Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E

First Published: 2014-12-19
Last Modified: 2018-09-18

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

PREFACE

Preface ix

Document Conventions ix

Related Documentation xxi

Obtaining Documentation and Submitting a Service Request xxi

PART I

CleanAir 73

CHAPTER 1

Cisco CleanAir 1

Finding Feature Information 1

Prerequisites for CleanAir 1

Restrictions for CleanAir 2

Information About Cisco CleanAir 3

Cisco CleanAir Components 3

Cisco CleanAir-Related Terms 5

Interference Types that Cisco CleanAir can Detect 6

Interference Device Merging 7

Persistent Devices 7

Persistent Devices Detection 7

Persistent Device Avoidance 7

EDRRM and AQR Update Mode 7

CleanAir High Availability 8

How to Configure CleanAir 8

Enabling CleanAir for the 2.4-GHz Band 8

Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices 9

Configuring Interference Reporting for a 2.4-GHz Device 10
Enabling CleanAir for the 5-GHz Band 11
Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices 12
Configuring Interference Reporting for a 5-GHz Device 13
Configuring EDRRM for a CleanAir Event 14
Configuring Persistent Device Avoidance 15
Configuring Cisco CleanAir using the Controller GUI 15
Configuring Cisco CleanAir on the Cisco Wireless LAN Controller (GUI) 15
Configuring Cisco CleanAir on an Access Point (GUI) 17
Configuring Cisco Spectrum Expert 18
Configuring Spectrum Expert (GUI) 18
Configuring Spectrum Expert (CLI) 19
Monitoring CleanAir Parameters 20
Monitoring Interference Devices 23
Monitoring the Interference Devices (GUI) 23
Monitoring the Worst Air Quality of Radio Bands (GUI) 24
Configuration Examples for CleanAir 24
CleanAir FAQs 25
Additional References 27

PART II

High Availability 29

CHAPTER 2

Configuring High Availability 31
Finding Feature Information 31
Information about High Availability 31
Information About Redundancy 32
Configuring Redundancy in Access Points 32
Configuring Heartbeat Messages 33
Information about Access Point Stateful Switch Over 33
Initiating Graceful Switchover 34
Configuring EtherChannels for High Availability 34
Configuring LACP 35
Troubleshooting High Availability 36
Access the Standby Console 36
Before a Switchover 36
Contents

After a Switchover 37
Viewing Redundancy Switchover History (GUI) 38
Viewing Switchover States (GUI) 38
Monitoring the Switch Stack 40
LACP Configuration: Example 40
Flex Link Configuration: Example 42

PART III IPv6 45

CHAPTER 3 IPv6 Client IP Address Learning 47
Prerequisites for IPv6 Client Address Learning 47
Restrictions for IPv6 Client Address Learning 47
Information About IPv6 Client Address Learning 48
 SLAAC Address Assignment 48
Stateful DHCPv6 Address Assignment 49
Static IP Address Assignment 50
Router Solicitation 50
Router Advertisement 50
Neighbor Discovery 51
Neighbor Discovery Suppression 51
RA Guard 51
 RA Throttling 52
Configuring RA Guard Policy 52
Applying RA Guard Policy 53
Configuring RA Throttle Policy (CLI) 54
Applying RA Throttle Policy on VLAN (CLI) 54
Configuring IPv6 Snooping 55
Configuring IPv6 ND Suppress Policy 56
Configuring IPv6 Snooping on VLAN/PortChannel 57
Configuring IPv6 on Controller Interface 58
Configuring DHCP Pool 59
Configuring Stateless Auto Address Configuration Without DHCP (CLI) 60
Configuring Stateless Auto Address Configuration With DHCP 61
Configuring Stateful DHCP Locally 62
CHAPTER 4
Configuring IPv6 WLAN Security 69
Prerequisites for IPv6 WLAN Security 69
Restrictions for IPv6 WLAN Security 69
Information About IPv6 WLAN Security 69
How to Configure IPv6 WLAN Security 72
  Configuring Local Authentication 72
    Creating a Local User 72
    Creating an EAP Profile 72
    Configuring an EAP Profile 73
    Creating a Local Authentication Model 75
    Creating a Client VLAN 77
    Configuring Local Authentication with WPA2+AES 78
  Configuring External RADIUS Server 81
    Configuring RADIUS Authentication Server Host 81
    Configuring RADIUS Authentication Server Group 82
    Creating a Client VLAN 83
  Creating 802.1x WLAN Using an External RADIUS Server 84
Additional References 86
Feature Information for IPv6 WLAN Security 87

CHAPTER 5
Configuring IPv6 ACL 89
Prerequisites for Configuring IPv6 ACL 89
Restrictions for Configuring IPv6 ACL 89
Information About IPv6 ACL 90
  Understanding IPv6 ACLs 90
  Types of ACL 91
    Per User IPv6 ACL 91
    Filter ID IPv6 ACL 92
CHAPTER 6

Configuring IPv6 Web Authentication 107
  Prerequisites for IPv6 Web Authentication 107
  Restrictions for IPv6 Web Authentication 107
  Information About IPv6 Web Authentication 108
    Web Authentication Process 108
  How to Configure IPv6 Web Authentication 109
    Disabling WPA 109
    Enabling Security on the WLAN 110
    Enabling a Parameter Map on the WLAN 110
    Enabling Authentication List on WLAN 111
    Configuring a Global WebAuth WLAN Parameter Map 111
    Configuring the WLAN 112
    Enabling IPv6 in Global Configuration Mode 113
  Verifying IPv6 Web Authentication 114

Downloadable IPv6 ACL 92
Configuring IPv6 ACLs 92
  Default IPv6 ACL Configuration 92
  Interaction with Other Features and Switches 93
How To Configure an IPv6 ACL 93
  Creating an IPv6 ACL 93
  Applying an IPv6 to an Interface 97
  Creating WLAN IPv6 ACL 99
Verifying IPv6 ACL 99
  Displaying IPv6 ACLs 99
Configuration Examples for IPv6 ACL 100
  Example: Creating an IPv6 ACL 100
  Example: Applying IPv6 ACLs 100
  Example: Displaying IPv6 ACLs 101
  Example: Configuring RA Throttling and NS Suppression 101
  Configuring RA Guard Policy 102
  Configuring IPv6 Neighbor Binding 104
Additional References 104
  Feature Information for IPv6 ACLs 105
CHAPTER 11

Configuring UniDirectional Link Detection 193
Finding Feature Information 193
Restrictions for Configuring UDLD 193
Information About UDLD 194
   Modes of Operation 194
      Normal Mode 194
      Aggressive Mode 194
   Methods to Detect Unidirectional Links 195
      Neighbor Database Maintenance 195
      Event-Driven Detection and Echoing 196
   UDLD Reset Options 196
   Default UDLD Configuration 196
How to Configure UDLD 197
   Enabling UDLD Globally (CLI) 197
   Enabling UDLD on an Interface (CLI) 198
Monitoring and Maintaining UDLD 199
Additional References for UDLD 199
Feature Information for UDLD 200
 Contents

Prerequisites for Configuring the Access Point Retransmission Interval and Retry Count 215
Information About Retransmission Interval and Retry Count 216
How to Configure Access Point Retransmission Interval and Retry Count 216
  Configuring the Access Point Retransmission Interval and Retry Count (CLI) 216
  Configuring the Access Point Retransmission Interval and Retry Count (GUI) 217
Viewing CAPWAP Maximum Transmission Unit Information (CLI) 218
Viewing CAPWAP Maximum Transmission Unit Information (GUI) 218
Configuration Examples for Configuring Access Point Retransmission Interval and Retry Count 219
  Viewing the CAPWAP Retransmission Details: Example 219
  Viewing Maximum Transmission Unit Information: Example 219

CHAPTER 15
Configuring Adaptive Wireless Intrusion Prevention System 221
Finding Feature Information 221
Prerequisites for Configuring wIPS 221
How to Configure wIPS on Access Points 222
  Configuring wIPS on an Access Point (CLI) 222
  Configuring wIPS on an Access Point (GUI) 223
Monitoring wIPS Information 224
Configuration Examples for Configuring wIPS on Access Points 224
  Displaying the Monitor Configuration Channel Set: Example 224
  Displaying wIPS Information: Examples 225

CHAPTER 16
Configuring Authentication for Access Points 227
Finding Feature Information 227
Prerequisites for Configuring Authentication for Access Points 227
Restrictions for Configuring Authentication for Access Points 228
Information about Configuring Authentication for Access Points 228
How to Configure Authentication for Access Points 228
  Configuring Global Credentials for Access Points (CLI) 228
  Configuring Authentication for Access Points (CLI) 230
  Configuring the Switch for Authentication (CLI) 232
Configuration Examples for Configuring Authentication for Access Points 234
  Displaying the Authentication Settings for Access Points: Examples 234
CHAPTER 17

Converting Autonomous Access Points to Lightweight Mode 235

Finding Feature Information 235
Guidelines for Converting Autonomous Access Points to Lightweight Mode 235
Information About Autonomous Access Points Converted to Lightweight Mode 236
Reverting from Lightweight Mode to Autonomous Mode 236
Using DHCP Option 43 and DHCP Option 60 236
How Converted Access Points Send Crash Information to the Switch 237
Uploading Memory Core Dumps from Converted Access Points 237
Displaying MAC Addresses for Converted Access Points 237
Configuring a Static IP Address for a Lightweight Access Point 237
How to Convert a Lightweight Access Point Back to an Autonomous Access Point 238
Converting a Lightweight Access Point Back to an Autonomous Access Point (CLI) 238
Converting a Lightweight Access Point Back to an Autonomous Access Point (Using the Mode Button and a TFTP Server) 238
Authorizing Access Points (CLI) 239
Authorizing Access Points (GUI) 240
Disabling the Reset Button on Converted Access Points (CLI) 240
Monitoring the AP Crash Log Information 241
How to Configure a Static IP Address on an Access Point 242
Configuring a Static IP Address on an Access Point (CLI) 242
Configuring a Static IP Address on an Access Point (GUI) 243
Recovering the Access Point Using the TFTP Recovery Procedure 244
Configuration Examples for Converting Autonomous Access Points to Lightweight Mode 244
Example: Displaying the IP Address Configuration for Access Points 244
Example: Displaying Access Point Crash File Information 245

CHAPTER 18

Using Cisco Workgroup Bridges 247

Finding Feature Information 247
Information About Cisco Workgroup Bridges and non-Cisco Workgroup bridges 247
Monitoring the Status of Workgroup Bridges 248
Debugging WGB Issues (CLI) 248
Configuration Examples for Configuring Workgroup Bridges 249
WGB Configuration: Example 249
CHAPTER 19

Configuring Probe Request Forwarding 251
Finding Feature Information 251
Information About Configuring Probe Request Forwarding 251
How to Configure Probe Request Forwarding (CLI) 251

CHAPTER 20

Optimizing RFID Tracking 253
Finding Feature Information 253
Optimizing RFID Tracking on Access Points 253
How to Optimize RFID Tracking on Access Points 253
Optimizing RFID Tracking on Access Points (CLI) 253
Configuration Examples for Optimizing RFID Tracking 254
Displaying all the Access Points in Monitor Mode: Example 254

CHAPTER 21

Country Codes 257
Finding Feature Information 257
Information About Country Codes 257
Prerequisites for Configuring Country Codes 258
How to Configure Country Codes 258
Configuration Examples for Configuring Country Codes 260
Displaying Channel List for Country Codes: Example 260

CHAPTER 22

Configuring Link Latency 263
Finding Feature Information 263
Prerequisites for Configuring Link Latency 263
Restrictions for Configuring Link Latency 263
Information About Configuring Link Latency 264
TCP MSS 264
Link Tests 264
How to Configure Link Latency 265
Configuring Link Latency (CLI) 265
Configuring Link Latency (GUI) 267
How to Configure TCP MSS 268
Configuring TCP MSS (CLI) 268
## Mobility Control Protocols

289

- About Mobility Control Protocols 289
- Initial Association and Roaming 289
- Initial Association 290
- Intra Switch Handoff 291
- Intra Switch Peer Group Handoff 291
- Inter Switch Peer Group Handoff 292
- Inter Sub Domain Handoff 293
- Inter Mobility Group Handoff 295
- Three Way Sub Domain Handoff 295

## Configuring Mobility

297

- Configuring Mobility Controller 297

  - Configuring Converged Access Controllers 297

    - Creating Peer Groups, Peer Group Member, and Bridge Domain ID (CLI) 297
    - Creating Peer Groups, Peer Group Member, and Bridge Domain ID (GUI) 297
    - Configuring Optional Parameters for Roaming Behavior 299
    - Configuring Local Mobility Group (CLI) 300
    - Configuring Local Mobility Group (GUI) 301
    - Adding a Peer Mobility Group (CLI) 301
    - Adding a Peer Mobility Group (GUI) 302
    - Configuring Optional Parameters for Roaming Behavior 302
    - Pointing the Mobility Controller to a Mobility Oracle (CLI) 303
    - Pointing the Mobility Controller to a Mobility Oracle (GUI) 303
    - Configuring Guest Controller 304
    - Configuring Guest Anchor 305

- Configuring Converged Access Controller on 5508 or WiSM 2 306

  - Enabling the New Mobility 306
  - Configuring Mobility Controller 306
  - Creating Peer Groups, Peer Group Member, and Bridge Domain ID (CLI) 306
  - Configuring Local Mobility Group (CLI) 308
  - Adding a Peer Mobility Group (CLI) 309
  - Configuring Optional Parameters for Roaming Behavior 309
IGMP Report Suppression 325
IGMP Filtering and Throttling 326
Default IGMP Configuration 326
Default IGMP Snooping Configuration 327
Default IGMP Filtering and Throttling Configuration 327
How to Configure IGMP 328
  Configuring the Switch as a Member of a Group (CLI) 328
  Controlling Access to IP Multicast Group (CLI) 329
Changing the IGMP Version (CLI) 331
Modifying the IGMP Host-Query Message Interval (CLI) 332
Changing the IGMP Query Timeout for IGMPv2 (CLI) 334
Changing the Maximum Query Response Time for IGMPv2 (CLI) 335
Configuring the Switch as a Statically Connected Member (CLI) 336
Configuring IGMP Profiles (CLI) 337
Applying IGMP Profiles (CLI) 339
Setting the Maximum Number of IGMP Groups (CLI) 340
Configuring the IGMP Throttling Action (CLI) 342
How to Configure IGMP Snooping 343
  Enabling IGMP Snooping 343
  Enabling or Disabling IGMP Snooping on a VLAN Interface (CLI) 344
Setting the Snooping Method (CLI) 345
Configuring a Multicast Router Port (CLI) 346
Configuring a Host Staticaly to Join a Group (CLI) 348
Enabling IGMP Immediate Leave (CLI) 349
Configuring the IGMP Leave Timer (CLI) 350
Configuring the IGMP Robustness-Variable (CLI) 351
Configuring the IGMP Last Member Query Count (CLI) 353
Configuring TCN-Related Commands 354
Configuring the IGMP Snooping Querier (CLI) 357
Disabling IGMP Report Suppression (CLI) 359
Monitoring IGMP 360
  Monitoring IGMP Snooping Information 361
  Monitoring IGMP Filtering and Throttling Configuration 362
Configuration Examples for IGMP 363
Example: Configuring the Switch as a Member of a Multicast Group 363
Example: Controlling Access to Multicast Groups 363
Examples: Configuring IGMP Snooping 363
Example: Configuring IGMP Profiles 364
Example: Applying IGMP Profile 365
Example: Setting the Maximum Number of IGMP Groups 365
Example: Interface Configuration as a Routed Port 365
Example: Interface Configuration as an SVI 365
Additional References 366
Feature History and Information for IGMP 367

CHAPTER 29 Configuring Wireless Multicast 369
Finding Feature Information 369
Prerequisites for Configuring Wireless Multicast 369
Restrictions on Configuring Wireless Multicast 370
Restrictions for IPv6 Snooping 370
Restrictions for IPv6 RA Guard 370
Information About Wireless Multicast 370
Multicast Optimization 371
IPv6 Global Policies 372
IPv6 RA Guard 372
Information About IPv6 Snooping 372
IPv6 Neighbor Discovery Inspection 372
How to Configure Wireless Multicast 374
Configuring Wireless Multicast-MCMC Mode (CLI) 374
Configuring Wireless Multicast-MCUC Mode (CLI) 375
Configuring IPv6 Snooping (CLI) 376
Configuring IPv6 Snooping Policy (CLI) 376
Configuring Layer 2 Port as Multicast Router Port (CLI) 377
Configuring IPv6 RA Guard (CLI) 377
Configuring Non-IP Wireless Multicast (CLI) 378
Configuring Wireless Broadcast (CLI) 379
Configuring IP Multicast VLAN for WLAN (CLI) 380
Monitoring Wireless Multicast 381
# Contents

## CHAPTER 31

**Configuring Cisco IOS Configuration Engine** 403

- Prerequisites for Configuring the Configuration Engine 403
- Restrictions for Configuring the Configuration Engine 403
- Information About Configuring the Configuration Engine 404

  - Cisco Configuration Engine Software 404
  - Configuration Service 405
  - Event Service 405
  - NameSpace Mapper 406
  - Cisco Networking Services IDs and Device Hostnames 406
    - ConfigID 406
    - DeviceID 406
    - Hostname and DeviceID 407
    - Hostname, DeviceID, and ConfigID 407
  - Cisco IOS CNS Agents 407
    - Initial Configuration 407
    - Incremental (Partial) Configuration 408
    - Synchronized Configuration 408
  - Automated CNS Configuration 408
  - How to Configure the Configuration Engine 409
    - Enabling the CNS Event Agent 409
    - Enabling the Cisco IOS CNS Agent 411
    - Enabling an Initial Configuration for Cisco IOS CNS Agent 412
    - Refreshing DeviceIDs 417
    - Enabling a Partial Configuration for Cisco IOS CNS Agent 419
  - Monitoring CNS Configurations 420
  - Additional References 421
  - Feature History and Information for the Configuration Engine 422

