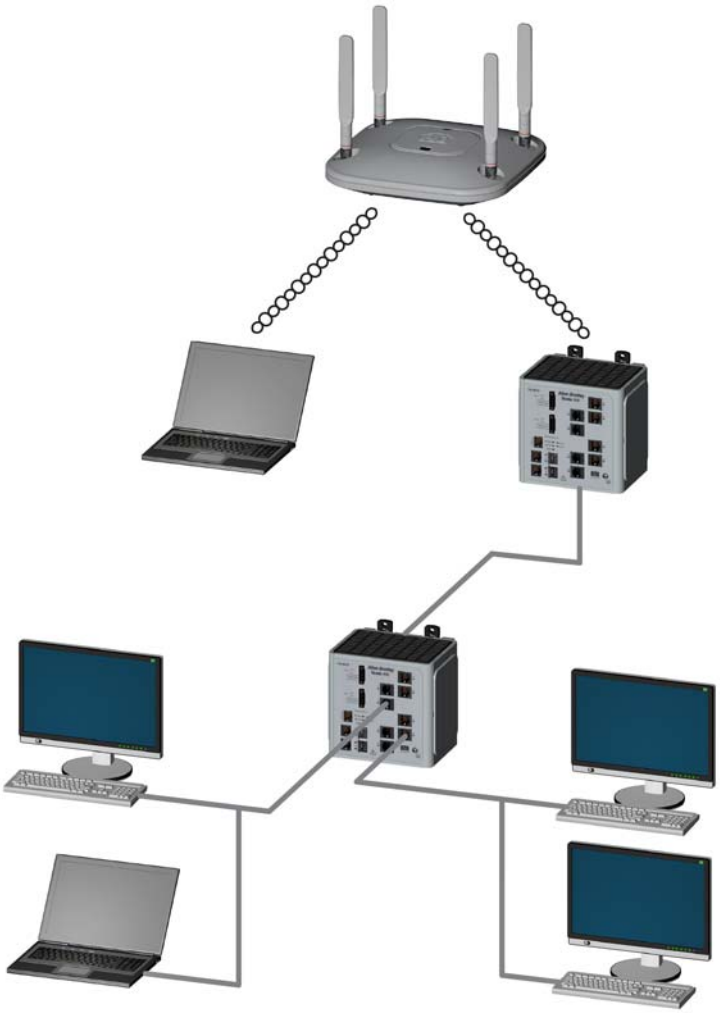
If multiple BSSIDs are configured on a root access point that is designated as the parent of a workgroup bridge, the parent MAC address can change if a BSSID on the parent is added or deleted. If you use multiple BSSIDs on your wireless LAN and a workgroup bridge on your wireless LAN is configured to associate to a specific parent, check the association status of the workgroup bridge when you

add or delete BSSIDs on the parent access point. If necessary, reconfigure the workgroup bridge to use the BSSID's new MAC address.

Although it functions as a bridge, an access point in workgroup bridge mode has a limited radio range. Workgroup bridges don't support the distance setting, that enables you to configure wireless bridges to communicate across several kilometers.

This figure shows an access point in workgroup bridge mode.

Figure 110 - Access Point in Workgroup Bridge Mode



Treat Workgroup Bridges as Infrastructure Devices or as Client Devices

The access point that a workgroup bridge associates can treat the workgroup bridge as an infrastructure device or as a simple client device. By default, access points and bridges treat workgroup bridges as client devices.

For increased reliability, you can configure access points and bridges to treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. Treating a workgroup bridge as an infrastructure device means that the access point reliably delivers multicast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge. You use the infrastructure-client configuration interface command to configure access points and bridges to treat workgroup bridges as infrastructure devices.

Configuring access points and bridges to treat a workgroup bridge as a client device allows more workgroup bridges to associate to the same access point, or to associate by using an SSID that is not an infrastructure SSID. The performance cost of reliable multicast delivery—duplication of each multicast packet sent to each workgroup bridge—limits the number of infrastructure devices, including workgroup bridges, that can associate to an access point or bridge.

To increase beyond 20 the number of workgroup bridges that can associate to the access point, the access point must reduce the delivery reliability of multicast packets to workgroup bridges. With reduced reliability, the access point cannot confirm whether multicast packets reach the intended workgroup bridge, so workgroup bridges at the edge of the access point's coverage area can lose IP connectivity.

When you treat workgroup bridges as client devices, you increase performance but reduce reliability. You use the no infrastructure client configuration interface command to configure access points and bridges to treat workgroup bridges as simple client devices. This is the default setting.

Use a workgroup bridge as an infrastructure device if the devices connected to the workgroup bridge require network reliability equivalent to that of an access point or a bridge. Use a workgroup bridge as a client device if these conditions are true:

- More than 20 workgroup bridges associate to the same access point or bridge
- The workgroup bridge associates by using an SSID that is not an infrastructure SSID
- The workgroup bridge is mobile, for example, not in fixed position and may roam between access points

Configure a Workgroup Bridge for Roaming

If your workgroup bridge is mobile, you can configure it to scan for a better radio connection to a parent access point or bridge. Use this command to configure the workgroup bridge as a mobile station:

```
ap(config)# mobile station
```

When you enable this setting, the workgroup bridge scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. By using these criteria, a workgroup bridge configured as a mobile station searches for a new parent association and roams to a new parent before it loses its current association. When the mobile station setting is disabled (the default setting) the workgroup bridge does not search for a new association until it loses its current association.

Configure a Workgroup Bridge for Limited Channel Scanning

In mobile environments such as railroads, a workgroup bridge instead of scanning all the channels is restricted to scan only a set of limited channels to reduce the hand-off delay when the workgroup bridge roams from one access point to another. By limiting the number of channels the workgroup bridge scans only to those required, the mobile workgroup bridge achieves and maintains a continuous wireless LAN connection with fast and smooth roaming.

Configure the Limited Channel Set

This limited channel set is configured by using the mobile station scan `<set of channels>` command to invoke scanning to all or specified channels. There is no limitation on the maximum number of channels that can be configured. The maximum number of channels that can be configured is restricted only by the number of channels a radio can support. When executed, the workgroup bridge scans only this limited channel set. This limited channel feature also affects the known channel list that the workgroup bridge receives from the associated access point. Channels are added only to the known channel list if they are also a part of the limited channel set.

The following example shows how the command is used. In the example, channels 1, 6, and 11 are specified to scan:

```
ap#
ap#confure terminal
Enter configuration commands, one per line.End with
CNTL/Z.
ap(config)#int d0
ap(config-if)#ssid limited_scan
ap(config-if)#station-role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station scan 1 6 11
```

```
ap(config-if)#end
ap#
```

Use the `no mobile station scan` command to restore scanning to all the channels.

Ignore the CCX Neighbor List

In addition, the workgroup bridge updates its known channel list by using CCX reports such as the AP Adjacent report or Enhanced Neighbor List report. However, when a workgroup bridge is configured for limited channel scanning, it does not need to process the CCX reports to update its known channel list.

Use the mobile station ignore neighbor-list command to disable processing of CCX neighbor list reports. This command is effective if the workgroup bridge is configured only for limited scanning channel scanning. The following example shows how this command is used

```
ap#
ap#confure terminal
Enter configuration commands, one per line.  End
with CNTL/Z.
ap(config)#int d0
ap(config-if)#mobile station ignore neighbor-list
ap(config-if)#end
```

Workgroup Bridge VLAN Tagging

The Workgroup-Bridge (WGB) VLAN tagging feature enables segregation of VLAN traffic based on the VLAN numbers for Unified WGB solution.

When this feature is enabled, the WGB removes the 802.1q header while sending the packet from a VLAN client to the wireless LAN controller (WLC). WGB gets the packet to a VLAN client without 802.1q header and WGB code has to be modified to add the 802.1q header while forwarding the frame to the switch behind WGB.

WGB updates the WLC with the wired-client VLAN information in the Internet Access Point Protocol (IAPP) Association message. WLC treats the WGB client as a VLAN-client and forwards the packet in the right VLAN interface based on the source-mac-address.

In the upstream direction, WGB removes the 802.1q header from the packet while sending to the WLC. In the downstream direction while forwarding the packet to the switch connecting the wired-client, the WLC sends the packet to WGB without the 802.1q tag and WGB adds a 4-byte 802.1q header based on the destination mac-address.

For detailed information on VLANs, see Configure Virtual Local Area Networks (VLAN) on page 403.

```
WGB(config)#workgroup-bridge unified-vlan-client
```

Configuring Workgroup Bridge Mode

Beginning in privileged EXEC mode, follow these steps to configure an access point as a workgroup bridge.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.

   ```
   interface dot11radio {0 | 1}
   ```

3. Set the radio role to workgroup bridge. If your access point contains two radios, the radio not set to workgroup bridge mode is automatically disabled.

   ```
   station-role workgroup-bridge
   ```

4. Create the SSID that the workgroup bridge uses to associate to a parent access point or bridge.

   ```
   ssid ssid-string
   ```

5. (Optional) If the parent access point is configured to require EAP authentication, configure the credentials profile that the workgroup bridge uses when it performs EAP authentication.

The username and password in the credentials profile must match the username and password that you set up for the workgroup bridge on the authentication server.

```
dot1x credentials profile-name
```

6. Exit SSID configuration mode and return to radio interface configuration mode.

   ```
   exit
   ```

7. (Optional) Enter the MAC address for the access point that needs to be associated to the workgroup bridge.
   - (Optional) You can enter MAC addresses for up to four parent access points. The workgroup bridge attempts to associate to MAC address 1 first; if that access point does not respond, the workgroup bridge tries the next access point in its parent list. If multiple BSSIDs are configured on the parent access point, the MAC address for the parent can change if a BSSID on the parent is added or deleted.
   - (Optional) You can also enter a timeout value in seconds that determines how long the workgroup bridge attempts to associate to a parent access point before trying the next parent in the list. Enter a timeout value from 0... 65535 seconds.

   ```
   parent {1-4} mac-address [timeout]
   ```

8. Exit radio configuration mode and return to global configuration mode.

   ```
   exit
   ```

9. (Optional) Configure the workgroup bridge as a mobile station. When you enable this setting, the workgroup bridge scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. When this setting is disabled (the default setting) the workgroup bridge does not search for a new association until it loses its current association.

   ```
   mobile station
   ```

10. Return to privileged EXEC mode.

    ```
    end
    ```

11. (Optional) Save your entries in the configuration file.

    ```
    copy running-config startup-config
    ```

This example shows how to configure an access point as a workgroup bridge. In this example, the workgroup bridge uses the configured credentials profile EAP-profile to perform EAP authentication.

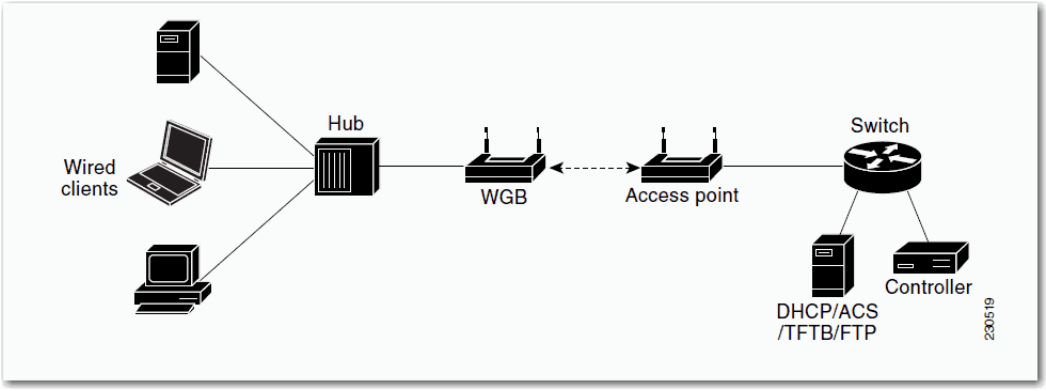
```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# station-role workgroup-bridge
AP(config-if)# ssid infra
AP(config-if)# exit
AP(config)# dot11 ssid infra
AP(config-ssid)# dot1x credentials EAP-profile
AP(config-ssid)# exit
AP(config-if)# exit
AP(config)# end
```

Use Workgroup Bridges in a Lightweight Environment

You can configure an access point to operate as a workgroup bridge so that it can provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the workgroup bridge access point. A workgroup bridge connects to a wired network over a single wireless segment by learning the MAC address of its wired clients on the Ethernet interface and reporting them to the lightweight access point by using Internet Access Point Protocol (IAPP) messaging.

The workgroup bridge provides wireless access connectivity to wired clients by establishing a single connection to the lightweight access point. The lightweight access point treats the workgroup bridge as a wireless clients.

Figure 111 - Workgroup Bridge in a Lightweight Environment



If the lightweight access point fails, the workgroup bridge attempts to associate to another access point.

Guidelines for Using Workgroup Bridges in a Lightweight Environment

Follow these guidelines for using workgroup bridges on your lightweight network.

- The workgroup bridge can be any autonomous access point that supports the workgroup bridge mode and is running Cisco IOS Release JA or greater (on 32-MB access points).

  TIP If your access point has two radios, you can configure only one for workgroup bridge mode. This radio is used to connect to the lightweight access point. We recommend that you disable the second radio.

Perform one of the following to enable the workgroup bridge mode on the workgroup bridge:

- On the workgroup bridge access point GUI, choose Workgroup Bridge for the role in radio network on the Settings > Network Interfaces page.
- On the workgroup bridge access point CLI, enter this command: `station-role workgroup-bridge`
- Only workgroup bridge in client mode (default value) are supported. Those in infrastructure mode are not supported. Perform one of the following to enable client mode on the workgroup bridge:
- On the workgroup bridge access point GUI, choose Disabled for the Reliable Multicast to workgroup bridge parameter.
- On the workgroup bridge access point CLI, enter this command: `no infrastructure client`.

  TIP Multiple VLANs and trunking are not supported for use with workgroup bridges.

- These lightweight features are supported for use with a workgroup bridge:
  - Guest N+1 redundancy
  - Local EAP
- These lightweight features are not supported for use with a workgroup bridge:
  - Idle timeout
  - Web authentication

  TIP If a workgroup bridge associates to a web-authentication WLAN, the workgroup bridge is added to the exclusion list, and all of the workgroup bridge wired clients are deleted.

- In a mesh network, a workgroup bridge can associate to any lightweight mesh access point, regardless of whether it acts as a root access point or a mesh access point.

- Wired clients connected to the workgroup bridge are not authenticated for security. Instead, the workgroup bridge is authenticated against the access point to which it associates. Therefore, We recommend that you physically secure the wired side of the workgroup bridge.
- With Layer 3 roaming, if you plug a wired client into the workgroup bridge network after the workgroup bridge has roamed to another controller (for example, to a foreign controller), the wired client's IP address appears only on the anchor controller, not on the foreign controller.
- When you delete a workgroup bridge record from the controller, all of the workgroup bridge wired clients' records are also deleted.
- Wired clients connected to a workgroup bridge inherit the workgroup bridge's QoS and AAA override attributes.
- These features are not supported for wired clients connected to a workgroup bridge:
  - MAC filtering
  - Link tests
  - Idle timeout
- You don't need to configure anything on the controller to enable the workgroup bridge to communicate with the lightweight access point. However, to ensure proper communication, create a WLAN on the controller that matches the SSID and security method that was configured on the workgroup bridge.

Sample Workgroup Bridge Configuration

Here is a sample configuration of a workgroup bridge access point by using WPA2-PSK with pre-shared key.

```
ap#confure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
ap(config) #dot11 ssid WGB-PSK
ap(config-ssid) #authentication open
ap(config-ssid) #authentication key-management wpa
version 2
ap(config-ssid) #wpa-psk ascii presharedkey
ap(config-ssid) #exit
ap(config) #interface dot11Radio 1
ap(config-if) #encryption mode ciphers aes-ccm
ap(config-if) #ssid WGB-PSK
ap(config-if) #station-role workgroup-bridge
ap(config-if) #end
```

To verify that the workgroup bridge is associated to an access point, enter this command on the workgroup bridge:

```
show dot11 association
```

If a wired client does not send traffic for an extended period of time, the workgroup bridge 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 workgroup bridge to a large value. Accomplish this by using the following IOS commands on the workgroup bridge:

```
configure terminal
bridge bridge-group-number aging-time seconds
exit
end
```

where bridge-group-number is a value between 1...255, and seconds is a value between 10...1,000,000 seconds. We recommend configuring the seconds parameter to a value greater than the wired client's idle period.