## CHAPTER 32

**Configuring the Cisco Discovery Protocol** 423

- Information About CDP 423
  - Cisco Discovery Protocol Overview 423
  - CDP and Stacks 424
  - Default Cisco Discovery Protocol Configuration 424
How to Configure CDP  424
  Configuring Cisco Discovery Protocol Characteristics  424
  Disabling Cisco Discovery Protocol  426
  Enabling Cisco Discovery Protocol  427
  Disabling Cisco Discovery Protocol on an Interface  428
  Enabling Cisco Discovery Protocol on an Interface  429
  Monitoring and Maintaining Cisco Discovery Protocol  431
  Additional References  431
  Feature History and Information for Cisco Discovery Protocol  432

CHAPTER 33  433
Configuring Simple Network Management Protocol  433
  Finding Feature Information  433
  Prerequisites for SNMP  433
  Restrictions for SNMP  435
  Information About SNMP  436
    SNMP Overview  436
    SNMP Manager Functions  436
    SNMP Agent Functions  436
    SNMP Community Strings  437
    SNMP MIB Variables Access  437
    SNMP Notifications  438
    SNMP iFIndex MIB Object Values  438
    Default SNMP Configuration  438
    SNMP Configuration Guidelines  439
  How to Configure SNMP  439
    Disabling the SNMP Agent  439
    Configuring Community Strings  441
    Configuring SNMP Groups and Users  443
    Configuring SNMP Notifications  446
    Setting the Agent Contact and Location Information  451
    Limiting TFTP Servers Used Through SNMP  452
    Configuring Trap Flags for SNMP  453
    Enabling SNMP Wireless Trap Notification  455
  Monitoring SNMP Status  456
CHAPTER 34

Configuring Service Level Agreements 461
Finding Feature Information 461
Restrictions on SLAs 461
Information About SLAs 462
Cisco IOS IP Service Level Agreements (SLAs) 462
Network Performance Measurement with Cisco IOS IP SLAs 463
IP SLA Responder and IP SLA Control Protocol 464
Response Time Computation for IP SLAs 464
IP SLAs Operation Scheduling 465
IP SLA Operation Threshold Monitoring 465
UDP Jitter 466
How to Configure IP SLAs Operations 467
Default Configuration 467
Configuration Guidelines 467
Configuring the IP SLA Responder 468
Implementing IP SLA Network Performance Measurement 469
Analyzing IP Service Levels by Using the UDP Jitter Operation 473
Analyzing IP Service Levels by Using the ICMP Echo Operation 477
Monitoring IP SLA Operations 480
Monitoring IP SLA Operation Examples 481
Additional References 481
Feature History and Information for Service Level Agreements 483

CHAPTER 35

Configuring Local Policies 485
Finding Feature Information 485
Restrictions for Configuring Local Policies 485
Information About Configuring Local Policies 486
How to Configure Local Policies 487
Configuring Local Policies (CLI) 487
Creating a Service Template (CLI) 488
Creating an Interface Template (CLI) 489
Creating a Parameter Map (CLI) 489
Creating a Class Map (CLI) 491
Creating a Policy Map (CLI) 491
Applying a Local Policy for a Device on a WLAN (CLI) 492
Configuring Local Policies (GUI) 494
Creating a Service Template (GUI) 494
Creating a Policy Map (GUI) 495
Applying Local Policies to WLAN (GUI) 496
Monitoring Local Policies 496
Examples: Local Policies Configuration 497
Additional References for Configuring Local Policies 499
Feature History for Performing Local Policies Configuration 499

CHAPTER 36 Configuring SPAN and RSPAN 501
Prerequisites for SPAN and RSPAN 501
Restrictions for SPAN and RSPAN 501
Information About SPAN and RSPAN 503
SPAN and RSPAN 503
Local SPAN 503
Remote SPAN 504
SPAN and RSPAN Concepts and Terminology 505
SPAN and RSPAN Interaction with Other Features 510
SPAN and RSPAN and Device Stacks 511
Flow-Based SPAN 511
Default SPAN and RSPAN Configuration 512
Configuration Guidelines 512
SPAN Configuration Guidelines 512
RSPAN Configuration Guidelines 513
FSPAN and FRSPAN Configuration Guidelines 513
How to Configure SPAN and RSPAN 513
Creating a Local SPAN Session 513
Creating a Local SPAN Session and Configuring Incoming Traffic 516
Specifying VLANs to Filter 518
Adding or Modifying Capture Point Parameters 558
Deleting Capture Point Parameters 560
Deleting a Capture Point 562
Activating and Deactivating a Capture Point 563
Clearing the Capture Point Buffer 566
Monitoring Wireshark 568
Configuration Examples for Wireshark 568
Example: Displaying a Brief Output from a .pcap File 568
Example: Displaying Detailed Output from a .pcap File 569
Example: Simple Capture and Display 571
Example: Simple Capture and Store 572
Example: Using Buffer Capture 575
Example: Capture Sessions 581
Example: Capture and Store in Lock-step Mode 582
Example: Simple Capture and Store of Packets in Egress Direction 583
Additional References 585
Feature History and Information for WireShark 586

PART IX
QoS 587

CHAPTER 38 Configuring QoS 589
Finding Feature Information 589
Prerequisites for Quality of Service 589
QoS Components 590
QoS Terminology 590
Information About QoS 591
QoS Overview 591
Modular QoS Command-Line Interface 591
Wireless QoS Overview 591
QoS and IPv6 for Wireless 592
Wireless QoS Overview 591
Supported QoS Features on Wireless Targets 594
Port Policies 596
Radio Policies 598
SSID Policies 598
Client Policies 599
Hierarchical QoS 600
Hierarchical Wireless QoS 600
QoS Implementation 602
  Layer 2 Frame Prioritization Bits 603
  Layer 3 Packet Prioritization Bits 603
  End-to-End QoS Solution Using Classification 603
  Packet Classification 603
QoS Wired Model 606
  Ingress Port Activity 606
  Egress Port Activity 606
Classification 607
  Access Control Lists 607
  Class Maps 608
  Policy Maps 608
Policing 610
  Token-Bucket Algorithm 611
Marking 611
  Packet Header Marking 611
  Switch Specific Information Marking 612
  Table Map Marking 612
Traffic Conditioning 613
  Policing 614
  Shaping 615
Queueing and Scheduling 616
  Bandwidth 617
  Weighted Tail Drop 618
  Priority Queues 619
  Queue Buffer 619
  Queuing in Wireless 621
Trust Behavior 621
  Trust Behavior for Wired and Wireless Ports 621
  Port Security on a Trusted Boundary for Cisco IP Phones 622
Wireless QoS Mobility 623
  Inter-Switch Roaming 623
  Intra-Switch Roaming 624
Precious Metal Policies for Wireless QoS 624
Standard QoS Default Settings 625
  Default Wired QoS Configuration 625
  Default Wireless QoS Configuration 626
Configuring Auto QoS for Wireless 627
  Information About Auto QoS for Wireless 627
  Configuring Auto QoS for Wireless (GUI) 628
  Configuring Auto QoS for Wireless (CLI) 629
Guidelines for QoS Policies 629
Restrictions for QoS on Wired Targets 629
Restrictions for QoS on Wireless Targets 632
How to Configure QoS 635
  Configuring Class, Policy, and Table Maps 635
    Creating a Traffic Class (CLI) 635
    Creating a Traffic Policy (CLI) 638
    Configuring Client Policies (GUI) 642
    Configuring Client Policies 644
    Configuring Class-Based Packet Marking (CLI) 645
    Configuring Class Maps for Voice and Video (CLI) 650
    Attaching a Traffic Policy to an Interface (CLI) 651
    Configuring SSID Policies (GUI) 652
    Applying an SSID or Client Policy on a WLAN (CLI) 654
    Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps (CLI) 655
    Classifying, Policing, and Marking Traffic on SVIs by Using Policy Maps (CLI) 658
    Configuring Table Maps (CLI) 661
Configuring Trust 664
  Configuring Trust Behavior for Wireless Traffic (CLI) 664
Configuring QoS Features and Functionality 664
  Configuring Call Admission Control (CLI) 664
  Configuring Bandwidth (CLI) 671
  Configuring Police (CLI) 673
Configuring the Tx-Power Control Threshold (CLI)  727
Configuring the Tx-Power Level (CLI)  728
Configuring Transmit Power Control (GUI)  728
Configuring 802.11 RRM Parameters  730
  Configuring Advanced 802.11 Channel Assignment Parameters (CLI)  730
  Configuring Dynamic Channel Assignment (GUI)  732
  Configuring 802.11 Coverage Hole Detection (CLI)  735
  Configuring Coverage Hole Detection (GUI)  737
  Configuring 802.11 Event Logging (CLI)  738
  Configuring 802.11 Statistics Monitoring (CLI)  739
  Configuring the 802.11 Performance Profile (CLI)  740
Configuring Rogue Access Point Detection in RF Groups  741
  Configuring Rogue Access Point Detection in RF Groups (CLI)  741
  Enabling Rogue Access Point Detection in RF Groups (GUI)  742
Monitoring RRM Parameters and RF Group Status  743
  Monitoring RRM Parameters  743
  Monitoring RF Group Status (CLI)  744
  Monitoring RF Group Status (GUI)  744
Examples: RF Group Configuration  745
Information About ED-RRM  745
  Configuring ED-RRM on the Cisco Wireless LAN Controller (CLI)  745
  Configuring ED-RRM (GUI)  746
Additional References for Radio Resource Management  747
Feature History and Information For Performing Radio Resource Management Configuration  747

PART XI  Security  749

CHAPTER 40  Preventing Unauthorized Access  751
  Finding Feature Information  751
  Preventing Unauthorized Access  751

CHAPTER 41  Controlling Switch Access with Passwords and Privilege Levels  753
  Finding Feature Information  753
  Restrictions for Controlling Switch Access with Passwords and Privileges  753
TACACS+ Authorization for Privileged EXEC Access and Network Services 774
TACACS+ Accounting 774
Default TACACS+ Configuration 774
How to Configure Switch Access with TACACS+ 774
Identifying the TACACS+ Server Host and Setting the Authentication Key 775
Configuring TACACS+ Login Authentication 776
Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services 779
Starting TACACS+ Accounting 780
Establishing a Session with a Router if the AAA Server is Unreachable 782
Monitoring TACACS+ 782
Additional References for Configuring Secure Shell 782
Feature Information for TACACS+ 783

CHAPTER 43 Configuring RADIUS 785
Finding Feature Information 785
Prerequisites for Configuring RADIUS 785
Restrictions for Configuring RADIUS 786
Information about RADIUS 787
  RADIUS and Switch Access 787
  RADIUS Overview 787
  RADIUS Operation 788
RADIUS Change of Authorization 789
  Change-of-Authorization Requests 790
  CoA Request Response Code 792
  CoA Request Commands 793
  Stacking Guidelines for Session Termination 795
Default RADIUS Configuration 796
RADIUS Server Host 796
RADIUS Login Authentication 797
AAA Server Groups 798
AAA Authorization 798
RADIUS Accounting 798
Vendor-Specific RADIUS Attributes 798
Vendor-Proprietary RADIUS Server Communication 810
How to Configure RADIUS  810
   Identifying the RADIUS Server Host  810
   Configuring RADIUS Login Authentication  813
   Defining AAA Server Groups  815
   Configuring RADIUS Authorization for User Privileged Access and Network Services  817
   Starting RADIUS Accounting  818
   Establishing a Session with a Router if the AAA Server is Unreachable  819
   Configuring Settings for All RADIUS Servers  820
   Configuring the Switch to Use Vendor-Specific RADIUS Attributes  821
   Configuring the Switch for Vendor-Proprietary RADIUS Server Communication  822
   Configuring CoA on the Switch  824
   Configuring RADIUS Server Load Balancing  826
   Monitoring CoA Functionality  826
   Configuration Examples for Controlling Switch Access with RADIUS  827
      Examples: Identifying the RADIUS Server Host  827
      Example: Using Two Different RADIUS Group Servers  827
      Examples: Configuring the Switch to Use Vendor-Specific RADIUS Attributes  827
      Example: Configuring the Switch for Vendor-Proprietary RADIUS Server Communication  828
   Additional References for Configuring Secure Shell  828
   Feature Information for RADIUS  829

CHAPTER 44

Configuring Kerberos  831
   Finding Feature Information  831
   Prerequisites for Controlling Switch Access with Kerberos  831
   Restrictions for Controlling Switch Access with Kerberos  832
   Information about Kerberos  832
      Kerberos and Switch Access  832
      Kerberos Overview  832
      Kerberos Operation  834
         Authenticating to a Boundary Switch  834
         Obtaining a TGT from a KDC  835
      Authenticating to Network Services  835
   How to Configure Kerberos  835
   Monitoring the Kerberos Configuration  835
Numbered Extended IPv4 ACLs  874
Named IPv4 ACLs   875
ACL Logging       875
Smart Logging     876
Hardware and Software Treatment of IP ACLs   876
VLAN Map Configuration Guidelines   877
VLAN Maps with Router ACLs   877
    VLAN Maps and Router ACL Configuration Guidelines   878
Time Ranges for ACLs   878
IPv4 ACL Interface Considerations   879
How to Configure ACLs   879
    Configuring IPv4 ACLs   879
    Creating a Numbered Standard ACL   880
    Creating a Numbered Extended ACL   881
    Creating Named Standard ACLs   885
    Creating Extended Named ACLs   886
    Configuring Time Ranges for ACLs   887
    Applying an IPv4 ACL to a Terminal Line   889
    Applying an IPv4 ACL to an Interface   890
    Creating Named MAC Extended ACLs   891
    Applying a MAC ACL to a Layer 2 Interface   893
    Configuring VLAN Maps   894
    Creating a VLAN Map   896
    Applying a VLAN Map to a VLAN   897
    Configuring VACL Logging   898
Monitoring IPv4 ACLs   900
Configuration Examples for ACLs   901
    Examples: Using Time Ranges with ACLs   901
    Examples: Including Comments in ACLs   901
    Examples: Troubleshooting ACLs   902
IPv4 ACL Configuration Examples   903
    ACLs in a Small Networked Office   903
    Examples: ACLs in a Small Networked Office   904
    Example: Numbered ACLs   905
Examples: Extended ACLs 905
Examples: Named ACLs 906
Examples: Time Range Applied to an IP ACL 906
Examples: Configuring Commented IP ACL Entries 907
Examples: ACL Logging 907
Configuration Examples for ACLs and VLAN Maps 909
Example: Creating an ACL and a VLAN Map to Deny a Packet 909
Example: Creating an ACL and a VLAN Map to Permit a Packet 909
Example: Default Action of Dropping IP Packets and Forwarding MAC Packets 909
Example: Default Action of Dropping MAC Packets and Forwarding IP Packets 910
Example: Default Action of Dropping All Packets 910
Configuration Examples for Using VLAN Maps in Your Network 911
Example: Wiring Closet Configuration 911
Example: Restricting Access to a Server on Another VLAN 912
Example: Denying Access to a Server on Another VLAN 912
Configuration Examples of Router ACLs and VLAN Maps Applied to VLANs 913
Example: ACLs and Switched Packets 913
Example: ACLs and Bridged Packets 914
Example: ACLs and Routed Packets 914
Example: ACLs and Multicast Packets 915
Additional References 916
Feature Information for IPv4 Access Control Lists 916

CHAPTER 49 IPv6 ACLs 919
Finding Feature Information 919
IPv6 ACLs Overview 919
Switch Stacks and IPv6 ACLs 920
Interactions with Other Features and Switches 920
Restrictions for IPv6 ACLs 920
Default Configuration for IPv6 ACLs 921
Configuring IPv6 ACLs 921
Attaching an IPv6 ACL to an Interface 925
Monitoring IPv6 ACLs 926
Additional References 927
Example of Configuring Inaccessible Authentication Bypass 1037
Configuring 802.1x Authentication with WoL 1038
Configuring MAC Authentication Bypass 1039
Configuring 802.1x User Distribution 1040
   Example of Configuring VLAN Groups 1040
Configuring NAC Layer 2 802.1x Validation 1041
Configuring Limiting Login for Users 1043
Configuring an Authenticator Switch with NEAT 1044
Configuring a Supplicant Switch with NEAT 1046
Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs 1048
   Configuring Downloadable ACLs 1048
   Configuring a Downloadable Policy 1050
Configuring VLAN ID-based MAC Authentication 1052
Configuring Flexible Authentication Ordering 1052
Configuring Open1x 1054
Disabling 802.1x Authentication on the Port 1055
   Resetting the 802.1x Authentication Configuration to the Default Values 1056
Monitoring 802.1x Statistics and Status 1057
Additional References for IEEE 802.1x Port-Based Authentication 1058
Feature Information for 802.1x Port-Based Authentication 1059

CHAPTER 54 Configuring MACsec Encryption 1061
   Finding Feature Information 1061
   Restriction for MACsec Encryption 1061
   Information About MACsec Encryption 1061
      Media Access Control Security and MACsec Key Agreement 1062
         MKA Policies 1063
         Virtual Ports 1063
         MACsec and Stacking 1063
         MACsec, MKA and 802.1x Host Modes 1064
   Configuring MKA and MACsec 1066
   Default MACsec MKA Configuration 1066
   Configuring an MKA Policy 1066
   Configuring MACsec on an Interface 1067
Information About Cisco TrustSec 1069
Configuring Cisco TrustSec MACsec 1071
  Configuring Cisco TrustSec Credentials on the Switch 1071
  Configuring Cisco TrustSec Switch-to-Switch Link Security in 802.1x Mode 1072
  Configuring Cisco TrustSec Switch-to-Switch Link Security in Manual Mode 1074
Configuration Examples 1077
  Example: Configuring MACsec on an Interface 1077
  Cisco TrustSec Switch-to-Switch Link Security Configuration Example 1080

CHAPTER 55
Web-Based Authentication 1083
Finding Feature Information 1083
Web-Based Authentication Overview 1083
  Device Roles 1085
  Host Detection 1085
  Session Creation 1085
  Authentication Process 1086
  Local Web Authentication Banner 1087
  Web Authentication Customizable Web Pages 1089
    Guidelines 1089
    Authentication Proxy Web Page Guidelines 1091
    Redirection URL for Successful Login Guidelines 1091
    Custom Web Authentication Guidelines 1092
Web-based Authentication Interactions with Other Features 1092
  Port Security 1092
  LAN Port IP 1092
  Gateway IP 1092
  ACLs 1092
  Context-Based Access Control 1092
  EtherChannel 1093
How to Configure Web-Based Authentication 1093
  Default Web-Based Authentication Configuration 1093
  Web-Based Authentication Configuration Guidelines and Restrictions 1093
  Web-Based Authentication Configuration Task List 1095
  Configuring the Authentication Rule and Interfaces 1095
Configuring AAA Authentication 1096
Configuring Switch-to-RADIUS-Server Communication 1098
Configuring the HTTP Server 1100
    Customizing the Authentication Proxy Web Pages 1101
   Specifying a Redirection URL for Successful Login 1102
Configuring the Web-Based Authentication Parameters 1103
Configuring a Web-Based Authentication Local Banner 1104
Configuring Web-Based Authentication without SVI 1105
Configuring Web-Based Authentication with VRF Aware 1106
Removing Web-Based Authentication Cache Entries 1107
Downloading Web Authentication Tar Bundle (CLI) 1108
Downloading Web Authentication Tar Bundle (GUI) 1109
Integrating Customized Web Authentication Pages into a Parameter Map (CLI) 1109
Linking Image in Custom Pages 1111
Sample Web Authentication Login HTML 1112
Configuring a Parameter Map for Local Web Authentication (CLI) 1113
Monitoring Web-Based Authentication Status 1115
Feature Information for Web-Based Authentication 1116

CHAPTER 56

Configuring Cisco TrustSec 1117
    Information about Cisco TrustSec 1117
    Finding Feature Information 1118
    Feature Information for Cisco TrustSec 1118

CHAPTER 57

Configuring Wireless Guest Access 1119
    Finding Feature Information 1119
    Prerequisites for Guest Access 1119
    Restrictions for Guest Access 1120
    Information about Wireless Guest Access 1120
    Fast Secure Roaming 1120
    How to Configure Guest Access 1121
        Creating a Lobby Administrator Account 1121
        Configuring Guest User Accounts 1122
        Configuring Mobility Agent (MA) 1123
Manually Assigning IP Information to Multiple SVIs 1225
Modifying the Switch Startup Configuration 1226
  Specifying the Filename to Read and Write the System Configuration 1226
Boot the Switch in Installed Mode 1227
Boot the Switch in Bundle Mode 1229
Configuring a Scheduled Software Image Reload 1230
Monitoring Switch Setup Configuration 1232
  Example: Verifying the Switch Running Configuration 1232
  Examples: Displaying Software Bootup in Install Mode 1232
  Example: Emergency Installation 1234
Configuration Examples for Performing Switch Setup 1236
  Example: Configuring a Switch to Download Configurations from a DHCP Server 1236
  Examples: Scheduling Software Image Reload 1237
Additional References For Performing Switch Setup 1237
Feature History and Information For Performing Switch Setup Configuration 1238

CHAPTER 63
Configuring Right-To-Use Licenses 1239
  Finding Feature Information 1239
Restrictions for Configuring RTU Licenses 1239
Information About Configuring RTU Licenses 1240
  Right-To-Use Licensing 1240
  Right-To-Use Image-Based Licenses 1240
  Right-To-Use License States 1241
  License Activation for Switch Stacks 1241
Mobility Controller Mode 1242
  Right-To-Use AP-Count Licensing 1242
  Right-to-Use AP-Count Evaluation Licenses 1242
  Right-To-Use Adder AP-Count Rehosting Licenses 1243
How to Configure RTU Licenses 1243
  Activating an Image Based License 1243
  Activating an AP-Count License 1245
  Obtaining an Upgrade or Capacity Adder License 1245
  Rehosting a License 1246
Monitoring and Maintaining RTU Licenses 1247
CHAPTER 64  Configuring Administrator Usernames and Passwords  1253

Finding Feature Information  1253

Information About Configuring Administrator Usernames and Passwords  1253

Configuring Administrator Usernames and Passwords  1254

Examples: Administrator Usernames and Passwords Configuration  1256

Additional References for Administrator Usernames and Passwords  1257

Feature History and Information for Performing Administrator Usernames and Passwords Configuration  1257

CHAPTER 65  802.11 parameters and Band Selection  1259

Finding Feature Information  1259

Restrictions on Band Selection, 802.11 Bands, and Parameters  1259

Information About Configuring Band Selection, 802.11 Bands, and Parameters  1260

Band Selection  1260

802.11 Bands  1261

802.11n Parameters  1261

802.11h Parameters  1262

How to Configure 802.11 Bands and Parameters  1262

Configuring Band Selection (CLI)  1262

Configuring the 802.11 Bands (CLI)  1263

Configuring the 802.11 Bands (GUI)  1265

Configuring 802.11n Parameters (CLI)  1267

Configuring the 802.11n Parameters (GUI)  1269

Configuring 802.11h Parameters (CLI)  1270

Configuring the 802.11h Parameters (GUI)  1271
CHAPTER 66  Configuring Aggressive Load Balancing  1281
Finding Feature Information  1281
Restrictions for Aggressive Load Balancing  1281
Information for Configuring Aggressive Load Balancing Parameters  1282
 Aggressive Load Balancing  1282
How to Configure Aggressive Load Balancing  1283
 Configuring Aggressive Load Balancing  1283
Monitoring Aggressive Load Balancing  1284
Examples: Aggressive Load Balancing Configuration  1284
Additional References for Aggressive Load Balancing  1285
Feature History and Information For Performing Aggressive Load Balancing Configuration  1286

CHAPTER 67  Configuring Client Roaming  1287
Finding Feature Information  1287
Restrictions for Configuring Client Roaming  1287
Information About Client Roaming  1287
 Inter-Subnet Roaming  1289
 Voice-over-IP Telephone Roaming  1289
 CCX Layer 2 Client Roaming  1289
# How to Configure Layer 2 or Layer 3 Roaming

1290

## Configuring Layer 2 or Layer 3 Roaming

1290

## Configuring CCX Client Roaming Parameters (CLI)

1291

## Configuring Mobility Oracle

1293

## Configuring Mobility Controller

1293

## Configuring Mobility Agent

1295

## Monitoring Client Roaming Parameters

1296

## Monitoring Mobility Configurations

1296

## Additional References for Configuring Client Roaming

1297

## Feature History and Information for Performing Client Roaming Configuration

1298

---

## CHAPTER 68 Configuring Application Visibility and Control

1299

### Finding Feature Information

1299

### Information About Application Visibility and Control

1299

### Supported AVC Class Map and Policy Map Formats

1301

### Prerequisites for Application Visibility and Control

1303

### Guidelines for Inter-Switch Roaming with Application Visibility and Control

1303

### Restrictions for Application Visibility and Control

1303

### How to Configure Application Visibility and Control

1305

## Configuring Application Visibility and Control (CLI)

1305

### Creating a Flow Record

1305

### Creating a Flow Exporter (Optional)

1307

### Creating a Flow Monitor

1308

### Creating AVC QoS Policy

1309

### Configuring WLAN to Apply Flow Monitor in IPV4 Input/Output Direction

1320

### Configuring Application Visibility and Control (GUI)

1320

### Configuring Application Visibility (GUI)

1320

### Configuring Application Visibility and Control (GUI)

1321

### Monitoring Application Visibility and Control

1322

## Monitoring Application Visibility and Control (CLI)

1322

## Monitoring Application Visibility and Control (GUI)

1323

## Monitoring SSID and Client Policies Statistics (GUI)

1324

### Examples: Application Visibility and Control

1325

### Examples: Application Visibility Configuration

1325

---

### Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E

---
Contents

CHAPTER 71

Configuring Location Settings 1357
Finding Feature Information 1357
Information About Configuring Location Settings 1357
How to Configure Location Settings 1358
Configuring Location Settings (CLI) 1358
Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues 1360
Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues 1361
Monitoring Location Settings and NMSP Settings 1362
Monitoring Location Settings (CLI) 1362
Monitoring NMSP Settings (CLI) 1362
Examples: Location Settings Configuration 1363
Examples: NMSP Settings Configuration 1363
Additional References for Location Settings 1363
Feature History and Information For Performing Location Settings Configuration 1364

CHAPTER 72

Monitoring Flow Control 1365
Finding Feature Information 1365
Information About Flow Control 1365
Monitoring Flow Control 1365
Examples: Monitoring Flow Control 1366
Additional References for Monitoring Flow Control 1367
Feature History and Information For Monitoring Flow Control 1367

CHAPTER 73

Configuring System Message Logs 1369
Finding Feature Information 1369
Restrictions for Configuring System Message Logs 1369
Information About Configuring System Message Logs 1369
System Message Logging 1369
System Log Message Format 1370
Default System Message Logging Settings 1371
Syslog Message Limits 1372
Enabling Syslog Trap Messages 1372
How to Configure System Message Logs 1372
Setting the Message Display Destination Device 1372
Synchronizing Log Messages 1374
Disabling Message Logging 1375
Enabling and Disabling Time Stamps on Log Messages 1376
Enabling and Disabling Sequence Numbers in Log Messages 1377
Defining the Message Severity Level 1378
Limiting Syslog Messages Sent to the History Table and to SNMP 1378
Logging Messages to a UNIX Syslog Daemon 1379
Monitoring and Maintaining System Message Logs 1380
Monitoring Configuration Archive Logs 1380
Configuration Examples for System Message Logs 1380
Example: Switch System Message 1380
Additional References for System Message Logs 1381
Feature History and Information For System Message Logs 1382

CHAPTER 74
Configuring Online Diagnostics 1383
Finding Feature Information 1383
Information About Configuring Online Diagnostics 1383
Online Diagnostics 1383
How to Configure Online Diagnostics 1384
Starting Online Diagnostic Tests 1384
Configuring Online Diagnostics 1385
Scheduling Online Diagnostics 1385
Configuring Health-Monitoring Diagnostics 1386
Monitoring and Maintaining Online Diagnostics 1388
Displaying Online Diagnostic Tests and Test Results 1388
Configuration Examples for Online Diagnostic Tests 1389
Examples: Start Diagnostic Tests 1389
CHAPTER 83 Configuring VLAN Trunks 1503
Finding Feature Information 1503
Prerequisites for VLAN Trunks 1503
Restrictions for VLAN Trunks 1504
Information About VLAN Trunks 1505
Trunking Overview 1505
Trunking Modes 1505
Layer 2 Interface Modes 1505
Allowed VLANs on a Trunk 1506
Load Sharing on Trunk Ports 1506
  Network Load Sharing Using STP Priorities 1506
  Network Load Sharing Using STP Path Cost 1507
Feature Interactions 1507
How to Configure VLAN Trunks 1507
  Configuring an Ethernet Interface as a Trunk Port 1508
    Configuring a Trunk Port (CLI) 1508
    Defining the Allowed VLANs on a Trunk (CLI) 1510
    Changing the Pruning-Eligible List (CLI) 1511
    Configuring the Native VLAN for Untagged Traffic (CLI) 1512
  Configuring Trunk Ports for Load Sharing 1514
    Configuring Load Sharing Using STP Port Priorities (CLI) 1514
    Configuring Load Sharing Using STP Path Cost (CLI) 1517
Where to Go Next 1519
Additional References 1520
Feature History and Information for VLAN Trunks 1521

PART XV WLAN 1523

CHAPTER 84 WLANs 1525
  Finding Feature Information 1525
Information About WLANs 1525
   Band Selection 1526
   Off-Channel Scanning Defer 1526
   DTIM Period 1526
   Session Timeouts 1527
   Cisco Client Extensions 1527
   Peer-to-Peer Blocking 1528
   Diagnostic Channel 1528
   Per-WLAN Radius Source Support 1528
Prerequisites for WLANs 1529
Restrictions for WLANs 1529
How to Configure WLANs 1532
   Creating WLANs (CLI) 1532
   Creating WLANs (GUI) 1533
   Deleting WLANs (CLI) 1534
   Deleting WLANs (GUI) 1534
   Searching WLANs (CLI) 1535
   Searching WLANs (GUI) 1535
   Enabling WLANs (CLI) 1536
   Disabling WLANs (CLI) 1536
   Configuring General WLAN Properties (CLI) 1537
   Configuring General WLAN Properties (GUI) 1539
   Configuring Advanced WLAN Properties (CLI) 1540
   Configuring Advanced WLAN Properties (GUI) 1543
   Applying a QoS Policy on a WLAN (GUI) 1546
Monitoring WLAN Properties (CLI) 1547
Viewing WLAN Properties (GUI) 1548
Where to Go Next 1548
Additional References 1549
Feature Information for WLANs 1550

CHAPTER 85  DHCP for WLANs 1551
   Finding Feature Information 1551
   Information About the Dynamic Host Configuration Protocol 1551

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2014-2018 Cisco Systems, Inc. All rights reserved.
Preface

- Document Conventions, on page lxix
- Related Documentation, on page lxxi
- Obtaining Documentation and Submitting a Service Request, on page lxxi

Document Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ or Ctrl</td>
<td>Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)</td>
</tr>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>Italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
<tr>
<td><strong>Courier</strong> font</td>
<td>Terminal sessions and information the system displays appear in <strong>courier</strong> font.</td>
</tr>
<tr>
<td><strong>Bold Courier</strong> font</td>
<td><strong>Bold Courier</strong> font indicates text that the user must enter.</td>
</tr>
<tr>
<td>[x]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>...</td>
<td>An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.</td>
</tr>
<tr>
<td></td>
<td>A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt;: &gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Reader Alert Conventions**

This document may use the following conventions for reader alerts:

- **Note**
  Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

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

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

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

- **Warning**
  **IMPORTANT SAFETY INSTRUCTIONS**
  This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS
Related Documentation

Before installing or upgrading the switch, refer to the switch release notes.

- Cisco Catalyst 3850 Series Switches documentation, located at:
  http://www.cisco.com/go/cat3850_docs

- Cisco 5700 Series Wireless Controller documentation, located at:
  http://www.cisco.com/go/wlc5700_sw

- Cisco SFP, SFP+, and QSFP+ modules documentation, including compatibility matrixes, located at:

- Cisco Validated Designs documents, located at:
  http://www.cisco.com/go/designzone

Obtaining Documentation and Submitting a Service Request

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

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

CleanAir

• Cisco CleanAir, on page 1
Cisco CleanAir

- Finding Feature Information, on page 1
- Prerequisites for CleanAir, on page 1
- Restrictions for CleanAir, on page 2
- Information About Cisco CleanAir, on page 3
- How to Configure CleanAir, on page 8
- Configuring Cisco CleanAir using the Controller GUI, on page 15
- Configuring Cisco Spectrum Expert, on page 18
- Monitoring CleanAir Parameters, on page 20
- Configuration Examples for CleanAir, on page 24
- CleanAir FAQs, on page 25
- Additional References, on page 27

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for CleanAir

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Only Cisco CleanAir-enabled access points using the following access point modes can perform Cisco CleanAir spectrum monitoring:

- Local—In this mode, each Cisco CleanAir-enabled access point radio provides air quality and interference detection reports for the current operating channel only.

- Monitor—When Cisco CleanAir is enabled in monitor mode, the access point provides air quality and interference detection reports for all monitored channels.

The following options are available:
• All—All channels
• DCA—Channel selection governed by the DCA list
• Country—All channels are legal within a regulatory domain

Note
The access point does not participate in AQ HeatMap in Prime Infrastructure.

• SE-Connect—This mode enables a user to connect a Spectrum Expert application running on an external Microsoft Windows XP or Vista PC to a Cisco CleanAir-enabled access point in order to display and analyze detailed spectrum data. The Spectrum Expert application connects directly to the access point, bypassing the switch. An access point in SE-Connect mode does not provide any Wi-Fi, RF, or spectrum data to the switch. All CleanAir system functionality is suspended while the AP is in this mode, and no clients are served. This mode is intended for remote troubleshooting only. Up to three active Spectrum Expert connections are possible.

• Only Cisco Catalyst 3850 and Switches can function as a Mobility Agent.

• Cisco Catalyst 3850 Switches and Cisco 5760 Wireless LAN Controllers can function as Mobility Controllers.

Restrictions for CleanAir

• Access points in monitor mode do not transmit Wi-Fi traffic or 802.11 packets. They are excluded from radio resource management (RRM) planning and are not included in the neighbor access point list. IDR clustering depends on the switch’s ability to detect neighboring in-network access points. Correlating interference device detections from multiple access points is limited between monitor-mode access points.

• SE-connect is an access point mode similar to local mode or monitor mode. The access point provides spectrum information to Spectrum Expert only for the current channel(s). The spectrum data is available for the current active channel(s) and the common monitored channel list is available. The access point continues to send AQ (Air Quality) and IDR (Interference Device Reports) reports to the switch and perform normal activities according to the current mode. Sniffer and rogue detections access point modes are incompatible with all types of CleanAir spectrum monitoring.

• Local Mode access point—Serves WLAN clients with the time slicing off-channel scanning and listens for 50 ms on each channel, and scans configurable feature scanning for all/country/DCA channels.

• Monitor Mode access point—Does not serve WLAN clients and are dedicated to scanning only. These access points listen for 1.2 s on each channel, and scans all channels.

• Monitor Mode access point in slot 2 operates at 2.4 GHz only.

• We recommend a ratio of 1 monitor-mode access point for every 5 local-mode access points; this can vary based on the network design and expert guidance for best coverage.

• Spectrum Expert (Windows XP laptop client) and AP should be pingable, otherwise; it will not work.
**Information About Cisco CleanAir**

Cisco CleanAir is a solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all the users of a shared spectrum (both native devices and foreign interferers). It also enables the network to act upon this information. For example, you can manually remove the interfering device, or the system can automatically change the channel away from the interference. CleanAir provides spectrum management and Radio Frequency (RF) visibility.