Repeater Access Points

A repeater access point is not connected to the wired LAN; it is placed within radio range of an access point connected to the wired LAN to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. You can configure either the 2.4 GHz radio or the 5 GHz radio as a repeater. In access points with two radios, only one radio can be a repeater; the other radio must be configured as a root radio.

The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. When you configure an access point as a repeater, the access point's Ethernet port does not forward traffic.

You can set up a chain of several repeater access points, but throughput for client devices at the end of the repeater chain is low. Because each repeater must receive and then re-transmit each packet on the same channel, throughput is cut in half for each repeater you add to the chain.

A repeater access point associates to the access point that has the best connectivity. However, you can specify the access point that the repeater associates with. Setting up a static, specific association between a repeater and a root access point improves repeater performance.

To set up repeaters, you must enable Aironet extensions on both the parent (root) access point and the repeater access points. Aironet extensions are enabled by default. This improve the access point's ability to understand the capabilities of Cisco Aironet client devices associated with the access point. Disabling Aironet extensions sometimes improves the interoperability between the access point and non-Cisco client devices. Non-Cisco client devices can have difficulty communicating with repeater access points and the root access point to which repeaters are associated.

The infrastructure SSID must be assigned to the native VLAN. If more than one VLAN is created on an access point or wireless bridge, an infrastructure SSID cannot be assigned to a non-native VLAN. The following message appears when the infrastructure SSID is configured on non-native VLAN:

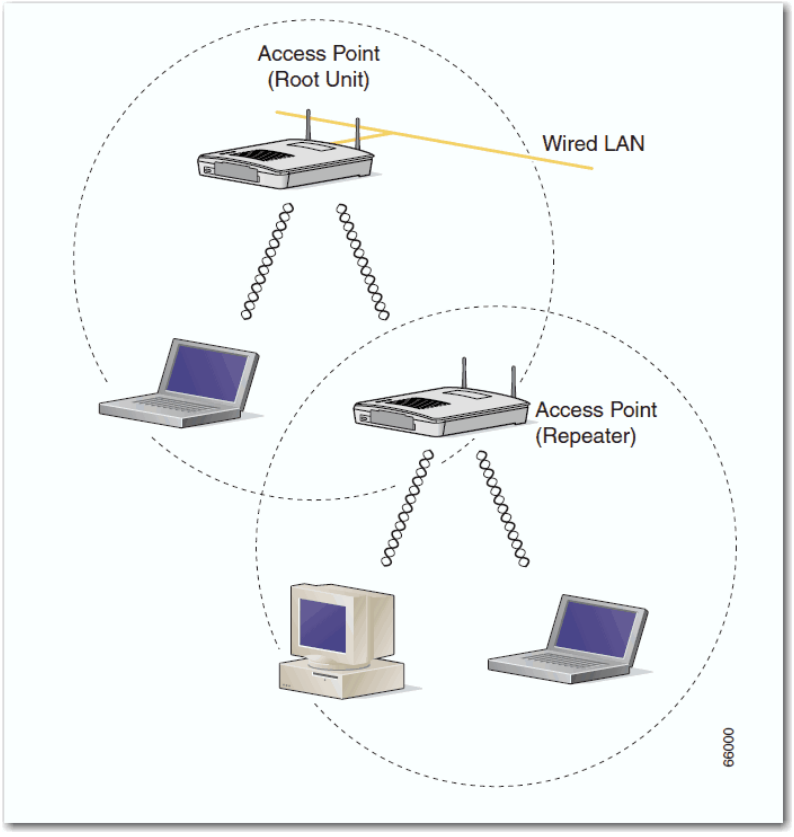
```
SSID [xxx] must be configured as native-vlan before
enabling infrastructure-ssid
```

TIP Because access points create a virtual interface for each radio interface, repeater access points associate to the root access point twice: once for the actual interface and once for the virtual interface.

You cannot configure multiple VLANs on repeater access points. Repeater access points support only the native VLAN.

This figure shows an access point acting as a repeater.

Figure 112 - Access Point as a Repeater



Configure a Repeater Access Point

This section provides instructions for setting up an access point as a repeater.

Default Configuration

Access points are configured as root units by default. This table shows the default values for settings that control the access point's role in the wireless LAN.

Feature	Default Setting
Station role	Root
Parent	none
Extensions	Aironet

Guidelines for Repeaters

Follow these guidelines when configuring repeater access points:

- Use repeaters to serve client devices that don't require high throughput. Repeaters extend the coverage area of your wireless LAN, but they drastically reduce throughput.
- Use repeaters when most if not all client devices that associate with the repeaters are Cisco Aironet clients. Non-Cisco client devices sometimes have trouble communicating with repeater access points.
- Make sure that the data rates configured on the repeater access point match the data rates on the parent access point. For instructions on configuring data rates, see Configure Radio Data Rates on page 256.
- Repeater access points support only the native VLAN. You cannot configure multiple VLANs on a repeater access point.

TIP Repeater access points running Cisco IOS software cannot associate to parent access points that don't run Cisco IOS software.

Repeater access points don't support wireless domain services (WDS). Don't configure a repeater access point as a WDS candidate, and don't configure a WDS access point to fall back to repeater mode in case of Ethernet failure.

If multiple BSSIDs are configured on a root access point that is designated as the parent of a repeater, the parent MAC address can change if a BSSID on the parent is added or deleted. If you use multiple BSSIDs on your wireless LAN and a repeater on your wireless LAN is configured to associate to a specific parent, check the association status of the repeater when you add or delete BSSIDs on the parent access point. If necessary, reconfigure the disassociated device to use the BSSID's new MAC address.

Set Up a Repeater

Beginning in Privileged Exec mode, follow these steps to configure an access point as a repeater.

1. Enter the global configuration mode.

   ```
   configure terminal
   ```

2. Enter interface configuration mode for the radio interface.
   - The 2.4 GHz 802.11n radio is 0.
   - The 5 GHz 802.11n radio is 1.

   ```
   interface dot11radio { 0 | 1 }
   ```

3. Create the SSID that the repeater uses to associate to a root access point; in the next step designate this SSID as an infrastructure SSID. If you created an infrastructure SSID on the root access point, create the same SSID on the repeater, also.

   ```
   ssid ssid-string
   ```

4. Designate the SSID as an infrastructure SSID. The repeater uses this SSID to associate to the root access point. Infrastructure devices must associate to the repeater access point by using this SSID unless you also enter the optional keyword.

   The infrastructure SSID must be assigned to the native VLAN. If more than one VLAN is created on an access point or wireless bridge, an infrastructure SSID cannot be assigned to a non-native VLAN. The following message appears when the infrastructure SSID is configured on non-native VLAN:

   SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid

   ```
   infrastructure-ssid [optional]
   ```

5. Exit SSID configuration mode and return to radio interface configuration mode.

   ```
   exit
   ```

6. Set the access point's role in the wireless LAN to repeater.

   ```
   station-role repeater
   ```

7. If Aironet extensions are disabled, enable Aironet extensions.

   ```
   dot11 extensions aironet
   ```

8. (Optional) Enter the MAC address for the access point to which the repeater should associate.

   You can enter MAC addresses for up to four parent access points. The repeater attempts to associate to MAC address 1 first; if that access point does not respond, the repeater tries the next access point in its parent list.

   If multiple BSSIDs are configured on the parent access point, the MAC address for the parent might change if a BSSID on the parent is added or deleted.

(Optional) You can also enter a timeout value in seconds that determines how long the repeater attempts to associate to a parent access point before trying the next parent in the list. Enter a timeout value from 0 to 65535 seconds.

```
parent {1-4} mac-address [timeout]
```

9. Return to privileged EXEC mode.

```
end
```

10. (Optional) Save your entries in the configuration file.

```
copy running-config startup-config
```

This example shows how to set up a repeater access point with three potential parents:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid chicago
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# exit
AP(config-if)# station-role repeater
AP(config-if)# dot11 extensions aironet
AP(config-if)# parent 1 0987.1234.h345 900
AP(config-if)# parent 2 7809.b123.c345 900
AP(config-if)# parent 3 6543.a456.7421 900
AP(config-if)# end
```

Align Antennas

When an access point is configured as a repeater, you can align its antenna with another remote antenna by using the `dot11 antenna-alignment` command.

The command invokes an alignment test. The radio disassociates from its parent, probes adjacent wireless devices, and records the MAC addresses and signal strengths of responses it receives. After the timeout, the radio reassociates with its parent.

Follow these steps to run an antenna alignment test:

1. Enter privileged EXEC mode.

```
enable
```

2. Enter interface configuration mode for the radio interface.
   - The 2.4 GHz 802.11n radio is 0.
   - The 5 GHz 802.11n radio is 1.

   ```
   dot11 dot11radio { 0 | 1 }
   ```
3. Establish the time in seconds that the antenna alignment test runs before timing out. The default is 5 seconds.

   ```
   antenna-alignment timeout
   ```

   Use the `show dot11 antenna-alignment` command to list the MAC addresses and signal level for the last 10 devices that responded to the probe.

Verify Repeater Operation

After you set up the repeater, check the status indicators on top of the repeater access point. If your repeater is functioning correctly, the status indicators on the repeater and the root access point should be steady blue.

The repeater access point appears as associated with the root access point in the root access point's Association Table.

Set Up a Repeater as a WPA Client

WPA key management uses a combination of encryption methods to protect communication between client devices and the access point. You can set up a repeater access point to authenticate to your network like other WPA-enabled client devices.

Beginning in Privileged Exec mode, follow these steps to set up the repeater as a WPA client.

1. Enter global configuration mode.

   ```
   configure terminal
   ```
2. Enter interface configuration mode for the radio interface.
   - The 2.4 GHz 802.11n radio is 0.
   - The 5 GHz 802.11n radio is 1.

   ```
   interface dot11radio { 0 | 1 }
   ```
3. Create an SSID and enter SSID configuration mode for the new SSID.

   The SSID can consist of up to 32 alphanumeric characters, but do not include spaces. SSIDs are case-sensitive.

   ```
   ssid ssid-string
   ```
4. Enable open authentication for the SSID.

   ```
   authentication open
   ```
5. Enable WPA authenticated key management for the SSID.

   ```
   authentication key-management wpa
   ```

6. Designate the SSID as the SSID that the repeater uses to associate to other access points.

   ```
   infrastructure ssid
   ```

7. Enter a pre-shared key for the repeater.

   Enter the key by using either hexadecimal or ASCII characters. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key. If you use ASCII, you must enter from 8...63 ASCII characters, and the access point expands the key for you.

   ```
   wpa-psk { hex | ascii } [ 0 | 7 ] encryption-key
   ```

8. Return to privileged EXEC mode.

   ```
   end
   ```

9. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Hot Standby

Hot Standby mode designates an access point as a back up for another access point. The standby access point is placed near the access point it monitors, configured exactly the same as the monitored access point. The standby access point associates with the monitored access point as a client and sends IAPP queries to the monitored access point through both the Ethernet and the radio ports. If the monitored access point fails to respond, the standby access point comes online and takes the monitored access point's place in the network.

Except for the IP address, the standby access point's settings can be identical to the settings on the monitored access point. If the monitored access point goes offline and the standby access point takes its place in the network, matching settings insures that client devices can switch easily to the standby access point.

The standby access point monitors another access point in a device-to-device relationship, not in an interface-to-interface relationship. For example, you cannot configure the standby access point's 5 GHz radio to monitor the 5 GHz radio in access point alpha and the standby's 2.4 GHz radio to monitor the 2.4 GHz radio in access point bravo. You also cannot configure one radio in a dual-radio access point as a standby radio and configure the other radio to serve client devices.

TIP Hot standby mode is disabled by default.

If the monitored access point malfunctions and the standby access point takes its place, repeat the hot standby setup on the standby access point when you repair or replace the monitored access point. The standby access point does not revert to standby mode automatically.

The MAC address of the monitored access point can change if a BSSID on the monitored unit is added or deleted. If you use multiple BSSIDs on your wireless LAN, check the status of the standby unit when you add or delete BSSIDs on the

monitored access point. If necessary, reconfigure the standby unit to use the BSSID's new MAC address.

Configure Hot Standby

When you set up the standby access point, you must enter the MAC address of the access point that the standby unit monitors. Record the MAC address of the monitored access point before you configure the standby access point.

The standby access point must duplicate several key settings on the monitored access point. These settings are:

- Primary SSID (as well as additional SSIDs configured on the monitored access point)
- Default IP Subnet Mask
- Default Gateway
- Data rates
- Encryption settings
- Authentication types and authentication servers

If the monitored access point goes offline and the standby access point takes its place in the network, matching settings ensures that client devices can switch easily to the standby access point. Check the monitored access point and record these settings before you set up the standby access point.

TIP Wireless client devices associated to the standby access point lose their connections during the hot standby setup process.

Configure a Hot Standby Access Point by Using CLI

When you set up the standby access point, you must enter the MAC address of the access point that the standby unit monitors. Record the MAC address of the monitored access point before you configure the standby access point.

The standby access point also must duplicate several key settings on the monitored access point. These settings are:

- Primary SSID (as well as additional SSIDs configured on the monitored access point)
- Default IP Subnet Mask
- Default Gateway
- Data rates
- WEP settings
- Authentication types and authentication servers

Check the monitored access point and record these settings before you set up the standby access point.

IMPORTANT Wireless client devices associated to the standby access point lose their connections during the hot standby setup process.

TIP To quickly duplicate the monitored access point's settings on the standby access point, save the monitored access point configuration and load it on the standby access point.

Beginning in Privileged Exec mode, follow these steps to enable hot standby mode on an access point.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Puts the access point into standby mode and specifies the MAC address of radio on the monitored access point.

   When you configure an access point with two radios to monitor a another access point with two radios, you must enter the MAC addresses of both the monitored 2.4 GHz and 5 GHz radios. Enter the 2.4 GHz radio MAC address first, followed by the 5 GHz radio MAC address.

   The MAC address of the monitored access point can change if a BSSID on the monitored unit is added or deleted. If you use multiple BSSIDs on your wireless LAN, check the status of the standby unit when you add or delete BSSIDs on the monitored access point. If necessary, reconfigure the standby unit to use the BSSID's new MAC address.

   ```
   iapp standby mac-address
   ```

3. Enter interface configuration mode for the radio interface.
   - The 2.4 GHz 802.11n radio is 0.
   - The 5 GHz 802.11n radio is 1.

   ```
   interface dot11radio { 0 | 1 }
   ```

4. Create the SSID that the standby access point uses to associate to the monitored access point; in the next step designate this SSID as an infrastructure SSID. If you created an infrastructure SSID on the monitored access point, create the same SSID on the standby access point, also.

   ```
   ssid ssid-string
   ```

5. Designate the SSID as an infrastructure SSID. The standby uses this SSID to associate to the monitored access point. If the standby access point takes the place of the monitored access point, infrastructure devices must associate to the standby access point by using this SSID unless you also enter the optional keyword.

   ```
   infrastructure-ssid [optional]
   ```

6. If the monitored access point is configured to require LEAP authentication, configure the username and password that the standby access point uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the standby access point on the authentication server.

   ```
   authentication client username username
   password password
   ```

7. Exit SSID configuration mode and return to radio interface configuration mode.

   ```
   exit
   ```

8. Sets the number of seconds between queries that the standby access point sends to the monitored access point's radio and Ethernet ports. The default poll frequency is 2 seconds.

   ```
   iapp standby poll-frequency seconds
   ```

9. Sets the number of seconds the standby access point waits for a response from the monitored access point before it assumes that the monitored access point has malfunctioned. The default timeout is 20 seconds.

   Increase the standby timeout setting if the bridged path between the standby and monitored access points can be lost for periods greater than 20 seconds (during spanning tree recalculation, for example).

   If the monitored access point is configured to select the least congested radio channel, you can increase the standby timeout setting. The monitored unit can take up to 40 seconds to select the least congested channel.

   ```
   iapp standby timeout seconds
   ```

10. (Optional) Configures the standby access point to send a Dumb Device Protocol (DDP) message to the monitored access point to disable the radios of the monitored access point when the standby unit becomes active. This feature prevents client devices that are associated to the monitored access point from remaining associated to the malfunctioning unit.

    ```
    iapp standby primary-shutdown
    ```

11. Verify your entries.
    - If the access point is in standby mode, the standby parameters appear, including the MAC address of the monitored access point, poll-frequency, and timeout values.
    - If the access point is not in standby mode, `no iapp standby mac-address` message appears.

    ```
    show iapp standby-parms
    ```
12. Return to privileged EXEC mode.

    ```
    end
    ```
13. (Optional) Save your entries in the configuration file.

    ```
    copy running-config startup-config
    ```

After you enable standby mode, configure the settings that you recorded from the monitored access point to match on the standby access point.

Verify Standby Operation

Use this command to check the status of the standby access point:

```
show iapp standby-status
```

This command provides the status of the standby access point. This table lists the standby status messages that can appear.

Table 113 - Standby Status Messages

Message	Description
IAPP Standby is Disabled	The access point is not configured for standby mode.
IAPP—AP is in standby mode	The access point is in standby mode.
IAPP—AP is operating in active mode	The standby access point has taken over for the monitored access point and is functioning as a root access point.
IAPP—AP is operating in repeater mode	The standby access point has taken over for the monitored access point and is functioning as a repeater access point.
Standby status: Initializing	The standby access point is initializing link tests with the monitored access point.
Standby status: Takeover	The standby access point has transitioned to active mode.
Standby status: Stopped	Standby mode has been stopped by a configuration command.
Standby status: Ethernet Linktest Failed	An Ethernet link test failed from the standby access point to the monitored access point.
Standby status: Radio Linktest Failed	A radio link test failed from the standby access point to the monitored access point.
Standby status: Standby Error	An undefined error occurred.
Standby State: Init	The standby access point is initializing link tests with the monitored access point.
Standby State: Running	The standby access point is operating in standby mode and is running link tests to the monitored access point.
Standby State: Stopped	Standby mode has been stopped by a configuration command.
Standby State: Not Running	The access point is not in standby mode.

Use this command to check the standby configuration:

```
show iapp standby-parms
```

This command provides the MAC address of the standby access point, the standby timeout, and the poll-frequency values. If no standby access point is configured, this message appears:

```
no iapp standby mac-address
```

If a standby access point takes over for the monitored access point, you can use the show iapp statistics command to help determine the reason that the standby access point took over.

Notes:

Configure System Message Logging

This chapter describes how to configure system message logging on your access point.

Topic	Page
System Message Logging	491
Configure System Message Logging	492
Display the Logging Configuration	504
Default System Message Logging Configuration	493
Disable and Enable Message Logging	493
Set the Message Display Destination Device	495
Enable and Disable Timestamps on Log Messages	496
Enable and Disable Sequence Numbers in Log Messages	497
Define the Message Severity Level	498
Limit Syslog Messages Sent to the History Table and to SNMP	500
Set a Logging Rate Limit	501
Configure UNIX Syslog Servers	502

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Security Command Reference for Release 12.3.

System Message Logging

By default, access points send the output from system messages and `debug privileged EXEC` commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console.

TIP The syslog format is compatible with 4.3 BSD UNIX.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages are displayed on the console after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the console and each of the destinations. You can timestamp log messages or set the syslog source address to enhance real-time debugging and management.

You can access logged system messages by using the access point command-line interface (CLI) or by saving them to a properly configured syslog server. The access point software saves syslog messages in an internal buffer. You can remotely monitor system messages by accessing the access point through Telnet or by viewing the logs on a syslog server.

Configure System Message Logging

This section describes how to configure system message logging. System log messages can contain up to 80 characters and a percent sign (%), that follows the optional sequence number or timestamp information, if configured. Messages are displayed in this format:

```
seq no:timestamp: %facility-severity-
MNEMONIC:description
```

The part of the message preceding the percent sign depends on the setting of the global configuration command:

```
service sequence-numbers, service timestamps log
datetime, service timestamps log datetime
[localtime] [msec] [show-timezone], or service
timestamps log uptime
```

This table describes the elements of `syslog` messages.

Table 114 - System Log Message Elements

Element	Description
seq no	Stamps log messages with a sequence number `only if the service sequence-numbers` global configuration command is configured. For more information, see Enable and Disable Sequence Numbers in Log Messages on page 497.

timestamp formats:
`mm/dd hh:mm:ss`
or
`hh:mm:ss (short uptime)`
or
`d h (long uptime)`
	Date and time of the message or event. This information appears only if the `service timestamps log [datetime | log]` global configuration command is configured.
	For more information, see the Enable and Disable Timestamps on Log Messages on page 496.

facility	The facility that the message refers to, for example, `SNMP, SYS`. A facility can be a hardware device, a protocol, or a module of the system software. It denotes the source or the cause of the system message.
severity	Single-digit code from 0…7 that is the severity of the message. For a description of the severity levels, see Table 116 on page 499.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

This example shows a partial access point system message:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1,
changed state to up

00:00:47: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up

00:00:47: %LINK-3-UPDOWN: Interface
GigabitEthernet0/2, changed state to up

00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Vlan1, changed state to down

00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/1, changed state to down
2

*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from
console by vty2 (10.34.195.36)

18:47:02: %SYS-5-CONFIG_I: Configured from console
by vty2 (10.34.195.36)

*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I:
Configured from console by vty2 (10.34.195.36)
```

Default System Message Logging Configuration

This table shows the default system message logging configuration.

Table 115 - Default System Message Logging Configuration

Feature	Default Setting
System message logging to the console	Enabled
Console severity	Debugging (and numerically lower levels; see Table 116 on page 499)
Logging buffer size	4096 bytes
Logging history size	1 message
Timestamps	Disabled
Synchronous logging	Disabled
Logging server	Disabled
Syslog server IP address	None configured
Server facility	Local7 (see Table 117 on page 504)
Server severity	Informational (and numerically lower levels; see Table 116 on page 499)

Disable and Enable Message Logging

Message logging is enabled by default. It must be enabled to send messages to any destination other than the console. When enabled, log messages are sent to a logging process, that logs messages to designated locations asynchronously to the processes that generated the messages.

Beginning in privileged EXEC mode, follow these steps to disable message logging.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Disable message logging.

   ```
   no logging on
   ```

3. Return to privileged EXEC mode.

   ```
   end
   ```

4. Verify your entries.

   ```
   show running-config
   ```

   or

   ```
   show logging
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Disabling the logging process can slow down the access point because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages are displayed on the console as soon as they are produced, often appearing in the middle of command output.

The `logging synchronous` global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press Return. For more information, see Enable and Disable Timestamps on Log Messages on page 496.

To re-enable message logging after it has been disabled, use the `logging on` global configuration command.

Set the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console. Beginning in privileged EXEC mode, use one or more of the following commands to specify the locations that receive messages.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

   Log messages to an internal buffer. The default buffer size is 4096. The range is 4096...2147483647 bytes. Levels include emergencies 0, alerts 1, critical 2, errors 3, warnings 4, notifications 5, informational 6, and debugging 7.

   TIP Don't make the buffer size too large because the access point could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the access point; however, this value is the maximum available, do not set the buffer size to this amount.

   ```
   logging buffered [size] [level]
   ```

2. Log messages to a UNIX syslog server host.

   For `host`, specify the name or IP address of the host to be used as the syslog server.

   To build a list of syslog servers that receive logging messages, enter this command more than once.

   For complete syslog server configuration steps, see the Configure UNIX Syslog Servers on page 502.

   ```
   logging host
   ```

3. Return to privileged EXEC mode.

   ```
   end
   ```

4. Log messages to a non-console terminal during the current session.

   Terminal parameter-setting commands are set locally and don't remain in effect after the session has ended. You must perform this step for each session to see the debugging messages.

   ```
   terminal monitor
   ```

5. Verify your entries.

   ```
   show running-config
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

The `logging buffered` global configuration command copies logging messages to an internal buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full.

- To display the messages that are logged in the buffer, use the `show logging` privileged EXEC command. The first message displayed is the oldest message in the buffer.
- To clear the contents of the buffer, use the `clear logging` privileged EXEC command.
- To disable logging to the console, use the `no logging console` global configuration command.
- To disable logging to a file, use the `no logging file [severity-level-number | type]` global configuration command.

Enable and Disable Timestamps on Log Messages

By default, log messages are not timestamped.

Beginning in privileged EXEC mode, follow these steps to enable timestamping of log messages.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable log timestamps.

   The first command enables timestamps on log messages, showing the time since the system was restarted.

   The second command enables timestamps on log messages. Depending on the options selected, the timestamp can include the date, time in milliseconds relative to the local time zone, and the time zone name.

   ```
   service timestamps log uptime
   ```

   or

   ```
   service timestamps log datetime [msec] [localtime] [show-timezone]
   ```

3. Return to privileged EXEC mode.

   ```
   end
   ```

4. Verify your entries.

   ```
   show running-config
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

- To disable timestamps for both debug and log messages, use the `no service timestamps` global configuration command.
- This example shows part of a logging display with the `service timestamps log datetime` global configuration command enabled:

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from
console by vty2 (10.34.195.36)
```

- This example shows part of a logging display with the `service timestamps log uptime` global configuration command enabled:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1,
changed state to up
```

Enable and Disable Sequence Numbers in Log Messages

Because there is a chance that more than one log message can have the same timestamp, you can display messages with sequence numbers so that you can unambiguously refer to a single message. By default, sequence numbers in log messages are not displayed.

Beginning in privileged EXEC mode, follow these steps to enable sequence numbers in log messages.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable sequence numbers.

   ```
   service sequence-numbers
   ```

3. Return to privileged EXEC mode.

   ```
   end
   ```

4. Verify your entries.

   ```
   show running-config
   ```

5. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

- To disable sequence numbers, use the `no service sequence-numbers` global configuration command.
- This example shows part of a logging display with sequence numbers enabled:

```
000019: %SYS-5-CONFIG_I: Configured from console by
vty2 (10.34.195.36)
```

Define the Message Severity Level

You can limit messages displayed to the selected device by specifying the severity level of the message, that are described in Table 116 on page 499. Specifying a level causes messages at that level and numerically lower levels to be displayed at the destination.

Beginning in privileged EXEC mode, follow these steps to define the message severity level.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Limit messages logged to the console.

   By default, the console receives debugging messages and numerically lower levels (see Table 116 on page 499).

   ```
   logging console level
   ```

3. Limit messages logged to the terminal lines.

   By default, the terminal receives debugging messages and numerically lower levels (see Table 116 on page 499).

   ```
   logging monitor level
   ```

4. Limit messages logged to the syslog servers.

   By default, syslog servers receive informational messages and numerically lower levels (see Table 116 on page 499).

   For complete syslog server configuration steps, see Configure UNIX Syslog Servers on page 502.

   ```
   logging trap level
   ```

5. Return to privileged EXEC mode.

   ```
   end
   ```

6. Verify your entries.

   ```
   show running-config
   ```

   or

   ```
   show logging
   ```

7. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

- To disable logging to the console, use the `no logging console` global configuration command.

- To disable logging to a terminal other than the console, use the `no logging monitor` global configuration command.
- To disable logging to syslog servers, use the `no logging trap` global configuration command.

This table describes the *level* keywords. It lists also the corresponding UNIX syslog definitions from the most severe level to the least severe level.

Table 116 - Message Logging Level Keywords

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

The software generates four other categories of messages:

- Error messages about software or hardware malfunctions, displayed at levels warnings through emergencies. These types of messages mean that the functionality of the access point is affected.
- Output from the `debug` commands, displayed at the debugging level. Debug commands are typically used only by the Technical Assistance Center (TAC).
- Interface up or down transitions and system restart messages, displayed at the notifications level. This message is only for information; access point functionality is not affected.
- Reload requests and low-process stack messages, displayed at the informational level. This message is for information only; access point functionality is not affected.

TIP Authentication request log messages are not logged on to a syslog server. This feature is not supported on Cisco Aironet access points.

Limit Syslog Messages Sent to the History Table and to SNMP

If you have enabled syslog message traps to be sent to an SNMP network management station by using the `snmp-server enable trap` global configuration command, you can change the level of messages sent and stored in the access point history table. You can also change the number of messages that are stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level `warning` and numerically lower levels (see Table 116 on page 499) are stored in the history table even if syslog traps are not enabled.

Beginning in privileged EXEC mode, follow these steps to change the level and history table size defaults.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Change the default level of `syslog` messages stored in the history file and sent to the SNMP server.

   See Table 116 on page 499 for a list of level keywords.

   By default, warnings, errors, critical, alerts, and emergencies messages are sent.

   ```
   logging history level
   ```

   Specify the number of `syslog` messages that can be stored in the history table. The default is to store one message. The range is 1...500 messages.

   ```
   logging history size number
   ```

3. Specify the number of syslog messages that can be stored in the history table.

   The default is to store one message. The range is 1 ...500 messages.

   ```
   logging history size number
   ```

4. Return to privileged EXEC mode.

   ```
   end
   ```

5. Verify your entries.

   ```
   show running-config
   ```

6. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

When the history table is full (it contains the maximum number of message entries specified with the `logging history size` global configuration command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

To return the logging of syslog messages to the default level, use the `no logging history` global configuration command. To return the number of messages in the history table to the default value, use the `no logging history size` global configuration command.

Set a Logging Rate Limit

You can enable a limit on the number of messages that the access point logs per second. You can enable the limit for all messages or for messages sent to the console, and you can specify that messages of a specific severity are exempt from the limit. To disable the rate limit, use the `no logging rate-limit` global configuration command.

Beginning in privileged EXEC mode, follow these steps to enable a logging rate limit.

1. Enter global configuration mode.

   ```
   configure terminal
   ```

2. Enable a logging rate limit in seconds.
   - (Optional) Apply the limit to all logging or to messages logged only to the console.
   - (Optional) Exempt a specific severity from the limit.

   ```
   logging rate-limit seconds
   [all | console]
   [except severity]
   ```

3. Return to privileged EXEC mode.

   ```
   end
   ```

4. (Optional) Save your entries in the configuration file.

   ```
   copy running-config startup-config
   ```

Configure UNIX Syslog Servers

The next sections describe how to configure the 4.3 BSD UNIX server syslog daemon and define the UNIX system logging facility.

Log Messages to a UNIX Syslog Daemon

Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server. Log in as root, and perform these steps.

TIP Some recent versions of UNIX syslog daemons no longer accept by default syslog packets from the network. If this is the case with your system, use the UNIX man syslogd command to determine what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

1. Add a line such as the following to the file /etc/syslog.conf:

   ```
   local7.debug /usr/adm/logs/cisco.log
   ```

   The `local7` keyword specifies the logging facility to be used; see Table 117 on page 504 for information on the facilities. The `debug` keyword specifies the syslog level; see Table 116 on page 499 for information on the severity levels. The syslog daemon sends messages at this level or at a more severe level to the file specified in the next field. The file must already exist, and the syslog daemon must have permission to write to it.

2. Create the log file by entering these commands at the UNIX shell prompt:

   ```
   $ touch /usr/adm/log/cisco.log
   $ chmod 666 /usr/adm/log/cisco.log
   ```

3. Make sure the syslog daemon reads the new changes by entering this command:

   ```
   $ kill -HUP `cat /etc/syslog.pid`
   ```

For more information, see the `man syslog.conf` and `man syslogd` commands on your UNIX system.

Configure the UNIX System Logging Facility

When sending system log messages to an external device, you can cause the access point to identify its messages as originating from any of the UNIX syslog facilities.

Beginning in privileged EXEC mode, follow these steps to configure UNIX system facility message logging.

1. Enter global configuration mode.

   `configure terminal`

2. Log messages to a UNIX syslog server host by entering its IP address.

   To build a list of syslog servers that receive logging messages, enter this command more than once.

   `logging host`

3. Limit messages logged to the syslog servers.

   Be default, syslog servers receive informational messages and lower.

   `logging trap level`

   See Table 116 on page 499 for level keywords.

4. Configure the syslog facility.

   The default is `local7`.

   `logging facility facility-type`

   See Table 117 on page 504 for facility-type keywords.

5. Return to privileged EXEC mode.

   `end`

6. Verify your entries.

   `show running-config`

7. (Optional) Save your entries in the configuration file.

   `copy running-config startup-config`

- To remove a syslog server, use the `no logging host global` configuration command, and specify the syslog server IP address.
- To disable logging to syslog servers, enter the `no logging trap` global configuration command.

This table lists the 4.3 BSD UNIX system facilities supported by the Cisco IOS software. For more information about these facilities, consult the operator's manual for your UNIX operating system.

Table 117 - Logging Facility-Type Keywords

Facility Type Keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-7	Locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Display the Logging Configuration

To display the current logging configuration and the contents of the log buffer, use the `show logging` privileged EXEC command.

For information about the fields in this display, see publication Cisco IOS Configuration Fundamentals Command Reference and the Cisco IOS IP and IP Routing Command Reference.

To display the logging history file, use the `show logging history` privileged EXEC command.

Troubleshoot

This chapter provides troubleshooting procedures for basic problems with the wireless access point/workgroup bridge.

For the most up-to-date and compressive troubleshooting information, see the Cisco TAC website at the following URL (select Top Issues and then select Wireless Technologies): http://www.cisco.com/tac

Topic	Page
Check Basic Settings	505
SSID	505
Pre-shared Keys	506
Security Settings	506
Reset to the Default Configuration	506
Web Browser Interface	507
CLI	513

Check the Status Indicators

If your wireless device is not communicating, check the status indicators on the top of the wireless access point/workgroup bridge.

See Stratix 5100 WAP Status Indicators on page 42 for detailed descriptions.

Check Basic Settings

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the wireless device does not communicate with client devices, check the areas described in this section.

SSID

Wireless clients attempting to associate with the wireless device must use the same SSID as the wireless device. If a client device's SSID does not match the SSID of an wireless device in radio range, the client device does not associate.

Pre-shared Keys

If you configure WPA2 key management with pre-shared keys, the root AP and a client (or a workgroup bridge) need to have the keys configured to the same value.

See Configure Cipher Suites on page 327 for more information.

Security Settings

Wireless clients attempting to authenticate with the wireless device must support the same security options configured in the wireless device, such as EAP or LEAP, MAC address authentication, Message Integrity Check (MIC) and 802.1X protocol versions.

If your radio clients are using EAP-FAST authentication, you must configure open authentication with EAP. If you don't configure open authentication with EAP, a warning message appears. If you are using CLI, the following warning appears:

> SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP can also be configured.

If you are using the GUI, this warning message appears:

> WARNING:
> Network EAP is used only for LEAP authentication. If radio clients are configured to authenticate by using EAP-FAST, Open Authentication with EAP can also be configured."

If a wireless client is unable to authenticate with the wireless device, contact the system administrator for proper security settings in the client adapter and for the client adapter driver and firmware versions that are compatible with the wireless device settings.

TIP The wireless device MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the wireless device radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Reset to the Default Configuration

If you forget the password that lets you to configure the wireless device, you need to completely reset the configuration.

IMPORTANT The following steps reset **all** configuration settings to factory defaults, including passwords, security settings, the IP address, and the SSID. The default username is `a blank field' and the password is `wirelessap'. It is case sensitive.

MODE Button

Follow these steps to delete the current configuration and return all access point settings to the factory defaults by using the MODE button.

1. Disconnect power (the power jack for external power or the Ethernet cable for inline power) from the access point.
2. Press and hold the MODE button while you reconnect power to the access point.
3. Hold the MODE button until the status indicator turns red (approximately 20...30 seconds), and release the button.
4. After the access point restarts, you must reconfigure the access point by using the Web-browser interface or CLI.

TIP The access point is configured with the factory default values including the IP address that is set to receive an IP address by using DHCP. The default username is blank and password are wirelessap, that is case-sensitive.

Web Browser Interface

Follow these steps to delete the current configuration and return all wireless device settings to the factory defaults by using the web browser interface.

1. Open your Internet browser. You must use Microsoft Internet Explorer (version 6.x or later) or Netscape Navigator (version 7.x or later).
2. Enter the wireless device's IP address in the browser address line and press Enter.

   An Enter Network Password screen appears.
3. Enter your username in the User Name field.
4. Enter the wireless device password in the Password field and press Enter.

   The Summary Status page appears.
5. Click System Software.

   The System Software screen appears.
6. Click System Configuration.

   The System Configuration screen appears.
7. Click the Reset to Defaults or Reset to Defaults (Except IP).
8. If you want to retain a static IP address, choose Reset to Defaults (Except IP).
9. Click Restart.

   The system restarts.

10. After the wireless device restarts, you must reconfigure the wireless device by using the web browser interface or CLI commands.

    The default username is blank and the password is wirelessap, that is case-sensitive.

Set Factory Defaults by Using CLI

Follow the steps below to delete the current configuration and return all wireless device settings to the factory defaults by using CLI commands.

1. Open CLI by using a Telnet session or a connect to the wireless device by using the console port.
2. Restart the wireless device by removing power and reapplying power.

   Let the wireless device start up until the command prompt appears and the wireless device begins to inflate the image. This can take a minute.

   When you see these lines on CLI, press Esc.

   ```
   Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/
   c350-k9w7-mx.v122_13_ja.20031010"
   ...##################################################
   ############################
   ##################################################
   ############################
   ##################################################
   ############################
   ####################
   ```

3. At the ap: prompt, enter the `flash_init` command to initialize the Flash.

   ```
   ap: flash_init
   Initializing Flash...
   flashfs[0]: 142 files, 6 directories
   flashfs[0]: 0 orphaned files, 0 orphaned
   directories
   flashfs[0]: Total bytes: 7612416
   flashfs[0]: Bytes used: 3407360
   flashfs[0]: Bytes available: 4205056
   flashfs[0]: flashfs fsck took 0 seconds.
   ...done initializing Flash.
   ```

4. Use the `dir flash:` command to display the contents of Flash and find the config.txt configuration file.

   ```
   ap: dir flash:
   ```