A Cisco CleanAir system consists of CleanAir-enabled access points, Cisco Wireless LAN Controllers, and Cisco Prime Infrastructure. These access points collect information about all the devices that operate in the industrial, scientific, and medical (ISM) bands, identify and evaluate the information as a potential interference source, and forward it to the Cisco WLC. The Cisco WLC controls the access points, collects spectrum data, and forwards information to Cisco Prime Infrastructure or a Cisco mobility services engine (MSE) upon request.

Any networking configurations can be performed only on the mobility controller, configurations cannot be performed in the MA mode. However, any radio level CleanAir configurations can be done using mobility anchor.

For every device operating in the unlicensed band, Cisco CleanAir provides information about what it is, where it is, how it is impacting your wireless network, and what actions you or your network should take. It simplifies RF.

Wireless LAN systems operate in unlicensed 2.4-GHz and 5-GHz ISM bands. Many devices, such as microwave ovens, cordless phones, and Bluetooth devices also operate in these bands and can negatively affect the Wi-Fi operations.

Some of the most advanced WLAN services, such as voice-over-wireless and IEEE 802.11n radio communications, might be significantly impaired by the interference caused by other legal users of the ISM bands. The integration of Cisco CleanAir functionality addresses this problem of RF interference.

**Cisco CleanAir Components**

The basic Cisco CleanAir architecture consists of Cisco CleanAir-enabled APs and switch. Cisco Prime Infrastructure (PI), Mobility Services Engine (MSE) and Cisco Spectrum Expert are optional system components. Cisco PI and MSE provide user interfaces for advanced spectrum capabilities such as historic charts, tracking interference devices, location services and impact analysis.
An access point equipped with Cisco CleanAir technology collects information about non-Wi-Fi interference sources, processes it, and forwards it to the MA. The access point sends the Air Quality Report (AQR) and Interference Device Report (IDR) to the controller.

The mobility controller (MC) controls and configures CleanAir-capable access points, and collects and processes spectrum data, and provides it to the PI and/or the MSE. The MC provides local user interfaces (GUI and CLI) to configure basic CleanAir features and services and display current spectrum information. The MC also detects, merges, and mitigates interference devices using RRM TPC and DCM. For details, see Interference Device Merging.

Cisco PI provides advanced user interfaces for CleanAir that include feature enabling and configuration, consolidated display information, historic AQ records and reporting engines. PI also shows charts of interference devices, AQ trends, and alerts.

Cisco MSE is required for location and historic tracking of interference devices, and provides coordination and consolidation of interference reports across multiple controllers. MSE also provides adaptive Wireless Intrusion Prevention System (WIPS) service that provides comprehensive over-the-air threat detection, location and mitigation. MSE also merges all the interference data.

To obtain detailed spectrum data that can be used to generate RF analysis plots similar to those provided by a spectrum analyzer, you can configure a Cisco CleanAir-enabled access point to connect directly to a Microsoft Windows XP or Vista PC running the Cisco Spectrum Expert application.

The switch performs the following tasks in a Cisco CleanAir system:

- Configures Cisco CleanAir capabilities on the access point.
- Provides interfaces (GUI CLI, and SNMP) for configuring Cisco CleanAir features and retrieving data.
- Displays spectrum data.
• Collects and processes AQRs from the access point and stores them in the air quality database. AQRs contain information about the total interference from all the identified sources represented by the Air Quality Index (AQI) and the summary for the most severe interference categories. The CleanAir system can also include unclassified interference information under per-interference type reports that enable you to take action in scenarios where interference because of unclassified interfering devices is more.

• Collects and processes IDRs from the access point and stores them in the interference device database.

• Forwards spectrum data to Prime Infrastructure and the MSE.

Note
In vEWLC, when Cisco CleanAir is disabled, both CleanAir and Air Quality reporting are disabled. In spite of this, Air Quality is still populated.

Cisco CleanAir-Related Terms

<table>
<thead>
<tr>
<th>Table 1: CleanAir-Related Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Term</strong></td>
</tr>
<tr>
<td>AQI</td>
</tr>
<tr>
<td>AQR</td>
</tr>
<tr>
<td>DC</td>
</tr>
<tr>
<td>EDRRM</td>
</tr>
<tr>
<td>IDR</td>
</tr>
<tr>
<td>ISI</td>
</tr>
<tr>
<td>MA</td>
</tr>
<tr>
<td>MC</td>
</tr>
<tr>
<td>RSSI</td>
</tr>
</tbody>
</table>
Interference Types that Cisco CleanAir can Detect

Cisco CleanAir can detect interference, report on the location and severity of the interference, and recommend different mitigation strategies. Two such mitigation strategies are persistent device avoidance and spectrum event-driven RRM.

Wi-Fi chip-based RF management systems share these characteristics:

- Any RF energy that cannot be identified as a Wi-Fi signal is reported as noise.
- Noise measurements that are used to assign a channel plan tend to be averaged over a period of time to avoid instability or rapid changes that can be disruptive to certain client devices.
- Averaging measurements reduces the resolution of the measurement. As such, a signal that disrupts clients might not look like it needs to be mitigated after averaging.
- All RF management systems available today are reactive in nature.

Cisco CleanAir is different and can positively identify not only the source of the noise but also its location and potential impact to a WLAN. Having this information allows you to consider the noise within the context of the network and make intelligent and, where possible, proactive decisions. For CleanAir, two types of interference events are common:

- Persistent interference
- Spontaneous interference

Persistent interference events are created by devices that are stationary in nature and have intermittent but largely repeatable patterns of interference. For example, consider the case of a microwave oven located in a break room. Such a device might be active for only 1 or 2 minutes at a time. When operating, however, it can be disruptive to the performance of the wireless network and associated clients. Using Cisco CleanAir, you can positively identify the device as a microwave oven rather than indiscriminate noise. You can also determine exactly which part of the band is affected by the device, and because you can locate it, you can understand which access points are most severely affected. You can then use this information to direct RRM in selecting a channel plan that avoids this source of interference for the access points within its range. Because this interference is not active for a large portion of the day, existing RF management applications might attempt to again change the channels of the affected access points. Persistent device avoidance is unique, however, in that it remains in effect as long as the source of interference is periodically detected to refresh the persistent status. The Cisco CleanAir system knows that the microwave oven exists and includes it in all future planning. If you move either the microwave oven or the surrounding access points, the algorithm updates RRM automatically.

Note

Spectrum event-driven RRM can be triggered only by Cisco CleanAir-enabled access points in local mode.

Note

All the APs using qualcomm atheros chipset sends air-quality as 100 percent even if the radios detect interference.

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a threshold for air quality (AQ) which, if exceeded, triggers an immediate channel change for the affected access
point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active. Cisco CleanAir also identifies and locates the source of interference so that more permanent mitigation of the device can be performed at a later time.

In the case of Bluetooth devices, Cisco CleanAir-enabled access points can detect and report interference only if the devices are actively transmitting. Bluetooth devices have extensive power-save modes. For example, interference can be detected when data or voice is being streamed between the connected devices.

**Interference Device Merging**

The Interference Devices (ID) messages are processed on a Mobility Controller (MC). The Mobility Anchor (MA) forwards the ID messages from APs and hence they are processed on the MC. The MC has visibility of the neighbor information across APs connected to different MAs.

ID merging logic requires AP neighbor information. Neighbor information is obtained from the RRM module. This API only gives neighbor information to the APs directly connected to MC.

Currently the AP neighbor list on MA is synced to MC once every 3 minutes; hence the AP neighbor list obtained by this API could be at most 3 mins old. This delay results in delay in merging of Devices as they are discovered. The subsequent periodic merge will pick up the updated neighbor information and merge is performed.

**Persistent Devices**

Some interference devices such as outdoor bridges and Microwave Ovens only transmit when needed. These devices can cause significant interference to the local WLAN due to short duration and periodic operation remain largely undetected by normal RF management metrics. With CleanAir the RRM DCA algorithm can detect, measure, register and remember the impact and adjust the DCA algorithm. This minimizes the use of channels affected by the persistent devices in the channel plan local to the interference source. Cisco CleanAir detects and stores the persistent device information in the switch and this information is used to mitigate interfering channels.

**Persistent Devices Detection**

CleanAir-capable Monitor Mode access point collects information about persistent devices on all configured channels and store the information in controller. Local/Bridge mode AP detects interference devices on the serving channels only.

**Persistent Device Avoidance**

When a Persistent Device (PD) is detected in the CleanAir module, it is reported to the RRM module on the MA. This information is used in the channel selection by the subsequent EDRRM Event Driven RRM (ED-RRM) signal sent to the RRM module.

**EDRRM and AQR Update Mode**

EDRRM is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels. A CleanAir access point always monitors AQ and reports the AQ every 15
minutes. AQ only reports classified interference devices. The key benefit of EDRRM is very fast action time. If an interfering device is operating on an active channel and causes enough AQ degradation to trigger an EDRRM, then no clients will be able to use that channel or the access point. You must remove the access point from the channel. EDRRM is not enabled by default, you must first enable CleanAir and then enable EDRRM.

AQRs are only available on the MC. The mode configuration and timers are held in Radio Control Block (RCB) on MA (for APs connected to MA). There is no change to the current API available for EMS/NMS. No change is required for directly connected APs as RCB (spectrum config and timers) is available locally. For remote APs (APs connected to MA), three new control messages are added. These three messages are for enable, restart timer and disable rapid update mode for a given AP MAC address and slot.

**CleanAir High Availability**

CleanAir configuration (network and radio) is stateful during the switchover. On the MC, Embedded Instrumentation Core (EICORE) provides the sync on network configurations across active and standby nodes. The radio configurations are synced using the HA Infrastructure. The CleanAir configurations on MA are pulled from the MC upon joining. The network configuration is not stored in the EICORE on MA, hence it is synced using HA Infrastructure.

CleanAir Data (AQ and IDR) reports are not stateful, that is, the standby and active nodes are not synced. On switchover, the APs send the reports to the current active slot. The RRM Client (HA Infra Client) is used for CleanAir HA sync.

**How to Configure CleanAir**

**Enabling CleanAir for the 2.4-GHz Band**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>ap dot11 24ghz cleanair</td>
<td>Enables the CleanAir feature on the 802.11b network. Run the no form of this command to disable CleanAir on the 802.11b network.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)#ap dot11 24ghz cleanair</td>
<td></td>
</tr>
<tr>
<td>Switch(config)#no ap dot11 24ghz cleanair</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap dot11 24ghz cleanair alarm air-quality threshold <strong>threshold_value</strong></td>
<td>Configures the alarm for the threshold value for air-quality for all the 2.4-GHz devices. Add the no form of this command to disable the alarm.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ap dot11 24ghz cleanair alarm device {bt-discovery</td>
<td>bt-link</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config)#ap dot11 24ghz cleanair alarm device canopy</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Interference Reporting for a 2.4-GHz Device

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
|      | **Example:**
|      | `Switch(config)# configure terminal` | |
| Step 2 | `ap dot11 24ghz cleanair device {bt-discovery | bt-link | canopy | cont-tx | dect-like | fh | inv | jammer | mw-oven | nonstd | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile | xbox | zigbee }` The following is a list of the keyword descriptions: |
|      | **Example:**
|      | `Switch(config)# ap dot11 24ghz cleanair device bt-discovery` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device bt-link` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device canopy` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device cont-tx` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device dect-like` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device fh` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device inv` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device jammer` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device mw-oven` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device superag` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device tdd-tx` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device video` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device wimax-fixed` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device wimax-mobile` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device xbox` | |
|      | `Switch(config)# ap dot11 24ghz cleanair device zigbee` | |
|      | **Purpose:** Configures the 2.4-GHz interference devices to report to the switch. Run the `no` form of this command to disable the configuration. |
Enabling CleanAir for the 5-GHz Band

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

Step 1

Configure terminal
Example:
Switch# configure terminal

Step 2

ap dot11 5ghz cleanair
Example:
Switch(config)#ap dot11 5ghz cleanair
Switch(config)#no ap dot11 5ghz cleanair

Step 3

end
Example:
Switch(config)# end

Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.
### Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>ap dot11 5ghz cleanair alarm air-quality threshold threshold_value</code></td>
<td>Configures the alarm for the threshold value for air-quality for all the 5-GHz devices. Add the <strong>No</strong> form of the command to disable the alarm.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)#ap dot11 5ghz cleanair alarm air-quality threshold 50</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>`ap dot11 5ghz cleanair alarm device {canopy</td>
<td>cont-tx</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)#ap dot11 5ghz cleanair alarm device</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring Interference Reporting for a 5-GHz Device

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Switch(config)# ap dot11 5ghz cleanair device canopy</td>
<td>Configures a 5-GHz interference device to report to the switch. Run the no form of this command to disable interference device reporting.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• canopy—Canopy device</td>
<td>The following is a list of the keyword descriptions:</td>
</tr>
<tr>
<td></td>
<td>• cont-tx—Continuous transmitter</td>
<td>• canopy—Canopy device</td>
</tr>
<tr>
<td></td>
<td>• dect-like—Digital Enhanced Cordless Communication-like phone</td>
<td>• cont-tx—Continuous transmitter</td>
</tr>
<tr>
<td></td>
<td>• fh—802.11-frequency hopping device</td>
<td>• dect-like—Digital Enhanced Cordless Communication-like phone</td>
</tr>
<tr>
<td></td>
<td>• inv—Device using spectrally-inverted Wi-Fi signals</td>
<td>• fh—802.11-frequency hopping device</td>
</tr>
<tr>
<td></td>
<td>• jammer—Jammer</td>
<td>• inv—Device using spectrally-inverted Wi-Fi signals</td>
</tr>
<tr>
<td></td>
<td>• nonstd—Device using nonstandard Wi-Fi channels</td>
<td>• jammer—Jammer</td>
</tr>
<tr>
<td></td>
<td>• radar—Radar</td>
<td>• nonstd—Device using nonstandard Wi-Fi channels</td>
</tr>
<tr>
<td></td>
<td>• report—Interference device reporting</td>
<td>• radar—Radar</td>
</tr>
<tr>
<td></td>
<td>• superag—802.11 SuperAG device</td>
<td>• report—Interference device reporting</td>
</tr>
<tr>
<td></td>
<td>• tdd-tx—TDD transmitter</td>
<td>• superag—802.11 SuperAG device</td>
</tr>
<tr>
<td></td>
<td>• video—Video camera</td>
<td>• tdd-tx—TDD transmitter</td>
</tr>
<tr>
<td></td>
<td>• wimax-fixed—WiMax fixed</td>
<td>• video—Video camera</td>
</tr>
<tr>
<td></td>
<td>• wimax-mobile—WiMax mobile</td>
<td>• wimax-fixed—WiMax fixed</td>
</tr>
</tbody>
</table>
### Configuring EDRRM for a CleanAir Event

#### Procedure

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch(config)# end
```
Configuring Persistent Device Avoidance

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} rrm channel device`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>ap dot11 24ghz rrm channel device</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Cisco CleanAir using the Controller GUI

#### Configuring Cisco CleanAir on the Cisco Wireless LAN Controller (GUI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Configuration &gt; Wireless &gt; 802.11a/n/ac or 802.11b/g/n &gt; CleanAir to open the 802.11a (or 802.11b) &gt; CleanAir page.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select the CleanAir check box to enable Cisco CleanAir functionality on the 802.11a/n or 802.11b/g/n network, or unselect it to prevent the switch from detecting spectrum interference. By default, the Cisco CleanAir is disabled.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select the Report Interferers check box to enable the Cisco CleanAir system to report any detected sources of interference, or unselect it to prevent the switch from reporting interferers. The default value is selected. <strong>Note</strong> Device Security alarms, Event Driven RRM, and the Persistence Device Avoidance algorithm do not work if Report Interferers are disabled.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Select the Persistent Device Propagation check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables you to propagate information about persistent devices to the neighboring access points connected to the same switch. Persistent interferers are present at the location and interfere with the WLAN operations even if they are not detectable at all times.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Ensure that any sources of interference that need to be detected and reported by the Cisco CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferences</td>
</tr>
</tbody>
</table>
Configure Cisco CleanAir as follows:

a) Select the **Enable AQI (Air Quality Index) Trap** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature. The default value is selected.

b) If you selected the **Enable AQI Trap** check box in Step a, enter a value between 1 and 100 (inclusive) in the AQI Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

c) Enter the AQI threshold in the **AQI Alarm Threshold** text box. An alarm is generated when the air quality reaches a threshold value. The default is 35. The range is from 1 and 100.

d) Select the **Enable Interference For Security Alarm** check box to trigger interferer alarms when the switch detects specified device types, or unselect it to disable this feature. The default value is selected.

e) Make sure that any sources of interference that need to trigger interferer alarms appear in the **Trap on These Types** box and any that do not need to trigger interferer alarms appear in the **Do Not Trap on These Types** box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.

For example, if you want the switch to send an alarm when it detects a jamming device, select the **Enable Interference For Security Alarm** check box and move the jamming device to the **Trap on These Types** box.

**Step 7**

Click **Apply**.
**Step 8**  
Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference as follows:

a) Look at the **EDRRM** field to see the current status of spectrum event-driven RRM and, if enabled, the Sensitivity Threshold field to see the threshold level at which event-driven RRM is invoked.

b) If you want to change the current status of event-driven RRM or the sensitivity level, go to the **802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA)** page.

c) Select the **EDRRM** check box to trigger RRM to run when an access point detects a certain level of interference, or unselect it to disable this feature. The default value is selected.

d) If you selected the **EDRRM** check box in Step c, choose **Low**, **Medium**, **High**, or **Custom** from the Sensitivity Threshold drop-down list to specify the threshold at which you want RRM to be triggered. When the interference for the access point rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. EDRRM prevents the access point from returning to the original channel for three hours after the event.

High—Represents an increased sensitivity to changes in the environment.

Custom—Allows you to set a threshold value in the Custom Sensitivity Threshold field. The default sensitivity is 35.

Low—Represents a decreased sensitivity to changes in the environment.

The EDRRM AQ threshold value for low sensitivity is 35, medium sensitivity is 50, and high sensitivity is 60.

e) Click **Apply**.

**Step 9**  
Click **Save Configuration**.

---

**Confguring Cisco CleanAir on an Access Point (GUI)**

**Procedure**

**Step 1**  
Choose **Configuration > Wireless > Access Points > Radios > 802.11a/n or 802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

**Step 2**  
Select the check box adjacent to the desired access point and click **Configure**. The 802.11a/n/ac (or 802.11b/g/n) Radios page appears.

The **CleanAir Capable** field shows whether this access point can support CleanAir functionality. If it can, go to the next step to enable or disable CleanAir for this access point. If the access point cannot support CleanAir functionality, you cannot enable CleanAir for this access point.

**Note**  
By default, the Cisco CleanAir functionality is enabled on the radios.

**Step 3**  
Enable Cisco CleanAir functionality for this access point by choosing **Enable** from the CleanAir Admin Status drop-down list. To disable CleanAir functionality for this access point, choose **Disable**. The default value is Enable. This setting overrides the global CleanAir configuration for this access point.

**Step 4**  
Click **Apply**.
Step 5   Click Save Configuration.

Configuring Cisco Spectrum Expert

Configuring Spectrum Expert (GUI)

Before you begin

• Spectrum Expert (Windows XP laptop client) and access point should be pingable, otherwise; it will not work.

• Prior to establishing a connection between the Spectrum Expert console and the access point, make sure that IP address routing is properly configured and the network spectrum interface (NSI) ports are open in any intervening firewalls.

• The access point must be a TCP server listening on ports 37540 for 2.4 GHz and 37550 for 5 GHz frequencies. These ports must be opened for the spectrum expert application to connect to the access point using the NSI protocol.

• You can view the NSI key from the switch CLI by using the show ap name ap_name config dot11 {24ghz | 5ghz} command.

Procedure

Step 1  Ensure that Cisco CleanAir functionality is enabled for the access point that will be connected to the Spectrum Expert console.

Note     The SE-Connect mode is set for the entire access point, not just a single radio. However, the Spectrum Expert console connects to a single radio at a time.

Step 2  Choose Configuration > Wireless > Access Points > All APs to open the All APs page.

Step 3  Click the name of the desired access point to open the All APs > Details page.

Step 4  Choose SE-Connect from the AP Mode drop-down list. This mode is available only for access points that are capable of supporting Cisco CleanAir functionality. For the SE-Connect mode to appear as an available option, the access point must have at least one spectrum-capable radio in the Enable state.

Step 5  Click Apply to commit your changes.

Step 6  Click OK when prompted to reboot the access point.

Step 7  On the Windows PC, access the Cisco Software Center from this URL:

  http://www.cisco.com/cisco/software/navigator.html

Step 8  Click Product > Wireless > Cisco Spectrum Intelligence > Cisco Spectrum Expert > Cisco Spectrum Expert Wi-Fi, and then download the Spectrum Expert 4.1.11 executable (*.exe) file.

Step 9  Run the Spectrum Expert application on the PC.
Step 10 When the Connect to Sensor dialog box appears, enter the IP address of the access point, choose the access point radio, and enter the 16-byte network spectrum interface (NSI) key to authenticate. The Spectrum Expert application opens a TCP/IP connection directly to the access point using the NSI protocol.

When an access point in SE-Connect mode joins a switch, it sends a Spectrum Capabilities notification message, and the switch responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the switch for NSI authentication. The switch generates one key per access point, which the access point stores until it is rebooted.

**Note** You can establish up to three Spectrum Expert console connections per access point radio.

Step 11 Verify that the Spectrum Expert console is connected to the access point by selecting the Slave Remote Sensor text box in the bottom right corner of the Spectrum Expert application. If the two devices are connected, the IP address of the access point appears in this text box.

Step 12 Use the Spectrum Expert application to view and analyze spectrum data from the access point.

---

**Configuring Spectrum Expert (CLI)**

**Before you begin**

- Spectrum Expert (Windows XP laptop client) and access point should be pingable, otherwise; it will not work.

- Prior to establishing a connection between the Spectrum Expert console and the access point, make sure that IP address routing is properly configured and the network spectrum interface (NSI) ports are open in any intervening firewalls.

- The access point must be a TCP server listening on ports 37540 for 2.4-GHz and 37550 for 5-GHz frequencies. These ports must be opened for the spectrum expert application to connect to the access point using the NSI protocol.

- You can view the NSI key from the switch CLI by using the `show ap name ap_name config dot11 {24ghz | 5ghz}` command.

**Procedure**

**Step 1** To configure the access point for SE-Connect mode, enter this command:

```
ap name ap_name mode se-connect
```

**Example:**

```
Switch# ap name Cisco_AP3500 mode se-connect
```

**Step 2** When prompted to reboot the access point, enter Y.

**Step 3** To view the NSI key for the access point, enter this command:

```
show ap name ap_name config dot11 {24ghz | 5ghz}
```

**Example:**

```
Switch# show ap name Cisco_AP3500 config dot11 24ghz
<snippet>
```
CleanAir Management Information

- CleanAir Capable: Yes
- CleanAir Management Admin State: Enabled
- CleanAir Management Operation State: Up
- CleanAir NSI Key: 274F1F9B1A5206683FAF57D87BFFBC9B
- CleanAir Sensor State: Configured

What to do next

On the Windows PC, download Cisco Spectrum Expert:

1. Access the Cisco Software Center from this URL: [http://www.cisco.com/cisco/software/navigator.html](http://www.cisco.com/cisco/software/navigator.html)
2. Click Product > Wireless > Cisco Spectrum Intelligence > Cisco Spectrum Expert > Cisco Spectrum Expert Wi-Fi, and then download the Spectrum Expert 4.1.11 executable (*.exe) file.
3. Run the Spectrum Expert application on the PC.
4. When the Connect to Sensor dialog box appears, enter the IP address of the access point, choose the access point radio, and enter the 16-byte network spectrum interface (NSI) key to authenticate. The Spectrum Expert application opens a TCP/IP connection directly to the access point using the NSI protocol.

When an access point in SE-Connect mode joins a switch, it sends a Spectrum Capabilities notification message, and the switch responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the switch for use in NSI authentication. The switch generates one key per access point, which the access point stores until it is rebooted.

Note: You can establish up to three Spectrum Expert console connections per access point radio.

- Verify that the Spectrum Expert console is connected to the access point by selecting the Slave Remote Sensor text box in the bottom right corner of the Spectrum Expert application. If the two devices are connected, the IP address of the access point appears in this text box.
- Use the Spectrum Expert application to view and analyze spectrum data from the access point.

Monitoring CleanAir Parameters

You can monitor CleanAir parameters using the following commands:

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap dot11 24ghz cleanair air-quality summary</td>
<td>Displays CleanAir AQ data for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair air-quality worst</td>
<td>Displays CleanAir AQ worst data for the 2.4-GHz band.</td>
</tr>
<tr>
<td>Command Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair config</td>
<td>Displays CleanAir configuration for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type all</td>
<td>Displays all the CleanAir interferers for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type bt-discovery</td>
<td>Displays CleanAir interferers of type BT Discovery for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type bt-link</td>
<td>Displays CleanAir interferers of type BT Link for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type canopy</td>
<td>Displays CleanAir interferers of type Canopy for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type cont-tx</td>
<td>Displays CleanAir interferers of type Continuous transmitter for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type dect-like</td>
<td>Displays CleanAir interferers of type DECT Like for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type fh</td>
<td>Displays CleanAir interferers of type 802.11FH for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type inv</td>
<td>Displays CleanAir interferers of type Wi-Fi Inverted for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type jammer</td>
<td>Displays CleanAir interferers of type Jammer for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type mw-oven</td>
<td>Displays CleanAir interferers of type MW Oven for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type nonstd</td>
<td>Displays CleanAir interferers of type Wi-Fi inverted channel for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type persistent</td>
<td>Displays CleanAir interferers of type Persistent for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type superag</td>
<td>Displays CleanAir interferers of type SuperAG for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type tdd-tx</td>
<td>Displays CleanAir interferers of type TDD Transmit for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type video</td>
<td>Displays CleanAir interferers of type Video Camera for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type wimax-fixed</td>
<td>Displays CleanAir interferers of type WiMax Fixed for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type wimax-mobile</td>
<td>Displays CleanAir interferers of type WiMax Mobile for the 2.4-GHz band.</td>
</tr>
</tbody>
</table>
You can also check the CleanAir status of the access points using the switch GUI:

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap dot11 24ghz clean device type xbox</td>
<td>Displays CleanAir interferers of type Xbox for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type zigbee</td>
<td>Displays CleanAir interferers of type Zigbee for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean air-quality summary</td>
<td>Displays CleanAir AQ data for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean air-quality worst</td>
<td>Displays CleanAir AQ worst data for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean air config</td>
<td>Displays CleanAir configuration for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type all</td>
<td>Displays all the CleanAir interferers for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type canopy</td>
<td>Displays CleanAir interferers of type Canopy for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type cont-tx</td>
<td>Displays CleanAir interferers of type Continuous TX for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type dect-like</td>
<td>Displays CleanAir interferers of type DECT Like for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type inv</td>
<td>Displays CleanAir interferers of type Wi-Fi Inverted for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type jammer</td>
<td>Displays CleanAir interferers of type Jammer for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type nonstd</td>
<td>Displays CleanAir interferers of type Wi-Fi inverted channel for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type persistent</td>
<td>Displays CleanAir interferers of type Persistent for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type superag</td>
<td>Displays CleanAir interferers of type SuperAG for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type tdd-tx</td>
<td>Displays CleanAir interferers of type TDD Transmit for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type video</td>
<td>Displays CleanAir interferers of type Video Camera for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type wimax-fixed</td>
<td>Displays CleanAir interferers of type WiMax Fixed for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz clean device type wimax-mobile</td>
<td>Displays CleanAir interferers of type WiMax Mobile for the 5-GHz band.</td>
</tr>
</tbody>
</table>
Procedure

Choose **Monitor > Wireless > Access Points > 802.11 a/n/ac 802.11 b/g/n**.

The **Radios** page is displayed showing a list of access points that are associated with the switch. You can see the CleanAir Admin and CleanAir Status.

The Cisco CleanAir status is one of the following:

- **UP**—The spectrum sensor for the access point radio is currently operational (error code 0).

- **DOWN**—The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio.

- **ERROR**—The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable Cisco CleanAir functionality on the radio.

- **N/A**—This access point radio is not capable of supporting Cisco CleanAir functionality.

---

**Monitoring Interference Devices**

When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed, which results in the spectrum sensor to stop detecting the device temporarily. This device is then correctly marked as down. Such a device is correctly removed from the spectrum database. In cases when all the interferer detections for a specific device are reported, the cluster ID is kept alive for an extended period of time to prevent possible device-detection bouncing. If the same device is detected again, it is merged with the original cluster ID and the device-detection history is preserved.

For example, some bluetooth headsets operate on battery power. These devices employ methods to reduce power consumption, such as turning off the transmitter when not actually needed. Such devices can appear to come and go from the classification. To manage these devices, CleanAir keeps the cluster IDs for longer and they are remerged into a single record upon detection. This process smoothen the user records and accurately represents the device history.

**Monitoring the Interference Devices (GUI)**

**Before you begin**

You can configure Cisco CleanAir only on CleanAir-enabled access points.

**Procedure**

**Step 1**

Choose **Monitor > Interferers > Cisco CleanAir > 802.11a/n or 802.11b/g/n > Interference Devices** to open the Cisco APs > Interference Devices page.
This page shows the following information:

- **AP Name**—The name of the access point where the interference device is detected.
- **Interferer Type**—Type of the interferer.
- **Affected Channel**—Channel that the device affects.
- **Severity**—Severity index of the interfering device.
- **Duty Cycle (%)**—Proportion of time during which the interfering device was active.
- **RSSI**—Receive signal strength indicator (RSSI) of the access point.
- **DevID**—Device identification number that uniquely identified the interfering device.
- **ClusterID**—Cluster identification number that uniquely identifies the type of the devices.

**Step 2**

Click the **Filter** icon or choose the **Quick Filter** option from the Show drop-down list to display the information about interference devices based on a particular criteria.

---

**Monitoring the Worst Air Quality of Radio Bands (GUI)**

**Procedure**

Choose **Monitor > Cisco CleanAir > Worst Air-Quality** to open the Air Quality Report page.

This page shows the air quality of both the 802.11a/n/ac and 802.11b/g/n radio bands. This page displays the following information:

- **AP Name**—Name of the access point that reported the worst air quality for the 802.11 radio band.
- **Channel Number**—Radio channel with the worst reported air quality.
- **Minimum Air Quality Index**—Minimum air quality for this radio channel. The range is from 1 to 100. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Average Air Quality Index**—Average air quality for this radio channel. The range is from 1 to 100. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Interference Device Count**—Number of interferers detected by the radios on the 802.11 radio band.

---

**Configuration Examples for CleanAir**

This example shows how to enable CleanAir on the 2.4-GHz band and an access point operating in the channel:

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz cleanair
Switch(config)#exit
```
Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices: Example

This example shows how to configure a CleanAir Alarm for 2.4-GHz Air-Quality threshold of 50 dBm and an Xbox device:

Switch#configure terminal
Switch(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50
Switch(config)#ap dot11 24ghz cleanair alarm device xbox
Switch(config)#end

Configuring Interference Reporting for 5-GHz Devices: Example

This example shows how to configure interference reporting for 5-GHz devices:

Switch#configure terminal
Switch(config)#ap dot11 5ghz cleanair alarm device xbox
Switch(config)#end

This example shows how to enable an EDRRM CleanAir event in the 2.4-GHz band and configure high sensitivity to non-Wi-Fi interference:

Switch#configure terminal
Switch(config)#ap dot11 24ghz rrm channel cleanair-event
Switch(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high
Switch(config)#end

Configuring Persistent Device Avoidance: Example

This example shows how to enable persistent non-Wi-Fi device avoidance in the 2.4-GHz band:

Switch#configure terminal
Switch(config)#ap dot11 24ghz rrm channel device
Switch(config)#end

Configuring an Access Point for SE-Connect Mode: Example

This example shows how to configure an access point in the SE-Connect mode:

Switch#ap name Cisco_AP3500 mode se-connect

CleanAir FAQs

Q. How do I check if my MC is up?
A. To check if the MC is up, use the command: `show wireless mobility summary`.

This example shows how to display the mobility summary:

Switch#show wireless mobility summary

```
Mobility Controller Summary:
  Mobility Role : Mobility Controller
  Mobility Protocol Port : 16666
  Mobility Group Name : MG-AK
  Mobility Oracle : Disabled
  Mobility Oracle IP Address : 0.0.0.0
  DTLS Mode : Enabled
  Mobility Domain ID for 802.11r : 0x39b2
```
Mobility Keepalive Interval : 10
Mobility Keepalive Count : 3
Mobility Control Message DSCP Value : 48
Mobility Domain Member Count : 2
Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

<table>
<thead>
<tr>
<th>IP</th>
<th>Public IP</th>
<th>Group Name</th>
<th>Multicast IP</th>
<th>Link Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.6.136.10</td>
<td>-</td>
<td>MG-AK</td>
<td>0.0.0.0</td>
<td>UP : UP</td>
</tr>
</tbody>
</table>

Q. Multiple access points detect the same interference device. However, the switch shows them as separate clusters or different suspected devices clustered together. Why does this happen?
A. Access points must be RF neighbors for the switch to consider merging the devices that are detected by these access points. An access point takes time to establish neighbor relationships. A few minutes after the switch reboots or after there is a change in the RF group, and similar events, clustering will not be very accurate.

Q. Can I merge two monitor-mode access points using a switch?
A. No, you cannot merge two monitor-mode access points using a switch. You can merge the monitor mode access points only using MSE.

Q. How do I view neighbor access points?
A. To view neighbor access points, use the `show ap ap_name auto-rf dot11 {24ghz | 5ghz}` command.

This example shows how to display the neighbor access points:

```
Switch# show ap name AS-5508-5-AP3 auto-rf dot11 24ghz
Nearby APs
AP 0C85.259E.C350 slot 0 : -12 dBm on 1 (10.10.0.5)
AP 0C85.25AB.CCA0 slot 0 : -24 dBm on 6 (10.10.0.5)
AP 0C85.25C7.B7A0 slot 0 : -26 dBm on 11 (10.10.0.5)
AP 0C85.25DE.2C10 slot 0 : -24 dBm on 6 (10.10.0.5)
AP 0C85.25DE.C8E0 slot 0 : -14 dBm on 11 (10.10.0.5)
AP 0C85.25DF.3280 slot 0 : -31 dBm on 6 (10.10.0.5)
AP 0CD9.96BA.5600 slot 0 : -44 dBm on 6 (10.0.0.2)
AP 24B6.5734.C570 slot 0 : -48 dBm on 11 (10.0.0.2)
```

Q. What are the debug commands available for CleanAir?
A. The debug commands for CleanAir are:

```
* debug cleanair { all | error | event | internal-event | nmsp | packet }
```
Q. Why are CleanAir Alarms not generated for interferer devices?
A. Verify that the access points are CleanAir-capable and CleanAir is enabled both on the access point and the switch.

Q. Can the Cisco Catalyst 3850 Series Switches function as a Mobility Agent (MA)?
A. Yes, the Cisco Catalyst 3850 Series Switches can function as an MA.

Q. Are CleanAir configurations available on the MA?
A. From Release 3.3 SE, CleanAir configurations are available on the MA. You can use the following two CleanAir commands on the MA:

- `show ap dot11 5ghz cleanair config`
- `show ap dot11 24ghz cleanair config`

## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CleanAir commands and their details</td>
<td>CleanAir Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td></td>
<td>CleanAir Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>High Availability configurations</td>
<td>High Availability Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>High Availability commands and their details</td>
<td>High Availability Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
PART II

High Availability

• Configuring High Availability, on page 31
Configuring High Availability

- Finding Feature Information, on page 31
- Information about High Availability, on page 31
- Information About Redundancy, on page 32
- Information about Access Point Stateful Switch Over, on page 33
- Initiating Graceful Switchover, on page 34
- Configuring EtherChannels for High Availability, on page 34
- Configuring LACP, on page 35
- Troubleshooting High Availability, on page 36

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information about High Availability

The high availability feature is enabled by default when the switches are connected using the stack cable and the technology is enabled. You cannot disable it; however, you can initiate a manual graceful-switchover using the command line interface to use the high availability feature enabled in the switch.