```
Directory of flash:/
3 .rwx 223 <date> env_vars
4 .rwx 2190 <date> config.txt
5 .rwx 27 <date> private.config
150 drwx 320 <date> c350.k9w7.mx.122.13.JA
4207616 bytes available (3404800 bytes used)
```

5. Use the `rename` command to change the name of the config.txt file to config.old.

   ```
   ap: rename flash:config.txt flash:config.old
   ```

6. Use the `reset` command to restart the wireless device.

   ```
   ap: reset
   Are you sure you want to reset the system (y/n)?y
   System resetting...
      using  eeprom values
   WRDTR,CLKTR: 0x80000800 0x80000000
   RQDC ,RFDC : 0x80000033 0x000001cb
      ddr init done
   IOS Bootloader - Starting system.
   Xmodem file system is available.
   DDR values used from system serial eeprom.
   WRDTR,CLKTR: 0x80000800, 0x80000000
   RQDC, RFDC : 0x80000033, 0x000001cb
   ```

7. When the access point has finished restarting the software, establish a new Telnet session to the access point.

   The wireless device is configured with factory default values, including the IP address that is set to receive an IP address by using DHCP and the default username (blank) and password (wirelessap).

8. When IOS software is loaded, you can use the `del privileged EXEC` command to delete the config.old file from Flash.

   ```
   ap# del flash:config.old
   Delete filename [config.old]
   Delete flash:config.old [confirm]
   ap#
   ```

Reload the Access Point Image

If the wireless device has a firmware failure, you must reload the image file by using the web browser interface or by pressing and holding the MODE button for around 30 seconds. You can use the browser interface if the wireless device firmware is still fully operational and you want to upgrade the firmware image. However, you can use the MODE button when the access point has a corrupt firmware image. In this case, you must reload the image file by using CLI through a Telnet or console port connection.

HTTP Interface

You can also use the Web browser interface to reload the wireless device image file. The Web browser interface supports loading the image file by using HTTP or TFTP interfaces.

TIP Your wireless device configuration does not change when you use the browser to reload the image file.

The HTTP interface enables you to browse to the wireless device image file on your computer and download the image to the wireless device. Follow the instructions below to use the HTTP interface.

1. Open your Internet browser.

   You must use Microsoft Internet Explorer (version 6.x or later) or Netscape Navigator (version 7.x).

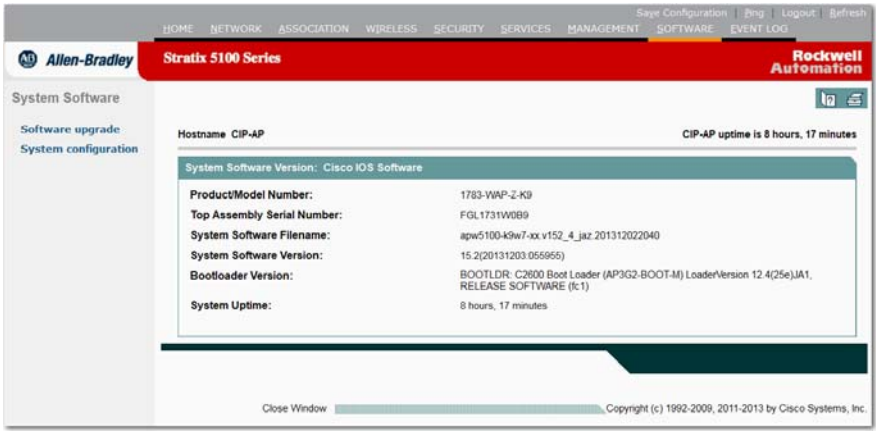
2. Enter the wireless device's IP address in the browser address line and press Enter.

   An Enter Network Password screen appears.

3. Enter your username, password and press Enter.

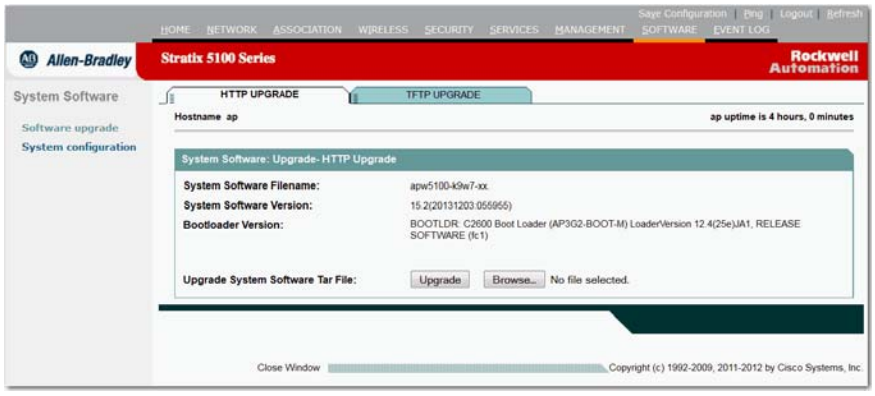
4. Click the System Software tab.

   The Summary Status page appears.



5. Click Software Upgrade.

   The HTTP Upgrade screen appears.



6. Browse to the image file on your PC.
7. Click Upload.

TFTP Interface

The TFTP interface allows you to use a TFTP server on a network device to load the wireless device image file. Follow the instructions below to use a TFTP server.

1. Open your Internet browser.

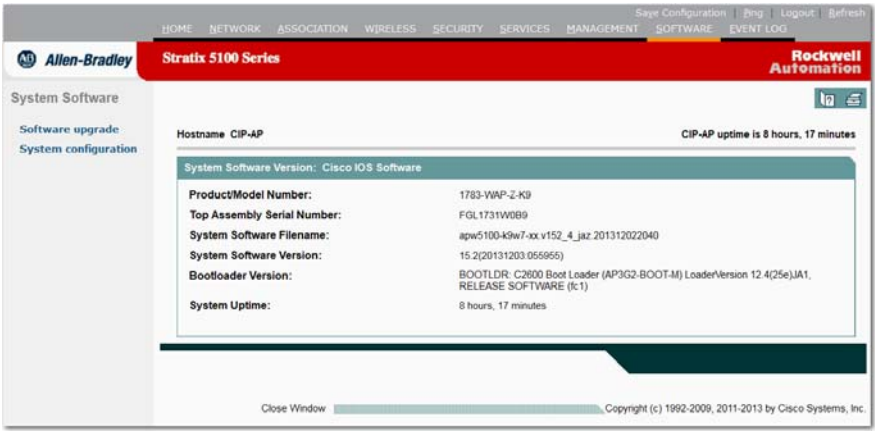
   You must use Microsoft Internet Explorer (version 6.x or later) or Netscape Navigator (version 7.x).

2. Enter the wireless device's IP address in the browser address line and press Enter.

   An Enter Network Password screen appears.

3. Enter your username, password and press Enter.

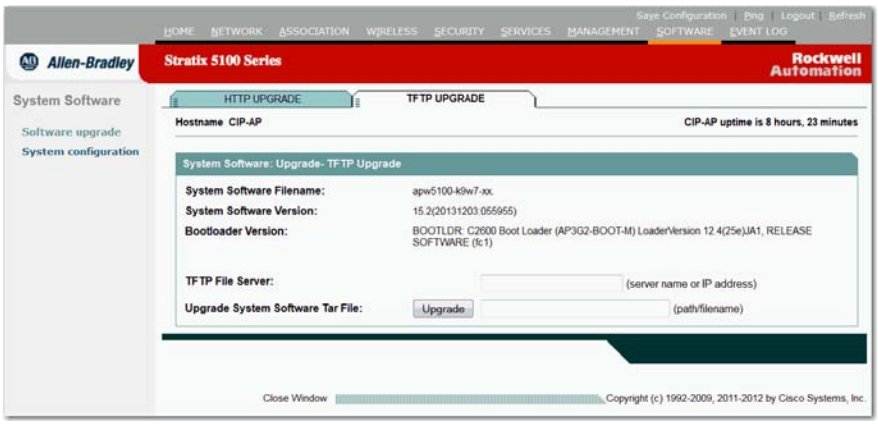
4. Click the System Software tab.



5. Click Software Upgrade.

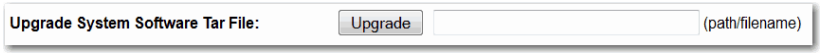
   The HTTP Upgrade screen appears.

6. Click the TFTP Upgrade tab.



7. Enter the IP address for the TFTP server in the TFTP Server field.

8. Enter the file name for the image file in the Upload New System Image Tar File field.



   - If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename.
   - If the file is located in the TFTP root directory, enter only the filename.

9. Click Upload.

CLI

Follow the steps below to reload the wireless device image by using CLI commands. When the wireless device begins to start, you interrupt the start-up process and use boot loader commands to load an image from a TFTP server to replace the image in the access point.

TIP Your wireless device configuration is not changed when using CLI to reload the image file.

1. Start CLI by using a connection to the wireless device console port.
2. Restart the wireless device by removing power and reapplying power.
3. Let the wireless device start until it begins to inflate the image. When you see these lines on CLI, press Esc:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/
c350-k9w7-mx.v122_13_ja.20031010"
...##################################################
##########################
##################################################
##########################
##################################################
##########################
##################
```

4. When the ap: command prompt appears, enter the **set** command to assign an IP address, subnet mask, and default gateway to the wireless device.

TIP You must use upper-case characters when you enter the IP-ADDR, NETMASK, and DEFAULT_ROUTER options with the set command.

Your entries can look like this example:

```
ap: set IP_ADDR 192.168.133.160
ap: set NETMASK 255.255.255.0
ap: set DEFAULT_ROUTER 192.168.133.1
```

5. Enter the `tftp_init` command to prepare the wireless device for TFTP.

```
ap: tftp_init
```

6. Enter the `tar` command to load and inflate the new image from your TFTP server.

   The command must include this information:

- -xtract option, that inflates the image when it is loaded
- IP address of your TFTP server

- Directory on the TFTP server that contains the image
- Name of the image
- Destination for the image (the wireless device Flash)

Your entry can look like this example:

```
ap: tar -xtract tftp://192.168.130.222/images/c350-
k9w7-tar.122-13.JA1.tar flash:
```

When the display becomes full, CLI pauses and `--MORE--` appears.

7. Press the spacebar to continue.

```
extracting info (229 bytes)

c350-k9w7-mx.122-13.JA1/ (directory) 0 (bytes)

c350-k9w7-mx.122-13.JA1/html/ (directory) 0 (bytes)

c350-k9w7-mx.122-13.JA1/html/level1/ (directory) 0
(bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
appsui.js (558 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
back.htm (205 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
cookies.js (5027 bytes).

extracting c350-k9w7-mx.122-13.JA1/html/level1/
forms.js (15704 bytes)...

extracting c350-k9w7-mx.122-13.JA1/html/level1/
sitewide.js (14621 bytes)...

extracting c350-k9w7-mx.122-13.JA1/html/level1/
config.js (2554 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
stylesheet.css (3215 bytes)

c350-k9w7-mx.122-13.JA1/html/level1/images/
(directory) 0 (bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/ap_title_appname.gif (1422 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_1st.gif (1171 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_cbottom.gif (318 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_current.gif (348 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_last.gif (386 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_last_filler.gif (327 bytes)
```

```
extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_last_flat.gif (318 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_button_nth.gif (1177 bytes)

extracting c350-k9w7-mx.122-13.JA1/html/level1/
images/apps_leftnav_dkgreen.gif (869 bytes)

 -- MORE --
```

TIP If you don't press the spacebar to continue, the process eventually times out and the wireless device stops inflating the image.