In Cisco Wireless LAN Controllers, high availability is achieved with redundancy.

In Cisco Wireless LAN Controllers, redundancy is achieved in two ways— n+1 and AP SSO redundancy.

Keepalive messages are sent and received between the active and standby controllers.

- If the standby controller does not respond, a new standby controller is elected.
- If the active controller does not respond, the standby controller becomes the active controller.

In addition, hello messages are sent and received by all stack members.

- If a stack member does not respond, that member is removed from the stack.
• If the standby controller does not respond, a new standby controller is elected.
• If the active controller does not respond, the standby controller becomes the active controller.

Information About Redundancy

In case of n+1 redundancy, access points are configured with primary, secondary, and tertiary controllers. When the primary controller fails, depending upon the number of access points managed by a controller, the access point fails over to the secondary controller. In case of AP SSO redundancy, once the primary controller is unavailable, the access points re-discover the controller and reestablishes the CAPWAP tunnel with the secondary controller. However, all clients must disconnect and a re-authentication is performed to rejoin the controller.

You can configure primary, secondary, and tertiary controllers for a selected access point and a selected controller.

In an ideal high availability deployment, you can have access points connected to primary and secondary controllers and one controller can remain without connection to any access points. This way the controller that does not have any access points can take over when a failure occurs and resume services of active controller.

Configuring Redundancy in Access Points

You must use the commands explained in this section to configure primary, secondary, or tertiary controllers for a selected access point.

Before you begin

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command or Action</td>
</tr>
</tbody>
</table>
| **Step 1** | conf t  
**Example:**  
Controller # conf t | Configures the terminal |
| **Step 2** | ap capwap backup primary  
**Example:**  
Controller # ap capwap backup primary  
WLAN-Controller-A | Configures the primary controller for the selected access point. |
| **Step 3** | ap capwap backup secondary  
**Example:**  
Controller # ap capwap backup secondary  
WLAN-Controller-B | Configures the secondary controller for the selected access point. |
| **Step 4** | ap capwap backup tertiary  
**Example:**  
Controller # ap capwap backup tertiary  
WLAN-Controller-C | Configures the tertiary controller for the selected access point. |
What to do next

Once you complete configuration of the primary, secondary, and tertiary controllers for a selected access point, you must verify the configuration using the `show ap name AP-NAME` command. For more details on, `show ap name AP-NAME` command, see the Lightweight Access Point Configuration Guide for Cisco Wireless LAN Controller.

Configuring Heartbeat Messages

Heartbeat messages enable you to reduce the controller failure detection time. When a failure occurs, a switchover from active to hot standby happens after the controller waits for the heartbeat timer. If the controller does not function within the heartbeat time, then the standby takes over as the active controller. Ideally the access point generates three heartbeat messages within the time out value specified, and when the controller does not respond within the timeout value, the standby controller takes over as active. You can specify the timeout value depending on your network. Ideally the timer value is not a higher value as some chaos will occur while performing a switchover. This section explains on how to configure heartbeat interval between the controller and the access points using a timeout value to reduce the controller failure detection time.

Before you begin

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>conf t</code></td>
<td>Configures the terminal.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>controller # conf t</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>ap capwap timers heartbeat-timeout</code></td>
<td>Configures the heartbeat interval between the controller and access points. The timeout value ranges from 1 to 30.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>controller # ap capwap timers heartbeat-timeout</code></td>
<td></td>
</tr>
</tbody>
</table>

Information about Access Point Stateful Switch Over

An Access Point Stateful Switch Over (AP SSO) implies that all the access point sessions are switched over state-fully and the user session information is maintained during a switchover, and access points continue to operate in network with no loss of sessions, providing improved network availability. The active switch in the stack is equipped to perform all network functions, including IP functions and routing information exchange. The switch supports 1000 access points and 12000 clients.

However, all the clients are de-authenticated and need to be re-associated with the new active switch except for the locally switched clients in FlexConnect mode when a switchover occurs.

Once a redundancy pair is formed while in a stack, high availability is enabled, which includes that access points continue to remain connected during an active-to-standby switchover.
You cannot disable AP SSO while in a switch stack once the switches form a redundant pair.

After switchover new standby gets reloaded during stack formation, this is due to bulk sync failure. This is seen after reload, 2nd attempt to form stack successfully. This happens when you execute the command `exception dump device second flash` which is used to enable, dump crashfile on flash when crashinfo directory is full. When crash occurs and if there is no space left in crashinfo, it proceeds to store the fullcore or crash files into flash.

Initiating Graceful Switchover

To perform a manual switchover and to use the high availability feature enabled in the switch, execute the `redundancy force-switchover` command. This command initiates a graceful switchover from the active to the standby switch.

```
Switch# redundancy force-switchover
System configuration has been modified. Save ? [yes/no] : yes
Building configuration ...
Preparing for switchover ...
Compressed configuration from 14977 bytes to 6592 bytes[OK] This will reload the active unit and force switchover to standby[confirm] : y
```

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
</tbody>
</table>

Configuring EtherChannels for High Availability

The LAG, or an EtherChannel, bundles all the existing ports in both the standby and active units into a single logical port to provide an aggregate bandwidth of 60 Gbps. The creation of an EtherChannel enables protection against failures. The EtherChannels or LAGs created are used for link redundancy to ensure high availability of access points.

For more details on configuring EtherChannel, and Etherchannel modes, see the Layer 2 (Link Aggregation) Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)

Procedure

Step 1 Connect two switches that are in powered down state using the stack cable.
Step 2 Power up and perform a boot on both switches simultaneously or power and boot one switch.
Step 3 The switches boot up successfully, and form a high availability pair.
Step 4 Configure EtherChannel or LAG on the units.
**Step 4** Use the `show etherchannel summary` command to view the status of the configured EtherChannel. On successful configuration, all the specified ports will be bundled in a single channel and listed in the command output of `show etherchannel summary`.

**Step 5** Execute the `show ap uptime` command to verify the connected access points.

---

### Configuring LACP

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>interface port-channel number</code></td>
<td>Enters port-channel interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>interface Port-channel Po2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>lacp max-bundle number</code></td>
<td>Defines the maximum number of active bundled LACP ports allowed in a port channel. The value ranges from 1 to 8.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# <code>lacp max-bundle 6</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>lacp port-priority number</code></td>
<td>Specifies port priority to be configured on the port using LACP. The value ranges from 0 to 65535.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# <code>lacp port-priority 4</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>switchport backup interface po2</code></td>
<td>Specifies an interface as the backup interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# <code>switchport backup interface Po2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>end</code></td>
<td>Exits the interface and configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>show etherchannel summary</code></td>
<td>Displays a summary of EtherChannel properties.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>show etherchannel summary</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>show interfaces switchport backup</code></td>
<td>Displays summary of backup EtherChannel properties.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>show interfaces switchport backup</code></td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting High Availability

Access the Standby Console

You can only access the console of the active switch in a stack. To access the standby switch, use the following commands.

**Before you begin**
Use this functionality only under supervision of Cisco Support.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>service internal</code></td>
<td>Enables Cisco IOS debug commands.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# service internal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>redundancy</code></td>
<td>Enters redundancy configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# redundancy</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>main-cpu</code></td>
<td>Enters the redundancy main configuration submode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# main-cpu</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>standby console enable</code></td>
<td>Enables the standby console.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# standby console enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>exit</code></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

Before a Switchover

A switchover happens when the active switch fails; however, while performing a manual switchover, you can execute these commands to initiate a successful switchover:
After a Switchover

This section defines the steps that you must perform to ensure that successful switchover from the active to standby switch is performed. On successful switchover of the standby switch as active, all access points connected to the active need to re-join the standby (then active) switch.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show redundancy states</td>
<td>Displays the high availability role of the active and standby switches.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show redundancy states</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> show switch detail</td>
<td>Display physical property of the stack. Verify if the physical states of the stacks are &quot;Ready&quot; or &quot;Port&quot;.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show switch detail</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show platform ses states</td>
<td>Displays the sequences of the stack manager.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show platform ses states</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> show ap summary</td>
<td>Displays all the access points in the active and standby switches.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show ap summary</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show capwap detail</td>
<td>Displays the details of the CAPWAP tunnel in the active and standby switches.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show capwap detail</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show dtls database-brief</td>
<td>Displays DTLS details in the active and standby switches.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show dtls database-brief</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show power inline</td>
<td>Displays the power on Ethernet power state.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show power inline</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When a failover occurs, the standby controller must be in a standby-hot state and the redundant port in a terminal state in SSO for successful switchover to occur.</td>
</tr>
</tbody>
</table>

### After a Switchover

This section defines the steps that you must perform to ensure that successful switchover from the active to standby switch is performed. On successful switchover of the standby switch as active, all access points connected to the active need to re-join the standby (then active) switch.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show ap uptime</td>
<td>Verify if the uptime of the access point after the switchover is large enough.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show ap uptime</td>
<td></td>
</tr>
</tbody>
</table>
### Viewing Redundancy Switchover History (GUI)

**Procedure**

**Step 1**  
Click Monitor > Controller > Redundancy > States.  
The Redundancy States page is displayed. The values for the following parameters are displayed in the page:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Displays the index number of the of the redundant unit.</td>
</tr>
<tr>
<td>Previous Active</td>
<td>Displays the Switches that was active before.</td>
</tr>
<tr>
<td>Current Active</td>
<td>Displays the Switches that is currently active.</td>
</tr>
<tr>
<td>Switch Over Time</td>
<td>Displays the system time when the switchover occurs.</td>
</tr>
<tr>
<td>Switch Over Reason</td>
<td>Displays the cause of the switchover.</td>
</tr>
</tbody>
</table>

**Step 2**  
Click Apply.

### Viewing Switchover States (GUI)

**Procedure**

**Step 1**  
Click Monitor > Controller > Redundancy > States.  
The Redundancy States page is displayed. The values for the following parameters are displayed in the page:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# show ap uptime</td>
<td>Display the clients connected in the active switch.</td>
</tr>
<tr>
<td>Step 2 show wireless summary</td>
<td>Display if the client has reached the uptime.</td>
</tr>
<tr>
<td>Example: Switch# show wireless summary</td>
<td></td>
</tr>
<tr>
<td>Step 3 show wcdb database all</td>
<td>Display the power over Ethernet power state.</td>
</tr>
<tr>
<td>Example: Switch# show wcdb database all</td>
<td></td>
</tr>
<tr>
<td>Step 4 show power inline</td>
<td></td>
</tr>
<tr>
<td>Example: Switch# show power inline</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>My State</td>
<td>Shows the state of the active CPU Switch module. Values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Active</td>
</tr>
<tr>
<td></td>
<td>• Standby HOT</td>
</tr>
<tr>
<td></td>
<td>• Disable</td>
</tr>
<tr>
<td>Peer State</td>
<td>Displays the state of the peer (or standby) CPU Switch module. Values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Standby HOT</td>
</tr>
<tr>
<td></td>
<td>• Disable</td>
</tr>
<tr>
<td>Mode</td>
<td>Displays the current state of the redundancy peer. Values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Simplex— Single CPU switch module</td>
</tr>
<tr>
<td></td>
<td>• Duplex— Two CPU switch modules</td>
</tr>
<tr>
<td>Unit ID</td>
<td>Displays the unit ID of the CPU switch module.</td>
</tr>
<tr>
<td>Redundancy Mode</td>
<td>Displays the current operational redundancy mode supported on the unit.</td>
</tr>
<tr>
<td>(Operational)</td>
<td></td>
</tr>
<tr>
<td>Redundancy Mode</td>
<td>Displays the current configured redundancy mode supported on the unit.</td>
</tr>
<tr>
<td>(Configured)</td>
<td></td>
</tr>
<tr>
<td>Redundancy State</td>
<td>Displays the current functioning redundancy state of the unit. Values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• SSP</td>
</tr>
<tr>
<td></td>
<td>• Not Redundant</td>
</tr>
<tr>
<td>Manual SWACT</td>
<td>Displays whether manual switchovers have been enabled without the force option.</td>
</tr>
<tr>
<td>Communications</td>
<td>Displays whether communications are up or down between the two CPU Switch modules.</td>
</tr>
<tr>
<td>Client Count</td>
<td>Displays the number of redundancy subsystems that are registered as RF clients.</td>
</tr>
<tr>
<td>Client Notification TMR</td>
<td>Displays, in milliseconds, the time that an internal RF timer has for notifying RF client subsystems.</td>
</tr>
<tr>
<td>Keep Alive TMR</td>
<td>Displays, in milliseconds, the time interval the RF manager has for sending keep-alive messages to its peer on the standby CPU switch module.</td>
</tr>
<tr>
<td>Keep Alive Count</td>
<td>Displays the number of keep-alive messages sent without receiving a response from the standby CPU Switch module.</td>
</tr>
<tr>
<td>Keep Alive Threshold</td>
<td>Displays the threshold for declaring that interprocessor communications are down when keep-alive messages have been enabled (which is the default).</td>
</tr>
<tr>
<td>RF Debug Mask</td>
<td>Displays an internal mask used by the RF to keep track of which debug modes are on.</td>
</tr>
</tbody>
</table>

**Step 2**

Click **Apply**.
Monitoring the Switch Stack

Table 3: Commands for Displaying Stack Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show switch</td>
<td>Displays summary information about the stack, including the status of</td>
</tr>
<tr>
<td></td>
<td>provisioned switches and switches in version-mismatch mode.</td>
</tr>
<tr>
<td>show switch</td>
<td>Displays information about a specific member.</td>
</tr>
<tr>
<td>stack-member-number</td>
<td></td>
</tr>
<tr>
<td>show switch detail</td>
<td>Displays detailed information about the stack.</td>
</tr>
<tr>
<td>show switch neighbors</td>
<td>Displays the stack neighbors.</td>
</tr>
<tr>
<td>show switch stack-ports</td>
<td>Displays port information for the stack. Use the summary keyword to</td>
</tr>
<tr>
<td>[summary]</td>
<td>display the stack cable length, the stack link status, and the loopback</td>
</tr>
<tr>
<td></td>
<td>status.</td>
</tr>
<tr>
<td>show redundancy</td>
<td>Displays the redundant system and the current processor information.</td>
</tr>
<tr>
<td></td>
<td>The redundant system information includes the system uptime, standby</td>
</tr>
<tr>
<td></td>
<td>failures, switchover reason, hardware, configured and operating</td>
</tr>
<tr>
<td></td>
<td>redundancy mode. The current processor information displayed includes the</td>
</tr>
<tr>
<td></td>
<td>active location, the software state, the uptime in the current state and</td>
</tr>
<tr>
<td></td>
<td>so on.</td>
</tr>
<tr>
<td>show redundancy state</td>
<td>Displays all the redundancy states of the active and standby switches.</td>
</tr>
</tbody>
</table>

LACP Configuration: Example

This example shows how to configure LACP and to verify creation of the LACP bundle and the status:

```
Switch(config)# !
interface TenGigabitEthernet1/0/1
  switchport mode trunk
  channel-group 1 mode active
  lacp port-priority 10
  ip dhcp snooping trust

interface TenGigabitEthernet1/0/2
  switchport mode trunk
  channel-group 1 mode active
  lacp port-priority 10
  ip dhcp snooping trust

interface TenGigabitEthernet1/0/3
  switchport mode trunk
  channel-group 1 mode active
  lacp port-priority 10
  ip dhcp snooping trust

interface TenGigabitEthernet1/0/4
  switchport mode trunk
  channel-group 1 mode active
  ip dhcp snooping trust
```
! interface TenGigabitEthernet1/0/5
  switchport mode trunk
  channel-group 1 mode active
  ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/6
  switchport mode trunk
  channel-group 1 mode active
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/1
  switchport mode trunk
  channel-group 1 mode active
  lACP port-priority 10
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/2
  switchport mode trunk
  channel-group 1 mode active
  lACP port-priority 10
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/3
  switchport mode trunk
  channel-group 1 mode active
  lACP port-priority 10
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/4
  switchport mode trunk
  channel-group 1 mode active
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/5
  switchport mode trunk
  channel-group 1 mode active
  ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/6
  switchport mode trunk
  channel-group 1 mode active
  ip dhcp snooping trust
!
interface Vlan1
  no ip address
  ip igmp version 1
  shutdown
!
Switch# show etherchannel summary

Flags:  D - down            P - bundled in port-channel
              I - stand-alone  s - suspended
              H - Hot-standby (LACP only)
              R - Layer3   S - Layer2
              U - in use   f - failed to allocate aggregator

              M - not in use, minimum links not met
              u - unsuitable for bundling
              w - waiting to be aggregated
              d - default port
Number of channel-groups in use: 1
Number of aggregators: 1

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Po1(SU)</td>
<td>LACP</td>
<td>Te1/0/1(P) Te1/0/2(P) Te1/0/3(P) Te1/0/4(H) Te1/0/5(H) Te1/0/6(H) Te2/0/1(P) Te2/0/2(P) Te2/0/3(P) Te2/0/4(H) Te2/0/5(H) Te2/0/6(H)</td>
</tr>
</tbody>
</table>

This example shows the switch backup interface pairs:

Switch# show interfaces switchport backup

Switch Backup Interface Pairs:

<table>
<thead>
<tr>
<th>Active Interface</th>
<th>Backup Interface</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-channel1</td>
<td>Port-channel2</td>
<td>Active Standby/Backup Up</td>
</tr>
</tbody>
</table>

This example shows the summary of the EtherChannel configured in the switch:

Switch# show ethernet summary

Flags: D - down  P - bundled in port-channel
I - stand-alone  s - suspended
H - Hot-standby (LACP only)
R - Layer3  S - Layer2
U - in use  f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 2
Number of aggregators: 2