8. Enter the `set BOOT` command to designate the new image as the image that the wireless device uses when it restarts.

   The wireless device creates a directory for the image that has the same name as the image, and you must include the directory in the command. Your entry can look like this example:

   ```
   ap: set BOOT flash:/c350-k9w7-mx.122-13.JA1/c350-
   k9w7-mx.122-13.JA1
   ```

9. Enter the `set` command to check your bootloader entries.

   ```
   ap: set

   BOOT=flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-
   mx.122-13.JA1

   DEFAULT_ROUTER=192.168.133.1

   IP_ADDR=192.168.133.160

   NETMASK=255.255.255.0
   ```

10. Enter the `boot` command to restart the wireless device.

    When the wireless device restarts, it loads the new image.

    ```
    ap: boot
    ```

Obtain TFTP Server Software

You can download TFTP server software from several websites. We recommend the shareware TFTP utility available at http://tftpd32.jounin.net

Follow the instructions on the website for installing and using the utility.

Notes:

Supported Management Information Bases (MIBs)

This appendix lists the Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) that the access point supports for this software release. The Cisco IOS SNMP agent supports SNMPv1, SNMPv2, and SNMPv3.

Topic	Page
MIB List	517
Access the MIB Files	518

MIB List

- IEEE802dot11-MIB
- Q-BRIDGE-MIB
- P-BRIDGE-MIB
- CISCO-DOT11-LBS-MIB
- CISCO-DOT11-IF-MIB
- CISCO-WLAN-VLAN-MIB
- CISCO-IETF-DOT11-QOS-MIB
- CISCO-IETF-DOT11-QOS-EXT-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-L2-DEV-MONITORING-MIB
- CISCO-DDP-IAPP-MIB
- CISCO-IP-PROTOCOL-FILTER-MIB
- CISCO-SYSLOG-EVENT-EXT-MIB
- CISCO-TBRIDGE-DEV-IF-MIB
- BRIDGE-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-FLASH-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB

- CISCO-SMI-MIB
- CISCO-TC-MIB
- CISCO-SYSLOG-MIB
- CISCO-WDS-INFO-MIB
- ENTITY-MIB
- IF-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-SYSTEM-MIB
- OLD-CISCO-TS-MIB
- RFC1213-MIB
- RFC1398-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPv2-TC

Access the MIB Files

You can access information about MIBs on the Cisco web site.

http://tools.cisco.com/ITDIT/MIBS/servlet/index

Error and Event Messages

This appendix lists the CLI error and event messages.

Topic	Page
Conventions	519
Software Auto Upgrade Messages	520
Association Management Messages	521
Unzip Messages	521
System Log Messages	522
802.11 Subsystem Messages	522
Inter-Access Point Protocol Messages	527
Local Authenticator Messages	527
WDS Messages	528
Mini IOS Messages	529
Access Point/Bridge Messages	529
Cisco Discovery Protocol Messages	529
External Radius Server Error Messages	530
Sensor Messages	530
SNMP Error Messages	531
SSH Error Messages	531

Conventions

System error messages are displayed in the format shown in this table.

Table 118 - Conventions for System Error Messages

Message Component	Description	Example
Error identifier	A string categorizing the error.	STATION-ROLE
Software component	A string identifying the software component of the error.	AUTO_INSTALL
Severity Level	A numerical string indicating the severity of the error.	0-LOG-EMERG—emergency situation, nothing is functional 1-LOG-ALERT—alerts user to a very serious problem 2-LOG-CRIT—warns of a possible serious critical error 3-LOG-ERR—warning of error condition, most features functional; exercise care 4-LOG-WARNING—warning that user can ignore if they prefer 5-LOG-NOTICE—notice that can be of concern to user 6-LOG-INFO—informational (not serious) 7-LOG-DEBUG—debug information (not serious)

Table 118 - Conventions for System Error Messages (Continued)

Message Component	Description	Example
Action Flags	Internal to the code for additional action to display.	0—No action flag MSG-TRACEBACK—includes traceback with message MSG-PROCESS—includes process information with message MSG-CLEAR—indicates condition had cleared MSG-SECURITY—indicates as security message MSG-NOSCAN—suppresses EEM pattern screening
%d	An integer number.	2450
%e	A MAC address.	000b.fcff.b04e
%s	A message string that provides more detail of the error.	"Attempt to protect port 1640 failed."
%x	A hexadecimal number.	0x001

Software Auto Upgrade Messages

This table explains the messages when you are upgrading the software.

Table 119 - Software Auto Upgrade Messages

Message	Explanation	Recommended Action
`SW-AUTO-UPGRADE-2-FATAL_FAILURE: "Attempt to upgrade software failed, software on flash may be deleted. Please copy software into flash.`	Auto upgrade of the software failed. Check to see if the software has been deleted. Copy software into the flash.	Copy software before restarting the unit.
`SW-AUTO-UPGRADE-7-DHCP_CLIENT_FAILURE: "%s": Auto upgrade of the software failed."`	Auto upgrade of the software failed.	Make sure that the DHCP client is running.
`SW-AUTO-UPGRADE-7-DHCP_SERVER_FAILURE: "%s": Auto upgrade of the software failed."`	Auto upgrade of the software failed.	Make sure that the DHCP server is configured correctly.
`SW-AUTO-UPGRADE-7_BOOT_FAILURE: "%s": Auto upgrade of the software failed."`	Auto upgrade of the software failed.	Restart the unit. If the message appears again, copy the error message exactly as it appears and report it to your technical support representative.
`AUTO-INSTALL-4-STATION_ROLE: "%s": The radio is operating in automatic install mode."`	The radio is operating in automatic install mode.	Use the **station-role** configuration interface command to configure the radio for a role other than install mode.
`AUTO-INSTALL-4-IP_ADDRESS_DHCP: "The radio is operating in automatic install mode and has set ip address dhcp."`	The radio is operating in automatic install mode and is configured to receive an IP address through DHCP.	Use the **station-role** configuration interface command to configure the radio for a role other than install mode.
`Error Message: AUTO-INSTALL-6_STATUS: "%s" %s. RSSI=-%d dBm.: "The radio is operating in install mode."`	The radio is operating in automatic install mode.	Use the **station-role** configuration interface command to configure the radio for a role other than install mode.
`AVR_IMAGE_UPDATE-7-UPDATE_COMPLETE: "The AVR "$d" firmware was successfully updated."`	The access point AVR firmware was successfully updated.	No action is required.
`AVR_IMAGE_UPDATE-2-UPDATE_FAILURE: "The AVR "$d" firmware is not current. Update error: "$s"."`	The AVR firmware is not current and the update failed	Copy the error message and report it to your technical support representative.
`AVR_IMAGE_UPDATE-4-UPDATE_SKIPPED: "AVR "$d" update processing was skipped:"$s"."`	AVR update processing was skipped due to an error.	No action is required.
`AVR_IMAGE_UPDATE-4-UPDATE_START: "The system is updating the AVR "$d" firmware. Please wait . . . "`	The system is updating the AVR firmware.	No action is required.

Association Management Messages

This table explains error message that are related to association management.

Table 120 - Association Management Messages

Message	Explanation	Recommended Action
DOT11-3-BADSTATE: "%s %s ->%s."	802.11 association and management uses a table-driven state machine to keep track and transition an association through various states. A state transition occurs when an association receives one of many possible events. When this error occurs, it means that an association received an event that it did not expect while in this state.	The system can continue but can lose the association that generates this error. Copy the message exactly as it appears and report it to your technical service representative.
DOT11-6-ASSOC: "Interface %s, Station %s e% %s KEY_MGMT (%s), MSGDEF_LIMIT_MEDIUM."	The indicated station associated to an access point on the indicated interface.	None.
DOT11-6-ADD: "Interface %s, Station %e associated to parent %e."	The indicated station associated to the parent access point on the indicated interface.	None.
DOT11-6-DISASSOC: Interface %s, Deauthenticating Station %e #s	Station disassociated from the access point.	No action is required.
DOT11-6-ROAMED: "Station %e roamed to %e."	The indicated station roamed to the indicated new access point.	None.
DOT11-4-ENCRYPT_MISMATCH: "Possible encryption key mismatch between interface %s and station %e."	The encryption setting of the indicated interface and indicated station can be mismatched.	Check the encryption configuration of this interface and the failing station to verify that the configurations match.
DOT11-4-DIVER_USED: Interface $s, Mcs rates 8-15 disabled due to only one transmit or recieve antenna enabled	These rates require that at least 2 receive and transmit antennas be enabled.	Copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl Also perform a search of the Bug Toolkit http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl.
DOT11-4-NO_HT: Interface %s, Mcs rates disabled on vlan %d due to %s	The correct configuration was not in use to allow the HT rates to be used.	Copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl. Also perform a search of the Bug Toolkit http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl.
DOT11-4-NO_MBSSID_BACKUP_VLAN: Backup VLANs cannot be configured if MBSSID is not enabled:"$s" not started	To enable backup VLAN, configure the MBSSID mode.	Configure MBSSID on the device.

Unzip Messages

This table explains the error message for Unzip.

Table 121 - Unzip Messages

Message	Explanation	Recommended Action
SOAP-4-UNZIP_OVERFLOW: "Failed to unzip %s, exceeds maximum uncompressed html size."	The HTTP server cannot retrieve a compressed file in response to an HTTP GET request because the file is too large for the buffers used in the uncompression process.	Make sure that the file is a valid HTML page. If it is, you need to copy an uncompressed version of the file into flash memory to retrieve it through HTTP.

System Log Messages

This table explains the system log messages.

Table 122 - System Log Messages

Message	Explanation	Recommended Action
%DOT11-4-LOADING_RADIO: Interface [chars], loading the radio firmware ([chars])	The radio has been stopped to load new firmware.	No action is required.
%LINEPROTO-5-UPDOWN: Line protocol on Interface [chars], changed state to [chars]	The data link level line protocol has changed state.	No action is required.
%SYS-5-RESTART: System restarted --[chars]	A reload or restart was requested.	Notification message only. No action is required.
%SYS-5-CONFIG_I: Configured from [chars] by [chars]	The router configuration has been changed.	This is a notification message only. No action is required.
%LINEPROTO-5-UPDOWN: Line protocol on Interface [chars], changed state to [chars]	The data link level line protocol has changed state on the interface shown.	No action is required.
%SNMP-5-COLDSTART: SNMP agent on host [chars] is undergoing a cold start	The SNMP server completed a coldstart.	Notification message only. No action is required.
%SYS-6-CLOCKUPDATE: System clock has been updated from [chars] to [chars], configured from [chars] by [chars].	The system clock has been modified.	This is an informational message only. No action is required.

802.11 Subsystem Messages

This table explains the subsystem messages.

Table 123 - Subsystem Messages

Message	Explanation	Recommended Action
DOT11-6-FREQ_USED: "Interface %s, frequency %d selected."	After scanning for an unused frequency, the indicated interface selected the displayed frequency.	None.
DOT11-4-NO-VALID_INFRA_SSID: "No infrastructure SSID configured. %s not started."	No infrastructure SSID was configured and the indicated interface was not started.	Add at least one infrastructure SSID to the radio configuration.
DOT11-4-VERSION_UPGRADE: "Interface %d, upgrading radio firmware."	When starting the indicated interface, the access point found the wrong firmware version. The radio is loaded with the required version.	None.
DOT11-2-VERSION_INVALID: "Interface %d, unable to find required radio version %x.%x/ %d/	When trying to upgrade the radio firmware on the indicated interface, the access point recognized that the indicated radio firmware packaged with the Cisco IOS software had the incorrect version.	None.
DOT11-3-RADIO_OVER_TEMPERATURE: "Interface %s Radio over temperature detected."	The radio's internal temperature exceeds maximum limits on the indicated radio interface.	Take steps necessary to reduce the internal temperature. These steps vary based on your specific installation.
DOT11-6-RADIO_TEMPERATURE_NORMAL: "Interface %s radio temperature returned to normal."	The radio's internal temperature has returned to normal limits on the indicated radio interface.	None.
DOT11-3-TX_PWR_OUT_OF_RANGE: "Interface %s Radio transmit power out of range."	The transmitter power level is outside the normal range on the indicated radio interface.	Remove unit from the network and service.
DOT11-3-RADIO_RF_LO: "Interface %s Radio cannot lock RF freq."	The radio phase lock loop (PLL) circuit is unable to lock the correct frequency on the indicated interface.	Remove unit from network and service.
DOT11-3-RADIO_IF_LO: "Interface %s Radio cannot lock IF freq."	The radio intermediate frequency (IF) PLL is unable to lock the correct frequency on the indicated interface.	Remove unit from network and service.
DOT11-6-FREQ_SCAN: "Interface %s Scanning frequencies for %d seconds."	Starting a scan for a least congested frequency on the interface indicated for a the time period indicated.	None.
DOT11-2-NO_CHAN_AVAIL: "Interface %s, no channel available."	No frequency is available, likely because RADAR has been detected within the previous 30 minutes.	None.

Table 123 - Subsystem Messages (Continued)

Message	Explanation	Recommended Action
DOT11-6-CHAN_NOT_AVAIL: "DFS configured frequency %d Mhz unavailable for %d minute(s).	Radar has been detected on the current channel. Dynamic Frequency Selection (DFS) regulations require no transmission for 30 seconds on the channel.	None.
DOT11-6-DFS_SCAN_COMPLETE: "DFS scan complete on frequency %d MHz."	The device has completed its Dynamic Frequency Scan (DFS) frequency scanning process on the displayed frequency.	None.
DOT11-6-DFS_SCAN_START: "DFS: Scanning frequency %d MHz for %d seconds."	The device has begun its DFS scanning process.	None.
DOT11-6-DFS_TRIGGERED: "DFS: triggered on frequency %d MHz."	DFS has detected RADAR signals on the indicated frequency.	None. The channel is placed on the non-occupancy list for 30 minutes and a new channel is selected.
DOT11-4-DFS_STORE_FAIL: "DFS: could not store the frequency statistics."	A failure occurred writing the DFS statistics to flash.	None.
DOT11-4-NO_SSID: "No SSIDs configured, %d not started."	All SSIDs were deleted from the configuration. At least one must be configured for the radio to run.	Configure at least one SSID on the access point.
DOT11-4-NO_SSID_VLAN: "No SSID with VLAN configured. %s not started."	No SSID was configured for a VLAN. The indicated interface was not started.	At least one SSID must be configured per VLAN. Add at least one SSID for the VLAN on the indicated interface.
DOT11-4-NO_MBSSID_VLAN: "No VLANs configured in MBSSID mode. %s not started."	No VLAN configured in MBSSID mode. The indicated interface was not started.	Add at least one SSID with the VLAN on the indicated interface configuration.
DOT11-4-NO_MBSSID_SHR_AUTH: "More than 1 SSID with shared authentication method in non-MBSSID mode % is down".	Not more than 1 SSID can have shared authentication method when MBSSID is not enabled.	Remove Dot11Radio radio interface or change authentication mode for SSID to open configuration.
DOT114-NO_MBSSID_BACKUP_VLAN: "Backup VLANs cannot be configured if MBSSID is not enabled. %s not started.	To enable a backup VLAN, configure the MBSSID mode.	Configure MBSSID on the device.
IF-4-MISPLACED_VLAN_TAG: "Detected a misplaced VLAN tag on source Interface %. Dropping packet.	Received an 802.1Q VLAN tag was detected on the indicated interface that could not be parsed correctly. The received packet was encapsulated or deencapsulated incorrectly.	None
DOT11-2-FW_LOAD_NET: "Interface %s cannot load on boot. Place image in flash root directory and reload."	The radio images cannot be loaded from a network when the access point starts.	Place the image on the root directory of the flash file-system.
DOT11-4-FW_LOAD_DELAYED: "Interface %s, network filesys not ready. Delaying firmware (%s) load."	The network file-system was not running or not ready when trying to upgrade new firmware into the indicated interface. Loading the identified firmware file has been delayed.	Make sure the network is up and ready before attempting to upgrade the new firmware.
DOT11-3-FLASH_UNKNOWN_RADIO: "Interface %s has an unknown radio."	The radio type could not be determined when the user attempted to upgrade new firmware into the indicated interface.	Restart the system and see if the firmware upgrade completes.
DOT11-4-UPLINK_ESTABLISHED: "Interface %s associated to AP %s %e %s.	The indicated repeater has associated to the indicated root access point. Clients can now associate to the indicated repeater and traffic can pass.	None.
DOT11-2-UPLINK_FAILED: "Uplink to parent failed: %s."	The connection to the parent access point failed for the displayed reason. The uplink stops the connection attempts.	Try resetting the uplink interface. Contact Technical Support if the problem persists.
DOT11-4-CANT_ASSOC: "Interface %, cannot associate %s."	The indicated interface device could not associate to an indicated parent access point.	Check the configuration of the parent access point and this unit to make sure there is a match.
DOT11-4-CANT_ASSOC: "Interface Dot11Radio 0, cannot associate."	Parent does not support client MFP. This error message appears on the access point only in workgroup bridge, repeater, or non-root bridge mode and is seen if the WGB, repeater, or non-root is configured with Client MFP SD required (or mandatory) but root Client MFP is disabled.	Check the configuration of the parent access point and this unit to make sure there is a match.

Table 123 - Subsystem Messages (Continued)

Message	Explanation	Recommended Action
DOT11-2-PROCESS_INITIALIZATION_FAILED: "The background process for the radio could not be started: %s)	The initialization process used by the indicated interface failed for some reason, possibly a transient error.	Perform a reload of the access point. If this fails to rectify the problem, perform a power cycle. If this still fails, try downgrading the access point firmware to the previous version.
DOT11-2-RADIO_HW_RESET: "Radio subsystem is undergoing hardware reset to recover from problem."	An unrecoverable error occurred that could not be resolved by a soft reset.	None.
DOT11-2-RESET_RADIO: "Interface %s, Radio %s, Trying hardware reset on radio."	Used a software reset to start a radio that has failed. Trying a hardware reset that resets all radios on the unit.	None.
DOT11-4-MAXRETRIES: "Packet to client %e reached max retries, removing the client."	The maximum packet send retry limit has been reached and the client is being removed. This error message indicates that the access point attempts to poll the client a certain number of times, but does not receive a response. Therefore, the client is removed from the association table. This issue is commonly seen when the client and access point are attempting to communicate in a noisy RF environment.	To resolve this issue, see if a snapshot reveals noise in the radio spectrum by trying to run a carrier busy test on the access point. Attempt to alleviate any unwanted noise. For more information, see the Perform a Carrier Busy Test on page 282. If there are several access points in the same area, they could be overlapping the channel signal or with any other wireless device in the surrounding area. Change the channels under Network Interfaces and select Radio-802.11. There are three non-overlapping channels: 1, 6, and 11.
DOT11-4-RM_INCAPABLE: "Interface %s	Indicated interface does not support the radio management feature.	None.
DOT11-4-RM_INCORRECT_INTERFACE: "Invalid interface, either not existing or non-radio."	A radio management request discovered that the interface either does not exist or is not a radio interface.	None.
DOT11-3-POWERS_INVALID: "Interface %s, no valid power levels available."	The radio driver found no valid power level settings.	Investigate and correct the power source and settings.
DOT11-4-RADIO_INVALID_FREQ: "Operating frequency (%d) invalid - performing a channel scan."	The indicated frequency is invalid for operation. A channel scan is being performed to select a valid frequency.	None.
DOT11-4-RADIO_NO_FREQ: "Interface &s, all frequencies have been blocked, interface not started."	The frequencies set for operation are invalid and a channel scan is being forced to select a valid operating frequency.	None.
DOT11-4-BCN_BURST_NO_MBSSID: "Beacon burst mode is enabled but MBSSID is not enabled, %s is down."	Beacon burst mode can only be enabled when MBSSID is enabled on the indicated interface.	Enable the MBSSID or disable beacon bursting on the indicated interface.
DOT11-4-BCN_BURST_TOO_MANY_DTIMS: "Beacon burst mode is enabled and there are too many different DTIM periods defined. %s is down.	Beacon burst mode can only support up to four unique DTIM values, each with a maximum of four BSSes.	Change the number of unique DTIMs on the SSIDs configured for the interface to a more reasonable set of values.
DOT11-2-RADIO_INITIALIZATION_ERROR: "The radio subsystem could not be initialized (%s)."	A critical error was detected while attempting to initialize the radio subsystem.	Reload the system.
DOT11-4-UPLINK_NO_ID_PWD: "Interface %s, no username/password supplied for uplink authentication."	The user failed to enter a username and/or password.	Enter the username and/or password and try again.
DOT11-5-NO_IE_CFG: "No IEs configured for %s (ssid index %u)."	When attempting to apply a beacon or probe response to the radio, the beacon or probe was undefined on the indicated SSID index.	Check the IE configuration.
DOT11-4-FLASHING_RADIO: "Interface %s, flashing radio firmware (%s)."	The indicated interface radio has been stopped to load the indicated new firmware.	None.
DOT11-4-LOADING_RADIO: "Interface %s, loading the radio firmware (%s)."	The indicated interface radio has been stopped to load new indicated firmware.	None.

Table 123 - Subsystem Messages (Continued)

Message	Explanation	Recommended Action
`DOT11-2-NO_FIRMWARE: "Interface %s, no radio firmware file (%s) was found."`	When trying to upgrade firmware, the file for the radio was not found in the flash file system. Or, the IOS on the access point is corrupt.	The wrong image has been loaded into the unit. Locate the correct image based on the type of radio used. To resolve this issue you can reload the access point with a new Cisco IOS image. Instructions for reloading an image are found in Reload the Access Point Image on page 510. If the IOS on the access point is corrupt, reload the access point image by using the Mode button method. See MODE Button on page 507.
`DOT11-2-BAD_FIRMWARE: "Interface %s, radio firmware file (%s) is invalid."`	When trying to upgrade firmware into the indicated interface the indicated radio firmware file was found to be invalid.	Make sure the correct firmware image file is in the place where the unit expects to find it.
`DOT11-2-RADIO_FAILED: "Interface %s, failed - %s."`	The radio driver on the indicated interface found a severe error and is shutting down for the indicated reason.	None.
`DOT11-4-FLASH_RADIO_DONE: "Interface %s, flashing radio firmware completed."`	The indicated interface radio firmware upgrade is complete, and the radio restarts with the new firmware.	None.
`DOT11-4-UPLINK_LINK_DOWN: "Interface %s, parent lost: %s."`	The connection to the parent access point on the indicated interface was lost for the reason indicated. The unit tries to find a new parent access point.	None.
`DOT11-4-CANT_ASSOC: Cannot associate: $s`	The unit could not establish a connection to a parent access point for the displayed reason.	Verify that the basic configuration settings (SSID, WEP, and others) of the parent access point and this unit match.
`DOT11-4-CLIENT_NOT_FOUND: "Client was not found."`	Client was not found while checking mic.	None.
`DOT11-4-MAXRETRIES: Packet to client [mac] reached max retries, remove the client`	A packet sent to the client has not been successfully delivered many times, and the max retries limit has been reached. The client is deleted from the association table.	None.
`DOT11-4-BRIDGE_LOOP: "Bridge loop detected between WGB %e and device %e."`	The indicated workgroup bridge reported the address of one of its indicated Ethernet clients and the access point already had that address marked as being somewhere else on the network.	Click Refresh on the Associations page on the access point GUI, or enter the `clear dot11 statistics` command on CLI.
`DOT11-4-ANTENNA_INVALID: "Interface %s, current antenna position not supported, radio disabled."`	The Indicated AIR-RM21A radio module does not support the high-gain position for the external antenna (the high-gain position is folded flat against the access point). The access point automatically disables the radio when the antenna is in the high-gain position.	Fold the antenna on the AIR-RM21A radio module so that it is oriented 90° degrees to the body of the access point.
`DOT11-6-ANTENNA_GAIN: "Interface %s, antenna position/gain changed, adjusting transmitter power."`	The antenna gain has changed so the list of allowed power levels must be adjusted.	None.
`DOT11-4-DIVER_USED: "Interface %s Mcs rates 8-15 disabled due to only one transmit or receive antenna enabled."`	The rates listed require at least 2 receive or transmit antennas be enabled.	Install and enable at least 2 receive or transmit antennas on the access point.
`DOT11-3-RF-LOOPBACK_FAILURE: "Interface %s Radio failed to pass RF loopback test."`	Radio loopback test failed for the interface indicated.	None.
`DOT11-3-RF-LOOPBACK_FREQ_FAILURE: "Interface %s failed to pass RF loopback test."`	Radio loopback test failed at a given frequency for the indicated interface.	None.
`DOT11-7-AUTH_FAILED: "Station %e Authentication failed"`	The indicated station failed authentication.	Verify that the user entered the correct username and password, and verify that the authentication server is online.

Table 123 - Subsystem Messages (Continued)

Message	Explanation	Recommended Action
DOT11-7-CCKM_AUTH_FAILED: "Station %e CCKM authentication failed."	The indicated station failed CCKM authentication.	Verify that the topology of the access points configured to use the WDS access point is functional.
DOT11-4-CCMP_REPLAY: "AES-CCMP TSC replay was detected on packet (TSC 0x%11x received from &e)."	AES-CCMP TSC replay was indicated on a frame. A replay of the AES-CCMP TSC in a received packet almost indicates an active attack.	None.
DOT11-4-CKIP_MIC_FAILURE: "CKIP MIC failure was detected on a packet (Digest 0x%x) received from %e)."	CKIP MIC failure was detected on a frame. A failure of the CKIP MIC in a received packet almost indicates an active attack.	None.
DOT11-4-CKIP_REPLAY: "CKIP SEQ replay was detected on a packet (SEQ 0x&x) received from %e."	CKIP SEQ replay was detected on a frame. A replay of the CKIP SEQ in a received packet almost indicates an active attack."	None.
DOT11-4-TKIP_MIC_FAILURE: "Received TKIP Michael MIC failure report from the station %e on the packet (TSC=0x%11x) encrypted and protected by %s key."	TKIP Michael MIC failure was detected from the indicated station on a unicast frame decrypted locally with the indicated pairwise key.	A failure of the Michael MIC in a received packet can indicate an active attack on your network. Search for and remove potential rogue devices from your wireless LAN. This failure can also indicate a misconfigured client or a faulty client.
DOT11-4-TKIP_MIC_FAILURE_REPORT: "Received TKIP Michael MIC failure report from the station %e on the packet (TSC=0x0) encrypted and protected by %s key	The access point received an EAPOL-key from the indicated station notifying the access point that TKIP Michael MIC failed on a packet transmitted by this access point.	None.
DOT11-3-TKIP_MIC_FAILURE_REPEATED: "Two TKIP Michael MIC failures were detected within %s seconds on %s interface. The interface will be put on MIC failure hold state for next %d seconds"	Two TKIP Michael MIC failures were detected within the indicated time on the indicated interface. Because this usually indicates an active attack on your network, the interface is put on hold for the indicated time. During this hold time, stations by using TKIP ciphers are disassociated and cannot reassociate until the hold time ends. At the end of the hold time, the interface operates normally.	MIC failures usually indicate an active attack on your network. Search for and remove potential rogue devices from your wireless LAN. If this is a false alarm and the interface must not be on hold this long, use the `countermeasure tkip hold-time` command to adjust the hold time.
DOT11-4-TKIP_REPLAY: "TKIP TSC replay was detected on a packet (TSC 0x%ssx received from %e)."	TKIP TSC replay was detected on a frame. A replay of the TKIP TSC in a received packet almost indicates an active attack.	None.
DOT11-4-WLAN_RESOURCE_LIMIT: "WLAN limit exceeded on interface %s and network-id %d."	This access point has reached its limit of 16 VLANs or WLANs.	Unconfigure or reduce static VLANS if access point is trying to associate with RADIUS assigned Network-ID turned on.
SOAP-3-WGB_CLIENT_VLAN_SOAP: "Workgroup Bridge Ethernet client VLAN not configured."	No VLAN is configured for client devices attached to the workgroup bridge.	Configure a VLAN to accommodate client devices attached to the workgroup bridge.
DOT11-4-NO_VLAN_NAME: "VLAN name %s from RADIUS server is not configured for station %e."	The VLAN name returned by the RADIUS server must be configured in the access point.	Configure the VLAN name in the access point.
DOT11-4-NO_VLAN_ID: "VLAN id %d from Radius server is not configured for station %e."	The VLAN ID returned by the Radius server must be configured on the access point.	Configure the VLAN ID on the access point.
SOAP-3-ERROR: "Reported on line %d in file %s.%s."	An internal error occurred on the indicated line number in the indicated filename in the controller ASIC.	None.
SOAP_FIPS-2-INIT_FAILURE: "SOAP FIPS initialization failure: %s."	SOAP FIPS initialization failure.	None.
SOAP_FIPS-4-PROC_FAILURE: "SOAP FIPS test failure: %s."	SOAP FIPS test critical failure.	None.
SOAP_FIPS-4-PROC_WARNING: "SOAP FIPS test warning: %s."	SOAP FIPS test non-critical failure.	
SOAP_FIPS-2-SELF_TEST_IOS_FAILURE: "IOS crypto FIPS self test failed at %s."	SOAP FIPS self test on IOS crypto routine failed.	Check IOS image.

Table 123 - Subsystem Messages (Continued)

Message	Explanation	Recommended Action
SOAP_FIPS-2-SELF_TEST_RAD_FAILURE: "RADIO crypto FIPS self test failed at %s on interface %s %d."	SOAP FIPS self test on radio crypto routine failed.	Check radio image.
SOAP_FIPS-2-SELF_TEST_IOS_SUCCESS: "IOS crypto FIPS self test passed."	SOAP FIPS self test passed.	None
SOAP_FIPS-2-SELF_TEST_RAD_SUCCESS: "RADIO crypto FIPS self test passed on interface %s %d."	SOAP FIPS self test passed on a radio interface.	
DOT11-6-MCAST_DISCARD: "%s mode multicast packets are discarded in %s multicast mode."	The access point configured as a workgroup bridge and drops infrastructure mode multicast packets in client mode and drops client mode multicast packets in infrastructure mode.	None

Inter-Access Point Protocol Messages

Table 124 - Inter-Access Point Protocol Messages

Message	Explanation	Recommended Action
DOT11-6-STANDBY_ACTIVE: "Standby to Active, Reason = %s (%d)."	The access point is transitioning from standby mode to active mode for the indicated reason.	None.
DOT11-6-STANDBY_REQUEST: "Hot Standby request to shutdown radios from %e."	The indicated standby access point has requested that this access point shut down its radio interfaces because a failure has been detected on one of this access point's radio interfaces.	None.
DOT11-6-ROGUE_AP: "Rogue AP %e reported. Reason: %s."	A station has reported a potential rogue access point for the indicated reason.	None.

Local Authenticator Messages

Table 125 - Local Authenticator Messages

Message	Explanation	Recommended Action
RADSRV-4-NAS_UNKNOWN: Unknown authenticator: [ip-address]	The local RADIUS server received an authentication request but does not recognize the IP address of the network access server (NAS) that forwarded the request.	Make sure that every access point on your wireless LAN is configured as a NAS on your local RADIUS server.
RADSRV-4-NAS_KEYMIS: NAS shared key mismatch.	The local RADIUS server received an authentication request but the message signature indicates that the shared key text does not match.	Correct the shared key configuration on either the NAS or on the local RADIUS server.
RADSRV-4_BLOCKED: Client blocked due to repeated failed authentications	A user failed authentication the number of times configured to trigger a block, and the account been disabled.	Use the `clear radius local-server user` *`username`* privileged EXEC command to unblock the user, or allow the block on the user to expire by the configured lockout time.
DOT1X-SHIM-6-AUTH_OK: "Interface %s authenticated [%s]."	The 802.1x authentication was successful.	None
DOT1X-SHIM-3-AUTH_FAIL: "Interface %s authentication failed."	The 802.1x authentication failed to the attached device.	Check the configuration of the 802.1x credentials on the client as well as the RADIUS server.

Table 125 - Local Authenticator Messages (Continued)

Message	Explanation	Recommended Action
`DOT1X-SHIM-3-INIT_FAIL: "Unable to init - %s."`	An error occurred during the initialization of the shim layer.	
`DOT1X-SHIM-3-UNSUPPORTED_KM: "Unsupported key management: %X."`	Am error occurred during the initialization of the shim layer. An unsupported key management type was found.	None.
`DPT1X-SHIM-4-PLUMB_KEY_ERR: "Unable to plumb keys - %s."`	An unexpected error occurred when the shim layer tried to plumb the keys.	None.
`DOT1X-SHIM-3-PKT_TX_ERR: "Unable to tx packet -%s."`	An unexpected error occurred when the shim layer tried to transmit the dot1x packet.	None
`DOT1X-SHIM-3-ENCAP_ERR: "Packet encap failed for %e."`	An unexpected error occurred when the shim layer tried to transmit the dot1x packet. The packet encapsulation failed.	None.
`DOT1X-SHIM-3-SUPP_START_FAIL: "Unable to start supplicant on %s."`	An unexpected error occurred when the shim layer tried to start the dot1x suppliant on the indicated interface.	None.
`DOT1X-SHIM=3-NO_UPLINK: "No uplink found for %s."`	While processing a dot1x event or message on a dot11 interface, a situation was encountered where an uplink was expected, but not found.	None.
`Information Group rad_acct: Radius server <ip address> is responding again (previously dead). Error Group acct: No active radius servers found. Id 106`	This message is seen if the `radius-server deadtime 10` command is configured on the access point.This command is configured to set an interval, the access point does not attempt to use servers that don't respond. Thus avoids the time needed to wait for a request to time out before trying the next configured server. A Radius server marked as dead is skipped by additional requests for the duration of the minutes unless all servers are marked dead. Configuring dead time for 10 minutes means that the server cannot be used for 10 minutes.	You can disable this command if you want this log to disappear. Actually this message is not really a major problem, it is just an informational log.

WDS Messages

Table 126 - WDS Messages

Message	Explanation	Recommended Action
`WLCCP-WDS-6-REPEATER_STOP: WLCCP WDS on Repeater unsupported, WDS is disabled.`	Repeater access points don't support WDS.	None.
`WLCCP-WDS-6-PREV_VER_AP: A previous version of AP is detected.`	The WDS device detected a previous version of the access point.	None.
`WLCCP-AP-6-INFRA: WLCCP Infrastructure Authenticated`	The access point successfully authenticated to the WDS device.	None.
`WLCCP-AP-6-STAND_ALONE: Connection lost to WLCCP server, changing to Stand-Alone Mode`	The access point lost its connection to the WDS device and is in Stand-Alone mode.	None.
`WLCCP-AP-6-PREV_VER_WDS: A previous version of WDS is detected`	The access point detected a previous version of WDS.	Check for an unsupported version of WDS on your network.
`WLCCP-AP-6-UNSUP_VER_WDS: An unsupported version of WDS is detected`	The access point detected an unsupported version of WDS.	Check for an unsupported version of WDS on your network.
`WLCCP-NM-3-WNM_LINK_DOWN: Link to WNM is down`	The network manager is not responding to keep-active messages.	Check for a problem with the network manager or with the network path to the network manager.

Table 126 - WDS Messages (Continued)

Message	Explanation	Recommended Action
WLCCP-NM-6-WNM_LINK_UP: Link to WNM is up	The network manager is now responding to keep-active messages.	None.
WLCCP-NM-6-RESET: Resetting WLCCP-NM	A change in the network manager IP address or a temporary out-of-resource state can cause a reset on the WDS network manager subsystem, but operation returns to normal shortly.	None.
WLCCP-WDS-3-RECOVER: "%s	WDS graceful recovery errors.	None.

Mini IOS Messages

Table 127 - Mini IOS Messages

Message	Explanation	Recommended Action
MTS-2-PROTECT_PORT_FAILURE: An attempt to protect port [number] failed	Initialization failed on attempting to protect port.	None.
MTS-2-SET_PW_FAILURE: Error %d enabling secret password.	Initialization failed when the user attempted to enable a secret password.	None
Saving this config to nvram may corrupt any network management or security files stored at the end of nvram. Continue? [no]:	This warning message appears on the access point CLI interface while saving configuration changes through CLI. This is due to insufficient space in flash memory. When a radio crashes, .rcore files are created. These files indicate a firmware or a hardware problem in the radio, although a hardware problem is less likely.	This warning message can be prohibited by removing the rcore files generated in flash memory. The rcore files have a .rcore extension. The files can be deleted because they simply show that the radio went down at some point. The .rcore files can be listed on CLI session and appear similar to this: r15_5705_AB50_A8341F30.rcore

Access Point/Bridge Messages

Table 128 - Access Point/Bridge Messages

Message	Explanation	Recommended Action
APBR-4-SEND_PCKT_FAILED: Failed to Send Packet on port ifDescr (error= errornum)errornum: status error number	HASH(0x2096974)	The access point or bridge failed to send a packet. This condition can be seen if there is external noise or interference.
Check for sources of noise or interference.	APBR-6-DDP_CLNT_RESET: Detected probable reset of hosthost: host MAC address HASH(0x2080f04)	The access point or bridge detects that another infrastructre device has restarted.
If this message appears continuously, reboot the access point.		

Cisco Discovery Protocol Messages

Table 129 - Cisco Discovery Protocol Messages

Message	Explanation	Recommended Action
CDP_PD-2-POWER_LOW: %s - %s %s (%e)	The system is not supplied with sufficient power.	Reconfigure or replace the source of inline power.

External Radius Server Error Messages

Table 130 - External Radius Server Error Messages

Message	Explanation	Recommended Action
`RADUYS:response-authenticator decrypt fail, paklen 32`	This error message means that there is a mismatch in the RADIUS shared key between the RADIUS server and the access point.	Make sure that the shared key used on the RADIUS server and the access point are the same.

Sensor Messages

Table 131 - Sensor Messages

Message	Explanation	Recommended Action
`SENSOR-3-TEMP_CRITICAL: System sensor "d" has exceeded CRITCAL temperature thresholds`	One of the measured environmental test points exceeds the extreme threshold.	Correct the specified condition, or the system can shut itself down as a preventive measure. Enter the `show environment all` command to help determine if this is due to temperature or voltage condition. If this is a critical temperature warning, please verify that the router fans are operating and that the room cooling and air-conditioning are functioning. This condition could cause the system to fail to operate properly.
`SENSOR-3-TEMP_NORMAL: "s" temperature sensor is now normal`	One of the measured environmental test points is under normal operating temperature.	None required.
`SENSOR-3-TEMP_SHUTDOWN: Shuting down the system because of dangerously HIGH temperature at sensor "d".`	One of the measured environmental test points exceeds the operating temperature environment of the router.	Investigate the cause of the high temperature.
`SENSOR-3-TEMP_WARNING: "s" temparature sensor "d" has exceeded WARNING temperature thresholds`	One of the measured environmental test points exceeds the warning threshold.	Closely monitor the condition and correct if possible, by cooling the environment.
`SENSOR-3-VOLT_CRITICAL: System sensor "d" has exceeded CRITCAL voltage thresholds`	One of the measured environmental test points exceeds the extreme voltage threshold.	Correct the specified condition, or the system can shut itself down as a preventive measure. Enter the `show environment all` command to help determine if this is due to voltage condition. This condition could cause the system to fail to operate properly.
`SENSOR-3-VOLT_NORMAL: System sensor "d"("d") is now operating under NORMAL voltage`	One of the measured environmental test points is under normal operating voltage.	None required.
`SENSOR-3-VOLT_WARNING: Voltage monitor "d"("d") has exceeded voltage thresholds`	One of the measured voltage test points indicates that voltage is out of normal range.	Check Power Supplies or contact TAC.

SNMP Error Messages

Table 132 - SNMP Error Messages

Message	Explanation	Recommended Action
SNMP-3-AUTHFAILIPV6: Authentication failure for SNMP request from hostUnrecognized format ‘ %P’	An SNMP request was sent by this host that was not properly authenticated.	Make sure that the community/user name used in the SNMP req has been configured on the router.
SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full	Snmp packet dropped due to input queue full error	Use the `show snmp` command to see the number of packets dropped. Stop any SNMP access to the device until the error condition is recovered.
SNMP-3-INTERRUPT_CALL_ERR: “s” function, cannot be called from interrupt handler	This message indicates that a call has been made to the function from an interrupt handler. This is not permitted because it fails and device restarts down the stack in malloc call.	If this messages recurs, copy it exactly as it appears and report it to your technical support representative.
SNMP-4-NOENGINEIDV6: Remote snmpEngineID for Unrecognized format ‘ %P’ not found when creating user: “s”	An attempt to create a user failed.This is likely because the engine ID of the remote agent (or SNMP manager) was not configured.	Configure the remote snmpEngineID and reconfigure the user. If the problem persists, copy the error message exactly as it appears, and report it to your technical support representative.
SNMP_MGR-3-MISSINGHOSTIPV6: Cannot locate information on SNMP informs host : Unrecognized format ‘ %P’	A table entry for the mentioned SNMP informs destination cannot be found. As a result, inform notifications are not sent to this destination.	Run the `show snmp host` and `show snmp` commands. Copy the error message and output from the show commands exactly as they appear, and report it to your technical support representative. Deleting and adding again the informs destination via the `snmp-server host` configuration command can clear the condition. Otherwise, reloading the system is necessary.

SSH Error Messages

Table 133 - SSH Error Messages

Message	Explanation	Recommended Action
SSH-5-SSH2_CLOSE: SSH2 Session from ”%s” (tty = “%d”) for user ’”%s”’ using crypto cipher ’”%s”’, hmac ’”%s”’ closed	The SSH Session closure information	No action necessary - informational message
SSH-5-SSH2_SESSION: SSH2 Session request from ”%s” (tty = “%d”) using crypto cipher ’”%s”’, hmac ’”%s”’ ”%s”	The SSH session request information	No action necessary - informational message
SSH-5-SSH2_USERAUTH: User ’”%s”’ authentication for SSH2 Session from ”%s” (tty = “%d”) using crypto cipher ’”%s”’, hmac ’”%s”’ ”%s”	The SSH user authentication status information	No action necessary - informational message
SSH-5-SSH_CLOSE: SSH Session from “%s”(tty = “%d”) for user ’”%s”’ using crypto cipher ’”%s”’ closed	The SSH Session closure information	No action necessary - informational message
SSH-5-SSH_SESSION: SSH Session request from ”%s” (tty = “%d”) using crypto cipher ’”%s”’ ”%s”	The SSH session request information	No action necessary - informational message
SSH-5-SSH_USERAUTH: User ’”%s”’ authentication for SSH Session from ”%s” (tty = “%d”) using crypto cipher ’”%s”’ ”%s”	The SSH user authentication status information	No action necessary - informational message

Notes:

The following terms and abbreviations are used throughout this manual. For definitions of terms not listed here, refer to the Allen-Bradley Industrial Automation Glossary, publication AG-7.1.

802.11 The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs operating in the 2.4 GHz band.

802.11a The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 5 GHz frequency band.

802.11b The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5 Mbps and 11 Mbps wireless LANs operating in the 2.4 GHz frequency band.

802.11g The IEEE standard that specifies carrier sense media across control and physical layer specifications for 6, 9, 12, 18, 24, 36, 48, and 54 Mbps LANs operating in the 2.4 GHz frequency band.

802.3af The IEEE standard that specifies a mechanism for Power over Ethernet (PoE). The standard provides the capability to deliver both power and data over standard Ethernet cabling.

access point A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.

ad hoc network A wireless network composed of stations without access points.

antenna gain The gain of an antenna is a measure of the 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.

associated A station is configured for wireless communication with an access point.

backoff time The random length of time that a station waits before sending a packet on the LAN. Backoff time is a multiple of slot time, so a decrease in slot time ultimately decreases the backoff time, that increases throughput.

beacon A wireless LAN packet that signals the availability and presence of the wireless device. Beacon packets are sent by access points and base stations; however, client radio cards send beacons when operating in computer to computer (Ad Hoc) mode.

BOOTP Boot Protocol. A protocol used for the static assignment of IP addresses to devices on the network.

BPSK A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mbps.

broadcast packet A single data message (packet) sent to all addresses on the same subnet.

CCK Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.

CCKM Cisco Centralized Key Management. By using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point.

cell The area of radio range or coverage that the wireless devices can communicate with the base station. The size of the cell depends upon the speed of the transmission, the type of antenna used, and the physical environment, as well as other factors.

client A radio device that uses the services of an wireless access point/workgroup bridge to communicate with other devices on a local area network.

CSMA Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.

data rates The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).

dBi A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain, and the more acute the angle of coverage.

DHCP Dynamic host configuration protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.

dipole A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.

domain name The text name that refers to a grouping of networks or network resources based on organization-type or geography; for example: name.com—commercial; name.edu—educational; name.gov—government; ISPname.net—network provider, for example, an ISP; name.ar—Argentina; name.au—Australia; and so on.

DNS Domain Name System server. A server that translates text names into IP addresses. The server maintains a database of host alphanumeric names and their corresponding IP addresses.

DSSS Direct sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

EAP Extensible Authentication Protocol. An optional IEEE 802.1x security feature ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server.

Ethernet The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to allow computers to share a network and operates at 10, 100, or 1000 Mbps, depending on the physical layer used.

ETSI The European Telecommunication Standardization Institute (ETSI) has developed standards that have been adopted by many European countries as well as many others. Under the ETSI regulations, the power output and EIRP regulations are much different than in the United States.

file server A repository for files so that a local area network can share files, mail, and programs.

firmware Software that is programmed on a memory chip.

gateway A device that connects two otherwise incompatible networks together.

GHz Gigahertz. One billion cycles per second. A unit of measure for frequency.

IEEE Institute of Electrical and Electronic Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.

infrastructure The wired Ethernet network.

IP address The Internet Protocol (IP) address of a station.

IP subnet mask The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway. This number is expressed in a form similar to an IP address; for example: 255.255.255.0.

isotropic An antenna that radiates its signal in a spherical pattern.

MAC Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device, such as an access point or your client adapter.

modulation Any of several techniques for combining user information with a transmitter's carrier signal.

multipath The echoes created as a radio signal bounces off of physical objects.

multicast packet A single data message (packet) sent to multiple addresses.

omni-directional This typically refers to a primarily circular antenna radiation pattern.

Orthogonal Frequency Division Multiplex (OFDM) A modulation technique used by IEEE 802.11a-compliant wireless LANs for transmission at 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

packet A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

PoE Power over Ethernet, describes standardized or ad-hoc systems that pass electrical power on Ethernet cabling. A single cable to pass data and electrical power to devices such as wireless access points. An advantage to using PoE is that you can pass data and power through long cable lengths.

Quadruple Phase Shift Keying A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 2 Mbps.

range A linear measure of the distance that a transmitter can send a signal.

receiver sensitivity A measurement of the weakest signal a receiver can receive and still correctly translate it into data.

RF Radio frequency. A generic term for radio-based technology.

roaming A feature of some Access Points that lets you move through a facility while maintaining an unbroken connection to the LAN.

RP-TNC A connector type unique to Cisco Aironet radios and antennas. Part 15.203 of the FCC rules covering spread spectrum devices limits the types of antennas that can be used with transmission equipment. In compliance with this rule, Cisco Aironet, like all other wireless LAN providers, equips its radios and antennas with a unique connector to prevent attachment of non-approved antennas to radios.

slot time The amount of time a device waits after a collision before retransmitting a packet. Short slot times decrease the backoff time, that increases throughput.

spread spectrum A radio transmission technology that spreads the user information over a much wider bandwidth than otherwise required to gain benefits such as improved interference tolerance and unlicensed operation.

SSID Service Set Identifier (also referred to as Radio Network Name). A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

transmit power The power level of radio transmission.

UNII Unlicensed National Information Infrastructure—regulations for UNII devices operating in the 5.15...5.35 GHz and 5.725...5.825 GHz frequency bands.

UNII-1 Regulations for UNII devices operating in the 5.15...5.25 GHz frequency band.

UNII-2 Regulations for UNII devices operating in the 5.25...5.35 GHz frequency band.

UNII-3 Regulations for UNII devices operating in the 5.725...5.825 GHz frequency band.

unicast packet A single data message (packet) sent to a specific IP address.

WDS Wireless Domain Services (WDS). An access point providing WDS on your wireless LAN maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the WDS access point forwards the client's credentials to the new access point with the multicast key. Only two packets pass between the client and the new access point, greatly shortening the reassociation time.

WEP Wired Equivalent Privacy. An optional security mechanism defined within the 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable.

workstation A computing device with an installed client adapter.

WPA Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and can be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.

Notes:

Numerics

2.4 GHz 184
5 GHz 184
802.11e 416
802.11i 273
802.11n channel width 264
802.11n guard interval 270
802.1H 274
802.1x authentication 303
802.1X Supplicant
configuring 206
creating a credentials profile 208
creating and applying EAP method profiles 210

A

abbreviating commands 193
access point 54, 180
configure 51
grounding 36
install 31
mounting 33
mounting options 30
prevent damage 30
securing 37
accounting
with RADIUS 385
with TACACS+ 395, 402
accounting command 287
Address Resolution Protocol (ARP) 275
Aironet
extensions 55
Aironet extensions 263, 274
antenna
connections 40
dual-band dipole 40
selection 271
specifications 41
ARP
caching 240
association 71
associations, limiting by MAC address 436
attributes, RADIUS
sent by the access point 392
vendor-proprietary 390
vendor-specific 389
authentication 199
local mode with AAA 230
RADIUS
key 377
login 220, 379
SSID 285
TACACS+
defined 395
key 397
login 226, 399
authentication client command 287
authentication server
configuring access point as local server 304
EAP 333, 375
authentication types
Network-EAP 332
open 332
shared key 332
authenticator 303
authorization
with RADIUS 224, 384
with TACACS+ 228, 395, 401

B

backup authenticator, local 303
bandwidth 264
basic settings
checking 505
beacon 54
beacon dtim-period command 279
beacon period command 279
bit-flip attack 273
blocking communication between clients 277
bridge virtual interface (BVI) 206
bridge-group command 277
broadcast key rotation 327, 328
broadcast-key command 343
BSSIDs 290

C

caching MAC authentications 343
Called-Station-ID
See CSID
carrier busy test 282
CCKM 24, 335
CDP
disabling for routing device 450
enabling and disabling
on an interface 450
monitoring 451
cdp enable command 450
channel
least congested 55
channel width 264
Cisco Discovery Protocol (CDP) 447
Cisco IOS Release 15.3(3)JC1 17
Cisco IOS Releases 17
Cisco Key Integrity Protocol (CKIP) 273
Cisco TAC 505
clear command 191
CLI 191
abbreviating commands 193
command modes 191
editing features
enabling and disabling 195

keystroke editing 196
wrapped lines 197
error messages 194
filtering command output 198
getting help 192
history 194
changing the buffer size 194
described 194
disabling 195
recalling commands 195
no and default forms of commands 193
Secure Shell (SSH) 199
Telnet 198
client ARP caching 240
client communication, blocking 277
Client MFP 368, 369
client power level, limiting 263
command modes 191, 192
command-line interface 24
See CLI
commands
abbreviating 193
accounting 287
authentication client 287
beacon dtim-period 279
beacon period 279
bridge-group 277
broadcast-key 343
cdp enable 450
clear 191
countermeasure tkip hold-time 346
debug 491
default form 193
del 509
dot11 aaa mac-authen filter-cache 343
dot11 extension aironet 274
dot11 interface-number carrier busy 282
dot1x reauth-period 345
edit 196
encapsulation dot1q 407
fragment-threshold 281
help 192
infrastructure-client 276
interface dot11radio 252
ip domain-name 249
ip redirect 296
no and default 193
no shutdown 193
packet retries 280
payload-encapsulation 275
permit tcp-port 296
power client 263
recall 195
rts retries 280
rts threshold 279
set 515
set BOOT 515
setting privilege levels 218
show 191
sort 198
ssid 287, 407
terminal history 195
terminal width 197
tftp_init 513
vlan 287, 407
wpa-psk 342
community strings
configuring 457
overview 456
configuration files
system contact and location information 462
configuring 260
connections 174
connections, secure remote 239
console cable 47
console port 31
countermeasure tkip hold-time command 346
counters 186
crypto software image 239
CSID format, selecting 386

D

Data Beacon Rate 277
data rate setting 256
data retries 280
data types
module defined 189
daylight saving time 244
debug command 491
default commands 193
default configuration
DNS 248
password and privilege level 214
RADIUS 220, 376
resetting 506
SNMP 457
system message logging 493
system name and prompt 247
TACACS+ 226, 397
default gateway 53, 74
default radio settings
description of 48
default settings
GUI 49
MODE 49
del command 509
delivery traffic indication message (DTIM) 278
Device Manager 46, 71
device manager 45
DFS 265
DHCP 177, 178
DHCP server
configuring access point as 236
receiving IP settings from 73
disable web-based management 66
DNS
default configuration 248
displaying the configuration 250
overview 248
setting up 248
Domain Name System
See DNS
domain names
DNS 248
dot11 aaa mac-authen filter-cache command 343
dot11 extension aironet command 274
dot11 interface-number carrier busy command 282
dot1x reauth-period command 345
DTIM 278
dual-band radios 21
duplex, Ethernet port 229
Dynamic Frequency Selection 265
blocking channels 270
CLI commands 267
configuring a channel 269
confirming DFS enabled 267

E

EAP 46
EAP authentication 78
EAP authentication, overview 332
EAP-FAST 303
EAP-TLS
applying EAP method profiles to 347
Easy Setup
network configuration 73
Easy Setup page
limitations 59
network configuration 73
radio configuration 75
security 58
edit CLI commands 196
editing features
enabling and disabling 195
keystrokes used 196
wrapped lines 197
electronic keying 173
compatible 173
disable 173
exact match 173
enable password 215
enable secret password 215
encapsulation dot1q command 407
encapsulation method 275
encrypted software image 239
encryption for passwords 215
enhanced distributed channel access 148
error and event messages 519
error messages
802.11 subsystem messages 522
access point/bridge messages 529
association management messages 521
Cisco discovery protocol messages 529
CLI 194
during command entry 194
explained 519
external radius server error messages 530
inter-access point protocol messages 527
local authenticator messages 527
mini IOS messages 529
sensor messages 530
setting the display destination device 495
severity levels 498
SNMP error messages 531
software auto upgrade messages 520
SSH error messages 531
system message format 492
unzip messages 521
Ethernet
address 172
Ethernet address 173
ethernet Cable 39
Ethernet speed and duplex settings 229
Ethertype filter 429
Event Log 72
event log 182
event messages 519

export 190
external antennas 39

F

fast secure roaming 349
faults 174
FCC 23
filter output (CLI commands) 198
filtering
Ethertype filters 444
IP filters 438
show and more command output 198
firmware
upgrade 46
fragmentation threshold 280
fragment-threshold command 281
FTP
accessing MIB files 518

G

get-bulk-request operation 455
get-next-request operation 455, 456
get-request operation 455, 456
get-response operation 455
Gigabit Ethernet port 31
global configuration mode 191, 192
Gratuitous Probe Response (GPR)
enabling and disabling 272
group key updates 342
guard interval 270
guest SSID 285

H

help 51
help, for the command line 192
high altitudes 32
history
changing the buffer size 194
described 194
disabling 195
recalling commands 195
history (CLI) 194
history table, level and number of syslog messages 500
home 71
host name 53, 73
HTTPS
certificate 66
enable secure browsing 62

I

IDF Closets 32
image, operating system 510
import 190
indicators
status 42
infrastructure-client command 276
inhibit module 174
inter-client communication, blocking 277
interface
CLI 191
web-browser 45
interface configuration mode 192
interface dot11radio command 252
interfaces
radio 71
invalid characters in 406
IP Address 73
IP address 53
ip domain-name command 249
IP filters 438
ip redirect command 296
IP redirection 295, 296
IP subnet mask 53, 74
IPv6
address 53
protocol 53
IPv6 protocol 74

J

jitter 416

K

keystrokes (edit CLI commands) 196

L

latency 416
LEAP authentication
local authentication 303
limited channel scanning 470
limiting client associations by MAC address 436
limiting client power level 263
line configuration mode 192
load balancing 273
local authenticator, access point as 303
login authentication
with RADIUS 220, 379
with TACACS+ 226, 399
Logix Designer 171
Add-on-Instruction 171

M

MAC address
ACLs, blocking association with 436
filter 429
MAC authentication caching 343
MAC filter 46

MAC-based authentication 303
management
CLI 191
Management Frame Protection 367
access points in root mode 368
broadcast management frames 368
overview 368
unicast management frames 368
Management Frame Protection 2
configuring 369
maximum data retries 280
Maximum RTS Retries 279
MCS rates 260, 261
Message Integrity Check (MIC) 273, 327, 506
MIBs
accessing files with FTP 518
location of files 518
overview 453
SNMP interaction with 456
MIC 327
MODE 49
mode button
disabling 212
enabling 212
modes
global configuration 191
interface configuration 192
line configuration 192
privileged EXEC 191
user EXEC 191
module
identification 175
monitoring
CDP 451
mounting bracket 31
move the cursor (CLI) 196
multicast messages 275
multiple basic SSIDs 290

N

names, VLAN 408
network
configuration settings 53
Network-EAP 332
no commands 193
no shutdown command 193
non-root 54, 76
non-root bridge 54

O

optional ARP caching 240

P

packet retries command 280
packet size (fragment) 280
parameters
association 97
band select 158
event log 167
event log configuration 169
GigabitEthernet status 84
HTTP upgrade 163
IP address 83
management 160
network configuration 73
network map 79
radio configuration 75
radio interface 88
security admin access 106
security encryption manager 108
security summary 105
server manager 116
software 162
software system 165
SSID manager 109
system setting 81
TFTP upgrade 164
webauth login 161
Wireless AP 99
Wireless WSD/WNM 100
password reset 506
passwords
default configuration 214
encrypting 215
overview 213
setting
enable 214
enable secret 215
with usernames 216
payload-encapsulation command 275
permit tcp-port command 296
per-VLAN Spanning Tree (PVST) 300
power client command 263
power connection 31
power level
on client devices 263
radio 273
power source 180
power-save client device 278
preferential treatment of traffic
See QoS
pre-shared key 341
pre-shared keys 506
preventing unauthorized access 213
prioritization 416
privilege levels
exiting 219
logging into 219
overview 213, 218
setting a command with 218
privileged EXEC mode 191, 192
protocol filters 429
Public Secure Packet Forwarding (PSPF) 277

Q

QBSS 417
dot11e parameter 422
QoS
overview 415
quality of service 148
See QoS

R

radio
activity 282
configuration settings 54
enable 55
interface 252
security 58
radio configuration
Aironet extensions 77
channel 77
non-root bridge 76
power 77
repeater 76
root bridge 76
scanner 76
security 75
SSID 75
universal workgroup bridge 76
VLAN 75
workgroup bridge 76
radio data rates 257
high vs low 257
radio network
optomize 54, 76
radio settings 48
radios 183
RADIUS 46
attributes
CSID format, selecting 386
sent by the access point 392
vendor-proprietary 390
vendor-specific 389
configuring
access point as local server 304
accounting 385
authentication 220, 379
authorization 224, 384
communication, global 377, 387
communication, per-server 376, 377
multiple UDP ports 376
default configuration 220, 376
defining AAA server groups 222, 381
displaying the configuration 225, 391
identifying the server 376
limiting the services to the user 224, 384
local authentication 303
method list, defined 376
operation of 375
overview 373
SSID 285
suggested network environments 373
tracking services accessed by user 385
rate limit, logging 501
recall commands 195
redirection, IP 295
regulatory domains 23
reliability problems with 257
reloading access point image 510
Remote Authentication Dial-In User Service
See RADIUS
repeater 54
as a WPA client 483
chain of access points 478
request to send (RTS) 279
reset 176
restricting access
overview 213
passwords and privilege levels 213
RADIUS 373
TACACS+ 226
RFC
1042 274
1157, SNMPv1 454
1901, SNMPv2C 454
1902 to 1907, SNMPv2 454
roaming
fast secure roaming using CCKM 349
Rockwell Automation Support 20
Role in radio network 54
role in radio network 72, 76, 93, 252, 300
root 54, 76
root bridge 54
rotation, broadcast key 327
rts retries command 280
RTS threshold 279
rts threshold command 279

S

sample configuration 261
scanner 54
secure remote connections 239
Secure Shell
See SSH
security 54
troubleshooting 506
security configuration 78
no security 78
security hasp 31
security settings, Easy Setup page 58
sequence numbers in log messages 497
server
protcol 53
server protocol 73
service set 181
service set identifiers (SSIDs)
See SSID
services 180
set BOOT command 515
set command 515
set-request operation 456
setting 270

severity filter 182
severity levels, defining in system messages 498
shared key 334
show cdp traffic command 451
show command 191
Simple Network Management Protocol
See SNMP
Simple Network Time Protocol
See SNTP
site survey 17
site surveys 30
SNMP 53
accessing MIB variables with 456
agent
described 455
disabling 457
community 74
community strings
configuring 457
overview 456
configuration examples 463
default configuration 457
limiting system log messages to NMS 500
manager functions 455
overview 453, 456
server groups 459
snmp-server view 462
status, displaying 465
system contact and location 462
trap manager, configuring 461
traps
described 455
enabling 460
overview 453, 456
types of 460
versions supported 454
SNMP versions supported 454
SNMP, FTP MIB files 518
snmp-server group command 459
SNTP
overview 241
software image 510
software upgrade
error and event messages 520
sort (CLI commands) 198
spectrum 54, 76
SSH 198, 199
crypto software image 239
described 239
displaying settings 239
SSH Communications Security, Ltd. 199
SSID 59, 181, 285, 406
assign 46
broadcast 54
create from security menu 60
guest mode 285
multiple SSIDs 285
troubleshooting 505
VLAN 286
ssid command 287, 407
static 178
statistics 188
CDP 451
status indicator
blinking green 42
blue 42
green 42
red 43
STP
displaying status 302
overview 299
Stratix 5100 wireless access point/workgroup bridge
compliance 38
login 48
operating temperature 38
power rating 38
specifications 38
summer time 244
switch
configuration 177
system clock
configuring
daylight saving time 244
manually 242
summer time 244
time zones 243
displaying the time and date 243
system management page 71
system message logging
default configuration 493
defining error message severity levels 498
disabling 493
displaying the configuration 504
enabling 493
facility keywords, described 504
level keywords, described 499
limiting messages 500
overview 491
rate limit 501
sequence numbers, enabling and disabling 497
setting the display destination device 495
timestamps, enabling and disabling 496
UNIX syslog servers
configuring the daemon 502
configuring the logging facility 503
facilities supported 504
system name
default configuration 247
manual configuration 247
See also DNS
system prompt
default setting 246, 247

T

TAC 505
TACACS+
accounting, defined 395
authentication, defined 395
authorization, defined 395
configuring
accounting 402

authentication key 397
authorization 228, 401
login authentication 226, 399
default configuration 226, 397
displaying the configuration 229, 402
identifying the server 397
limiting the services to the user 228, 401
operation of 396
overview 395
tracking services accessed by user 402
Telnet 48, 198
Temporal Key Integrity Protocol (TKIP) 327
Terminal Access Controller Access Control System Plus
See TACACS+
terminal history command 195
terminal width command 197
TFTP 513
tftp_init command 513
time
See SNTP and system clock
time zones 243
timestamps in log messages 496
TKIP 273, 327, 328
traps
configuring managers 460
defined 455
enabling 460
notification types 460
overview 453, 456
troubleshooting 505
error messages (CLI) 194
system message logging 491

U

unauthorized access 213
universal workgroup bridge 54
UNIX syslog servers
daemon configuration 502
facilities supported 504
message logging configuration 503
user EXEC mode 191, 192
username-based authentication 216

V

VLAN 54
configure 46
local authentication 303
names 408
SSID 285, 286
use 57
vlan command 287, 407

W

WDS 349, 355
configuring WDS-only mode 362
web-browser interface 24, 43, 45
WEP
with EAP 332
WEP key 78
Wi-Fi certified 21
Wi-Fi Multimedia 423
Wi-Fi Protected Access
See WPA
Wi-Fi Protected Access (WPA) 78
WMM 423
Workgroup bridge
configuring limited channel scanning 470
configuring the limited channel set 470
ignoring the CCX neighbor list 471
workgroup bridge 54, 275
guidelines for using in lightweight environment 475
in lightweight environment 474
sample lightweight network configuration 477
world mode 273
WPA 336
wpa-psk command 342
wraparound (CLI commands) 197

Rockwell Automation Support

Use the following resources to access support information.

Technical Support Center	Knowledgebase Articles, How-to Videos, FAQs, Chat, User Forums, and Product Notification Updates.	https://rockwellautomation.custhelp.com/
Local Technical Support Phone Numbers	Locate the phone number for your country.	http://www.rockwellautomation.com/global/support/get-support-now.page
Direct Dial Codes	Find the Direct Dial Code for your product. Use the code to route your call directly to a technical support engineer.	http://www.rockwellautomation.com/global/support/direct-dial.page
Literature Library	Installation Instructions, Manuals, Brochures, and Technical Data.	http://www.rockwellautomation.com/global/literature-library/overview.page
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	http://www.rockwellautomation.com/global/support/pcdc.page

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the How Are We Doing? form at http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1783-UM006D-EN-P - October 2017
Supersedes Publication 1783-UM006C-EN-P - August 2016