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Po1(SU)</td>
<td>LACP</td>
<td>Te1/0/1(P) Te1/0/2(P) Te1/0/3(P) Te1/0/4(P) Te1/0/5(P) Te1/0/6(P)</td>
</tr>
<tr>
<td>2</td>
<td>Po2(SU)</td>
<td>LACP</td>
<td>Te2/0/1(P) Te2/0/2(P) Te2/0/3(P) Te2/0/4(P) Te2/0/5(P) Te2/0/6(P)</td>
</tr>
</tbody>
</table>

Flex Link Configuration: Example

This example shows how to configure flex link and to verify creation and the status of the created link:

Switch(config)# !
interface Port-channel1
  description Ports 1-6 connected to NW-55-SW
  switchport mode trunk
  switchport backup interface Po2
  switchport backup interface Po2 preemption mode forced
  switchport backup interface Po2 preemption delay 1
  ip dhcp snooping trust
!
interface Port-channel2
  description Ports 7-12 connected to NW-55-SW
  switchport mode trunk
ip dhcp snooping trust
!
interface GigabitEthernet0/0
vrf forwarding Mgmt-vrf
no ip address
negotiation auto
!
interface TenGigabitEthernet1/0/1
switchport mode trunk
channel-group 1 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/2
switchport mode trunk
channel-group 1 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/3
switchport mode trunk
channel-group 1 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/4
switchport mode trunk
channel-group 1 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/5
switchport mode trunk
channel-group 1 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet1/0/6
switchport mode trunk
channel-group 1 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/1
switchport mode trunk
channel-group 2 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/2
switchport mode trunk
channel-group 2 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/3
switchport mode trunk
channel-group 2 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/4
switchport mode trunk
channel-group 2 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/5
switchport mode trunk
channel-group 2 mode on
ip dhcp snooping trust
!
interface TenGigabitEthernet2/0/6
switchport mode trunk
channel-group 2 mode on
ip dhcp snooping trust
!
interface Vlan1
no ip address

Switch# show etherchannel summary

Flags: D - down P - bundled in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       U - in use f - failed to allocate aggregator
       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 2
Number of aggregators: 2

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Po1(SU)</td>
<td>-</td>
<td>Te1/0/1(P) Te1/0/2(P) Te1/0/3(P) Te1/0/4(P) Te1/0/5(P) Te1/0/6(P)</td>
</tr>
<tr>
<td>2</td>
<td>Po2(SU)</td>
<td>-</td>
<td>Te2/0/1(P) Te2/0/2(P) Te2/0/3(D) Te2/0/4(P) Te2/0/5(P) Te2/0/6(P)</td>
</tr>
</tbody>
</table>
PART III

IPv6

• IPv6 Client IP Address Learning, on page 47
• Configuring IPv6 WLAN Security, on page 69
• Configuring IPv6 ACL, on page 89
• Configuring IPv6 Web Authentication, on page 107
• IPv6 Client Mobility, on page 117
• Configuring IPv6 Mobility, on page 125


IPv6 Client IP Address Learning

- Prerequisites for IPv6 Client Address Learning, on page 47
- Restrictions for IPv6 Client Address Learning, on page 47
- Information About IPv6 Client Address Learning, on page 48
- Configuring RA Guard Policy, on page 52
- Applying RA Guard Policy, on page 53
- Configuring RA Throttle Policy (CLI), on page 54
- Applying RA Throttle Policy on VLAN (CLI), on page 54
- Configuring IPv6 Snooping, on page 55
- Configuring IPv6 ND Suppress Policy, on page 56
- Configuring IPv6 Snooping on VLAN/PortChannel, on page 57
- Configuring IPv6 on Controller Interface, on page 58
- Configuring DHCP Pool, on page 59
- Configuring Stateless Auto Address Configuration Without DHCP (CLI), on page 60
- Configuring Stateless Auto Address Configuration With DHCP, on page 61
- Configuring Stateful DHCP Locally, on page 62
- Configuring Stateful DHCP Externally, on page 64
- Monitoring IPv6 Clients (GUI), on page 66
- Verifying IPv6 Address Learning Configuration, on page 66
- Additional References, on page 67
- Feature Information for IPv6 Client Address Learning, on page 68

Prerequisites for IPv6 Client Address Learning

Before configuring IPv6 client address learning, configure the wireless clients to support IPv6.

Restrictions for IPv6 Client Address Learning

There are no specific requirements for IPv6 client address learning.
Information About IPv6 Client Address Learning

Client Address Learning is configured on switch to learn the wireless client's IPv4 and IPv6 address and clients transition state maintained by the switch on an association, re-association, de-authentication and timeout.

There are three ways for IPv6 client to acquire IPv6 addresses:

- Stateless Address Auto-Configuration (SLACC)
- Stateful DHCPv6
- Static Configuration

For all of these methods, the IPv6 client always sends neighbor solicitation DAD (Duplicate Address Detection) request to ensure there is no duplicate IP address on the network. The switch snoops the client's NDP and DHCPv6 packets to learn about its client IP addresses.

SLAAC Address Assignment

The most common method for IPv6 client address assignment is Stateless Address Auto-Configuration (SLAAC). SLAAC provides simple plug-and-play connectivity where clients self-assign an address based on the IPv6 prefix. This process is achieved

Stateless Address Auto-Configuration (SLAAC) is configured as follows:

- Host sends a router solicitation message.
- Hosts waits for a Router Advertisement message.
- Hosts take the first 64 bits of the IPv6 prefix from the Router Advertisement message and combines it with the 64 bit EUI-64 address (in the case of ethernet, this is created from the MAC Address) to create a global unicast message. The host also uses the source IP address, in the IP header, of the Router Advertisement message, as its default gateway.
- Duplicate Address Detection is performed by IPv6 clients in order to ensure that random addresses that are picked do not collide with other clients.
- The choice of algorithm is up to the client and is often configurable.

The last 64 bits of the IPv6 address can be learned based on the following 2 algorithms:

- EUI-64 which is based on the MAC address of the interface, or
- Private addresses that are randomly generated.
The following Cisco IOS configuration commands from a Cisco-capable IPv6 router are used to enable SLAAC addressing and router advertisements:

```bash
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

**Stateful DHCPv6 Address Assignment**

The use of DHCPv6 is not required for IPv6 client connectivity if SLAAC is already deployed. There are two modes of operation for DHCPv6 called Stateless and Stateful.

The DHCPv6 Stateless mode is used to provide clients with additional network information that is not available in the router advertisement, but not an IPv6 address as this is already provided by SLAAC. This information can include the DNS domain name, DNS server(s), and other DHCP vendor-specific options. This interface configuration is for a Cisco IOS IPv6 router implementing stateless DHCPv6 with SLAAC enabled:

```bash
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
```
The DHCPv6 Stateful option, also known as managed mode, operates similarly to DHCPv4 in that it assigns unique addresses to each client instead of the client generating the last 64 bits of the address as in SLAAC. This interface configuration is for a Cisco IOS IPv6 router implementing stateful DHCPv6 on a local Switch:

```plaintext
dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64

domain-name cisco.com

dns-server 2001:db8:6:6::1

interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
end
```

This interface configuration is for a Cisco IOS IPv6 router implementing stateful DHCPv6 on an external DHCP server:

```plaintext
dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64

domain-name cisco.com

dns-server 2001:db8:6:6::1

interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp Relay destination 2001:DB8:0:20::2
end
```

### Static IP Address Assignment

Statically configured address on a client.

### Router Solicitation

A Router Solicitation message is issued by a host controller to facilitate local routers to transmit Router Advertisement from which it can obtain information about local routing or perform Stateless Auto-configuration. Router Advertisements are transmitted periodically and the host prompts with an immediate Router Advertisement using a Router Solicitation such as - when it boots or following a restart operation.

### Router Advertisement

A Router Advertisement message is issued periodically by a router or in response to a Router Solicitation message from a host. The information contained in these messages is used by hosts to perform Stateless Auto-configuration and to modify its routing table.
Neighbor Discovery

IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes. Neighbor Discovery replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4.

IPv6 Neighbor Discovery inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery packets that do not comply are dropped. The neighbor binding table in the controller tracks each IPv6 address and its associated MAC address. Clients are expired from the table according to Neighbor Binding timers.

Neighbor Discovery Suppression

The IPv6 addresses of wireless clients are cached by the switch. When the switch receives an NS multicast looking for an IPv6 address, and if the target address is known to the switch and belongs to one of its clients, the switch will reply with an NA message on behalf of the client. The result of this process generates the equivalent of the Address Resolution Protocol (ARP) table of IPv4 but is more efficient - uses generally fewer messages.

Note

The switch acts like proxy and respond with NA, only when the `ipv6 nd suppress` command is configured.

If the switch does not have the IPv6 address of a wireless client, the switch will not respond with NA and forward the NS packet to the wireless side. To resolve this, an NS Multicast Forwarding knob is provided. If this knob is enabled, the switch gets the NS packet for the IPv6 address that it does not have (cache miss) and forwards it to the wireless side. This packet reaches the intended wireless client and the client replies with NA.

This cache miss scenario occurs rarely, and only very few clients which do not implement complete IPv6 stack may not advertise their IPv6 address during NDP.

RA Guard

IPv6 clients configure IPv6 addresses and populate their router tables based on IPv6 router advertisement (RA) packets. The RA guard feature is similar to the RA guard feature of wired networks. RA guard increases the security of the IPv6 network by dropping the unwanted or rogue RA packets that come from wireless clients. If this feature is not configured, malicious IPv6 wireless clients announce themselves as the router for the network often with high priority, which would take higher precedence over legitimate IPv6 routers.

RA-Guard also examines the incoming RA’s and decides whether to switch or block them based solely on information found in the message or in the switch configuration. The information available in the frames received is useful for RA validation:

- Port on which the frame is received
- IPv6 source address
- Prefix list

The following configuration information created on the switch is available to RA-Guard to validate against the information found in the received RA frame:

- Trusted/Untrusted ports for receiving RA-guard messages
• Trusted/Untrusted IPv6 source addresses of RA-sender
• Trusted/Untrusted Prefix list and Prefix ranges
• Router Preference

RA guard occurs at the switch. You can configure the switch to drop RA messages at the switch. All IPv6 RA messages are dropped, which protects other wireless clients and upstream wired network from malicious IPv6 clients.

//Create a policy for RA Guard//
ipv6 nd raguard policy raguard-router
trusted-port
device-role router

//Applying the RA Guard Policy on port/interface//
interface tengigabitethernet1/0/1 (Katana)
interface gigabitethernet1/0/1 (Edison)
ipv6 nd raguard attach-policy raguard-router

**RA Throttling**

RA throttling allows the controller to enforce limits to RA packets headed toward the wireless network. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. If a client sends an RS packet, an RA is sent back to the client. This RA is allowed through the controller and unicasted to the client. This process ensures that the new clients or roaming clients are not affected by the RA throttling.

**Configuring RA Guard Policy**

Configure RA Guard policy on the switch to add IPv6 client addresses and populate the router table based on IPv6 router advertisement packets.

To configuring RA guard policy, perform this procedure:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 nd raguard policy raguard-router</td>
<td>Defines the RA guard policy name and enters RA guard policy configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Applying RA Guard Policy

Applying the RA Guard policy on the switch will block all the untrusted RA's.

To apply RA guard policy, perform this procedure:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: <code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface tengigabitethernet 1/0/1</td>
<td>Specifies an interface type and number, and places the device in interface configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Switch(config)# interface tengigabitethernet 1/0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ipv6 nd raguard attach-policy raguard-router</td>
<td>Applies the IPv6 RA Guard feature to a specified interface.</td>
</tr>
<tr>
<td>Example: <code>Switch(config-if)# ipv6 nd raguard attach-policy raguard-router</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring RA Throttle Policy (CLI)

Configure RA Throttle policy to allow the enforce the limits

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
configure terminal  
Example:  
Switch# configure terminal | Enters global configuration mode. |
| **Step 2**  
ipv6 nd ra-throttler policy ra-throttler1  
Example:  
Switch(config)# ipv6 nd ra-throttler policy ra-throttler1 | Define the router advertisement (RA) throttler policy name and enter IPv6 RA throttle policy configuration mode. |
| **Step 3**  
throttleperiod 500  
Example:  
Switch(config-nd-ra-throttle)# throttleperiod 500 | Configures the throttle period in an IPv6 RA throttler policy. |
| **Step 4**  
max-through 10  
Example:  
Switch(config-nd-ra-throttle)# max-through 500 | Limits multicast RAs per VLAN per throttle period. |
| **Step 5**  
allow-atleast 5 at-most 10  
Example:  
Switch(config-nd-ra-throttle)# allow-atleast 5 at-most 10 | Limits the number of multicast RAs per device per throttle period in an RA throttler policy. |

### Applying RA Throttle Policy on VLAN (CLI)

Applying the RA Throttle policy on a VLAN. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity.
IPv6 Snooping

IPv6 snooping must always be enabled on the switch and the controller. To configuring IPv6 snooping, perform this procedure:

**Before you begin**
Enable IPv6 on the client machine.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
- enable
- Example: Switch> enable | Enables privileged EXEC mode.
- Enter your password if prompted. |
| **Step 2**
- configure terminal
- Example: Switch# configure terminal | Enters global configuration mode. |
| **Step 3**
- vlan configuration 1
- Example: Switch(config)# vlan configuration 1 | Enters VLAN configuration mode. |
### Configuring IPv6 ND Suppress Policy

The IPv6 neighbor discovery (ND) multicast suppress feature stops as many ND multicast neighbor solicit (NS) messages as possible by dropping them (and responding to solicitations on behalf of the targets) or converting them into unicast traffic. This feature runs on a layer 2 switch or a wireless controller and is used to reduce the amount of control traffic necessary for proper link operations.

When an address is inserted into the binding table, an address resolution request sent to a multicast address is intercepted, and the device either responds on behalf of the address owner or, at layer 2, converts the request into a unicast message and forwards it to its destination.

To configure IPv6 ND suppress policy, perform this procedure:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 nd suppress policy</td>
<td>Defines the ND suppress policy name and enters ND suppress policy config</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ipv6 nd suppress policy</td>
<td></td>
</tr>
</tbody>
</table>
Configuring IPv6 Snooping on VLAN/PortChannel

Neighbor Discover (ND) suppress can be enabled or disabled on either the VLAN or a switchport.

To configure IPv6 snooping on VLAN/PortChannel, perform this procedure:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | `configure terminal` | Enters global configuration mode. |
| **Example:** | `Switch# configure terminal` | |

| **Step 3** | `vlan config901` | Creates a VLAN and enters the VLAN configuration mode. |
| **Example:** | `Switch(config)# vlan config901` | |

| **Step 4** | `ipv6 nd suppress` | Applies the IPv6 nd suppress on VLAN. |
| **Example:** | `Switch(config-vlan)# ipv6 nd suppress` | |

| **Step 5** | `end` | Exits vlan configuration mode and enters the global configuration mode. |
| **Example:** | `Switch(config-vlan)# end` | |

| **Step 6** | `interface gi1/0/1` | Creates a gigabitethernet port interface. |
| **Example:** | `Switch(config)# interface gi1/0/1` | |

| **Step 7** | `ipv6 nd suppress` | Applies the IPv6 nd suppress on the interface. |
| **Example:** | `Switch(config-vlan)# ipv6 nd suppress` | |

| **Step 8** | `end` | Exits vlan configuration mode and enters the global configuration mode. |
| **Example:** | `Switch(config-vlan)# end` | |
Configuring IPv6 on Controller Interface

To configure IPv6 on an interface, perform this procedure:

**Before you begin**
Enable IPv6 on the client and IPv6 support on the wired infrastructure.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface vlan 1</td>
<td>Creates a interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface vlan 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip address fe80::1 link-local</td>
<td>Configures IPv6 address on the interface using the link-local option.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip address</td>
<td></td>
</tr>
<tr>
<td>198.51.100.1 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ipv6 address</td>
<td></td>
</tr>
<tr>
<td>fe80::1 link-local</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ipv6 address</td>
<td></td>
</tr>
<tr>
<td>2001:DB8:0:1:FFFF:1234::5/64</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ipv6 address</td>
<td></td>
</tr>
<tr>
<td>2001:DB8:0:0:E000::F/64</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ipv6 enable</td>
<td>(Optional) Enables IPv6 on the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ipv6 enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Exits from the interface mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring DHCP Pool

To configure DHCP Pool on an interface, perform this procedure:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ipv6 dhcp pool Vlan21</td>
<td>Enters the configuration mode and configures the IPv6 DHCP pool on the Vlan.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# ipv6 dhcp pool vlan1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>address prefix 2001:DB8:0:1::FFFE:1234::/64 lifetime 300 10</td>
<td>Enters the configuration-dhcp mode and configures the address pool and its lifetime on a Vlan.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-dhcpv6)# address prefix 2001:DB8:0:1::FFFE:1234::/64 lifetime 300 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>dns-server 2001:100:0:1::1</td>
<td>Configures the DNS servers for the DHCP pool.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-dhcpv6)# dns-server 2001:20:21::1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>domain-name example.com</td>
<td>Configures the domain name to complete unqualified host names.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-dhcpv6)# domain-name example.com</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
# Configuring Stateless Auto Address Configuration Without DHCP (CLI)

To configure stateless auto address configuration without DHCP, perform this procedure:

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>interface vlan 1</code></td>
<td>Creates a interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>interface vlan 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>ip address fe80::1 link-local</code></td>
<td>Configures IPv6 address on the interface using the link-local option.</td>
</tr>
</tbody>
</table>
| **Example:** | Switch(config-if)# `ip address 198.51.100.1 255.255.255.0`  
Switch(config-if)# `ipv6 address fe80::1 link-local`  
Switch(config-if)# `ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`  
Switch(config-if)# `ipv6 address 2001:DB8:0:0:E000::F/64` | |
| **Step 5** | `ipv6 enable` | (Optional) Enables IPv6 on the interface. |
| **Example:** | Switch(config)# `ipv6 enable` | |
| **Step 6** | `no ipv6 nd managed-config-flag` | Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses. |
| **Example:** | Switch(config)# `interface vlan 1`  
Switch(config-if)# `no ipv6 nd managed-config-flag` | |
<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>no ipv6 nd other-config-flag</td>
<td>Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc).</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# no ipv6 nd other-config-flag</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

---

**Configuring Stateless Auto Address Configuration With DHCP**

To configure stateless auto address configuration with DHCP, perform this procedure:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface vlan 1</td>
<td>Creates a interface and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# interface vlan 1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip address fe80::1 link-local</td>
<td>Configures IPv6 address on the interface using the link-local option.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# ip address 198.51.100.1 255.255.255.0 Switch(config-if)# ipv6 address fe80::1 link-local Switch(config-if)# ipv6 address 2001:db8:0:1:ffff:1234::5/64 Switch(config-if)# ipv6 address 2001:db8:0:0:e000::f/64</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ipv6 enable</td>
<td>(Optional) Enables IPv6 on the interface.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# ipv6 enable</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Step 6</td>
<td>no ipv6 nd managed-config-flag</td>
<td>Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface vlan 1 Switch(config-if)# no ipv6 nd managed-config-flag</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>ipv6 nd other-config-flag</td>
<td>Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc.).</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# no ipv6 nd other-config-flag</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
<td>Exits from the interface mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring Stateful DHCP Locally

This interface configuration is for a Cisco IOS IPv6 router implementing stateful DHCPv6 on a local Switch

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 unicast-routing</td>
<td>Configures IPv6 for unicasting.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ipv6 unicast-routing</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>ipv6 dhcp pool IPv6_DHCPPPOOL</td>
<td>Enters the configuration mode and configures the IPv6 DHCP pool on the VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ipv6 dhcp pool IPv6_DHCPPPOOL</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> address prefix 2001:DB8:0:1:FFFF:1234::/64</td>
<td>Specifies the address range to provide in the pool.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> dns-server 2001:100:0:1::1</td>
<td>Provides the DNS server option to DHCP clients.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-dhcpv6)# dns-server 2001:100:0:1::1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> domain-name example.com</td>
<td>Provides the domain name option to DHCP clients.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-dhcpv6)# domain-name example.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Returns to the previous mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-dhcpv6)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> interface vlan1</td>
<td>Enters the interface mode to configure the stateful DHCP.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config)# interface vlan 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> description IPv6-DHCP-Stateful</td>
<td>Enter description for the stateful IPv6 DHCP.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-if)# description IPv6-DHCP-Stateful</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> ipv6 address 2001:DB8:0:20::1/64</td>
<td>Enters the IPv6 address for the stateful IPv6 DHCP.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-if)# ipv6 address 2001:DB8:0:20::1/64</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> ip address 192.168.20.1 255.255.255.0</td>
<td>Enters the IPv6 address for the stateful IPv6 DHCP.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-if)# ip address 192.168.20.1 255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> ipv6 nd prefix 2001:db8::/64 no-advertise</td>
<td>Configures the IPv6 routing prefix advertisement that must not be advertised.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Stateful DHCP Externally

This interface configuration is for a Cisco IOS IPv6 router implementing stateful DHCPv6 on an external DHCP server.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 unicast-routing</td>
<td>Configures the IPv6 for unicasting.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ipv6 unicast-routing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> dns-server 2001:100:0:1::1</td>
<td>Provides the DNS server option to DHCP clients.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-dhcpv6)# dns-server 2001:100:0:1::1</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>5</td>
<td>domain-name example.com</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-dhcpv6)# domain-name example.com</td>
</tr>
<tr>
<td>6</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-dhcpv6)# exit</td>
</tr>
<tr>
<td>7</td>
<td>interface vlan1</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# interface vlan 1</td>
</tr>
<tr>
<td>8</td>
<td>description IPv6-DHCP-Stateful</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# description IPv6-DHCP-Stateful</td>
</tr>
<tr>
<td>9</td>
<td>ipv6 address 2001:DB8:0:20::1/64</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# ipv6 address 2001:DB8:0:20::1/64</td>
</tr>
<tr>
<td>10</td>
<td>ip address 192.168.20.1 255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# ip address 192.168.20.1 255.255.255.0</td>
</tr>
<tr>
<td>11</td>
<td>ipv6 nd prefix 2001:db8::/64 no-advertise</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise</td>
</tr>
<tr>
<td>12</td>
<td>ipv6 nd managed-config-flag</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# ipv6 nd managed-config-flag</td>
</tr>
<tr>
<td>13</td>
<td>ipv6 nd other-config-flag</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# ipv6 nd other-config-flag</td>
</tr>
</tbody>
</table>
Monitoring IPv6 Clients (GUI)

To view the IPv6 clients associated with the Switch

Procedure

Select Monitor > Clients

The Clients page is displayed. The Clients page contains the following details:

- Client MAC Address — Displays the MAC address of the client.
- AP Name — Displays the access point name to which the client is connected to.
- WLAN — Displays the WLAN associated with the client.
- State — Displays the client authentication.
- Protocol — Displays the protocol used.

To view the client related general details, click the Client MAC Address parameter in the Clients page. The Client > Detail page displays IPv6 addresses of the client under the General tab.

Verifying IPv6 Address Learning Configuration

This example displays the output of the show ipv6 dhcp pool command. This command displays the IPv6 service configuration on the switch. The vlan 21 configured pool detail displays 6 clients that are currently using addresses from the pool.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>show ipv6 dhcp pool</td>
<td>Displays the IPv6 service configuration on the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
| Switch show ipv6 dhcp pool
DHCPv6 pool: vlan21
Address allocation prefix: 2001:DB8:0:1:FFFF:1234::/64 valid 86400
preference 86400 (6 in use, 0 conflicts)
DNS server: 2001:100:0:1::1 |                                             |
### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 command reference</td>
<td>IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>IP command reference</td>
<td>IP Command Reference (Catalyst 3850 Switches)IP Command Reference (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

#### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
Feature Information for IPv6 Client Address Learning

This table lists the features in this module and provides links to specific configuration information:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Client Address Learning Functionality</td>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring IPv6 WLAN Security

Prerequisites for IPv6 WLAN Security

A client VLAN must be mapped to the WLAN configured on the switch

Restrictions for IPv6 WLAN Security

RADIUS Server Support

If multiple RADIUS servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

Radius ACS Support

You must configure RADIUS on both your Cisco Secure Access Control Server (ACS) and your switch

RADIUS is supported on Cisco Secure ACS version 3.2 and later releases.

Information About IPv6 WLAN Security

Information About RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol that provides centralized security for users attempting to gain management access to a network. It serves as a back-end database similar to Local EAP and provides authentication and accounting services.
• Authentication—The process of verifying users when they attempt to log into the switch

Users must enter a valid username and password for the switch to authenticate users to the RADIUS server. If multiple databases are configured, then specify the sequence in which the backend database must be tried.

• Accounting—The process of recording user actions and changes.

Whenever a user successfully executes an action, the RADIUS accounting server logs the changed attributes, the user ID of the person who made the change, the remote host where the user is logged in, the date and time when the command was executed, the authorization level of the user, and a description of the action performed and the values provided. If the RADIUS accounting server is unreachable, the users can continue their sessions uninterrupted.

User Datagram Protocol—RADIUS uses User Datagram Protocol (UDP) for its transport. It maintains a database and listens on UDP port 1812 for incoming authentication requests and UDP port 1813 for incoming accounting requests. The switch, which requires access control, acts as the client and requests AAA services from the server. The traffic between the switch and the server is encrypted by an algorithm defined in the protocol and a shared secret key configured on both devices.

Configures multiple RADIUS accounting and authentication servers. For example, you can have one central RADIUS authentication server but several RADIUS accounting servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the controller automatically tries the second one, then the third one if necessary, and so on.

When RADIUS method is configured for the WLAN, the switch will use the RADIUS method configured for the WLAN. When the WLAN is configured to use local EAP, the RADIUS method configured on the WLAN points to Local. The WLAN must also be configured with the name of the local EAP profile to use.

If no RADIUS method is configured in the WLAN, the switch will use the default RADIUS method defined in global mode.

Information About Local EAP

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that maintain connectivity to wireless clients when the back-end system is disrupted or the external authentication server goes down. When you enable local EAP, the switch serves as the authentication server and the local user database, which removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP back-end database to authenticate users. Local EAP supports LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC authentication between the controller and wireless clients.

Without an EAP profile name being provided, or if a name was provided for an EAP profile that does not exist, then EAP by default allows no EAP method for local authentication.

The LDAP back-end database supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC. LEAP, EAP-FAST/MSCHAPv2, and PEAPv0. MSCHAPv2 is supported only if the LDAP server is set up to return a clear-text password.
Switch support Local EAP authentication against external LDAP databases such as Microsoft Active Directory and Novell’s eDirectory. For more information about configuring the controller for Local EAP authentication against Novell’s eDirectory, see the Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database whitepaper.

Figure 4: Local EAP Example
How to Configure IPv6 WLAN Security

Configuring Local Authentication

Creating a Local User

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>username aaa_test</td>
<td>Creates a username.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# username aaa_test</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>password 0 aaa_test</td>
<td>Assigns a password for the username.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# username aaa_test password 0 aaa_test</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Switch# configure terminal
Switch(config)# username aaa_test password 0 aaa_test
Switch(config)# end

Creating an Client VLAN and Interface

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>vlan</td>
<td>Creates a VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# vlan 137</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring an EAP Profile

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>eap profile name</td>
<td>Creates an EAP profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# eap profile wcm_eap_prof</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>method leap</td>
<td>Configures EAP-LEAP method on the profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-eap-profile)# method leap</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>method tls</td>
<td>Configures EAP-TLS method on the profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-eap-profile)# method tls</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>method peap</td>
<td>Configures PEAP method on the profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-eap-profile)# method peap</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>method fast</td>
<td>Configures EAP-FAST method on the profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-eap-profile)# method fast</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>method mschapv2</td>
<td>Configures EAP-MSCHAPV2 method on the profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-eap-profile)# method mschapv2</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>method md5</td>
<td>Configures EAP-MD5 method on the profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-eap-profile)# method md5</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>method gtc</td>
<td>Configures EAP-GTC method on the profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-eap-profile)# method gtc</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>method fast profile my-fast</td>
<td>Creates a EAP profile named my-fast.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-eap-profile)# eap method fast profile my-fast</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-eap-profile)# description my_local eap profile</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>description my_local eap profile</td>
<td>Provides a description for the local profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-eap-profile)#description my_local eap profile</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>exit</td>
<td>Exits the eap-profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-eap-profile)# exit</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>eap method fast profile myFast</td>
<td>Configures the EAP method profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config)# eap method fast profile myFast</td>
<td></td>
</tr>
</tbody>
</table>
Creating a Local Authentication Model

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>aaa new-model</td>
<td>Creates a AAA authentication model.</td>
</tr>
</tbody>
</table>

---

**Example**

Switch(config)#eap profile wcm_eap_prof
Switch(config-eap-profile)#method leap
Switch(config-eap-profile)#method tls
Switch(config-eap-profile)#method peap

Switch(config-eap-profile)#method mschav2
Switch(config-eap-profile)#method gtc
Switch(config-eap-profile)#eap method fast profile my-fast

Switch (config-eap-profile)#description my_local eap profile
Switch(config-eap-profile)# exit
Switch (config)# eap method fast profile myFast
Switch(config-eap-method-profile)#authority-id identity my_identity
Switch(config-eap-method-profile)#authority-id information my_information
Switch(config-eap-method-profile)#local-key 0 test
Switch(config-eap-method-profile)#pac-password 0 test
Switch(config-eap-method-profile)# end
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>authentication dot1x default local</strong></td>
<td>Implies that the dot1x must use the default local RADIUS when no other method is found.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa authentication dot1x default local</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>dot1x method_list local</strong></td>
<td>Assigns the local authentication for wcm_local method list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa authentication dot1x wcm_local local</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><strong>aaa authentication dot1x dot1x_name local</strong></td>
<td>Configures the local authentication for the dot1x method.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa authentication dot1x aaa_auth local</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><strong>aaa authorization credential-download name local</strong></td>
<td>Configures local database to download EAP credentials from Local/RADIUS/LDAP.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa authorization credential-download wcm_author local</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><strong>aaa local authentication auth-name authorization authorization-name</strong></td>
<td>Selects local authentication and authorization.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa local authentication wcm_local authorization wcm_author</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><strong>session ID</strong></td>
<td>Configures a session ID for AAA.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa session-id common</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><strong>dot1x system-auth-control</strong></td>
<td>Enables dot.1x system authentication control.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# dot1x system-auth-control</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

Switch(config)# aaa new-model  
Switch(config)# aaa authentication dot1x default local  
Switch(config)# aaa authentication dot1x wcm-local local  
Switch(config)# aaa authentication dot1x aaa_auth local  
Switch(config)# aaa authentication credential-download wcm_author local  
Switch(config)# aaa local authentication wcm_local authorization wcm_author
Creating a Client WLAN

This example uses 802.1x with dynamic WEP. You can use any other security mechanism supported by the wireless client and configurable on the switch.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wlan wlan name &lt;identifier&gt; SSID</td>
<td>Creates a WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# wlan wlanProfileName &lt;identifier&gt; SSID</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>broadcast-ssid</td>
<td>Configures to broadcast the SSID on a WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-wlan)# broadcast-ssid</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>no security wpa</td>
<td>Disables the wpa for WLAN to enable 802.1x.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-wlan)# no security wpa</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>security dot1x</td>
<td>Configures the 802.1x encryption security for the WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-wlan)# security dot1x</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>security dot1x authentication-list wcm-local</td>
<td>Configures the server group mapping to the WLAN for dot1x authentication.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-wlan)# security dot1x authentication-list wcm-local</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>local-auth wcm_eap_prof</td>
<td>Configures the eap profile on the WLAN for local authentication.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-wlan)# local-auth wcm_eap_profile</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>client vlan 137</td>
<td>Associates the VLAN to a WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-wlan)# client vlan 137</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Local Authentication with WPA2+AES

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>aaa new model</td>
<td>Creates a AAA authentication model.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>dot1x system-auth-control</td>
<td>Enables dot1x system authentication control.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# dot1x system-auth-control</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>aaa authentication dot1x default local</td>
<td>Configures the local authentication for the default dot1x method.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa authentication dot1x default local</td>
<td></td>
</tr>
</tbody>
</table>

---

**Example**

Switch# config terminal
Switch(config)# wlan wlanProfileName 1 ngwcSSID
Switch(config-wlan)# broadcast-ssid
Switch(config-wlan)# no security wpa
Switch(config-wlan)# security dot1x
Switch(config-wlan)# security dot1x authentication-list wcm-local
Switch(config-wlan)# local-auth wcm_eap_prof
Switch(config-wlan)# client vlan 137
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
Switch#
### Creating Client VLAN for WPA2+AES

Create a VLAN for the WPA2+AES type of local authentication. This VLAN is later mapped to a WLAN.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# dot1x system-auth-control</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa authentication dot1x default local</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa authorization credential-download default local</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa local authentication default authorization default</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# eap profile wcm_eap_profile</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# method leap</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> vlan vlan_ID</td>
<td>Creates a VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
Creating WLAN for WPA2+AES

Create a WLAN and map it to the client VLAN created for WPA2+AES.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch (config)# configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td>Switch (config)# vlan105</td>
<td></td>
</tr>
<tr>
<td>Switch (config-vlan)# exit</td>
<td></td>
</tr>
<tr>
<td>Switch (config)# interface vlan 105</td>
<td>Associates the VLAN to the interface.</td>
</tr>
<tr>
<td>Switch(config)# ip address 10.8.105.10 255.255.255.0</td>
<td>Assigns IP address to the VLAN interface.</td>
</tr>
<tr>
<td>Switch(config-if)# ipv6 address 2001:db8::10:1/64</td>
<td>Assigns IPv6 address to the VLAN interface.</td>
</tr>
<tr>
<td>Switch (config-if)# exit</td>
<td>Exits from the interface mode.</td>
</tr>
</tbody>
</table>

Switch# configure terminal
Switch(config)# vlan105
Switch (config-vlan)# exit
Switch (config)# interface vlan 105
Switch(config-if)#ip address 10.8.105.10 255.255.255.0
Switch(config-if)#ipv6 address 2001:db8::10:1/64
Switch(config-if)#exit
Switch(config)#

---

**IPv6**

Creating WLAN for WPA2+AES

Create a WLAN and map it to the client VLAN created for WPA2+AES.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch (config)# vlan105</td>
<td></td>
</tr>
<tr>
<td>Switch (config-vlan)# exit</td>
<td></td>
</tr>
<tr>
<td>Switch (config)# interface vlan 105</td>
<td>Associates the VLAN to the interface.</td>
</tr>
<tr>
<td>Switch(config)# ip address 10.8.105.10 255.255.255.0</td>
<td>Assigns IP address to the VLAN interface.</td>
</tr>
<tr>
<td>Switch(config-if)# ipv6 address 2001:db8::10:1/64</td>
<td>Assigns IPv6 address to the VLAN interface.</td>
</tr>
<tr>
<td>Switch (config-if)# exit</td>
<td>Exits from the interface mode.</td>
</tr>
</tbody>
</table>

Switch# configure terminal
Switch(config)# vlan105
Switch (config-vlan)# exit
Switch (config)# interface vlan 105
Switch(config-if)#ip address 10.8.105.10 255.255.255.0
Switch(config-if)#ipv6 address 2001:db8::10:1/64
Switch(config-if)#exit
Switch(config)#
### Configuring External RADIUS Server

#### Configuring RADIUS Authentication Server Host

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global command mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch# configure terminal
```

---

Switch# configure terminal
Switch(config)# wlan wpa2-aes-wlan 1 wpa2-aes-wlan
Switch(config-wlan)#client vlan 105
Switch(config-wlan)#local-auth wcm_eap_profile
Switch(config-wlan)#security dot1x authentication-list default
Switch(config-wlan)#no shutdown
Switch(config-wlan)#exit
```

---
### Configuring RADIUS Authentication Server Group

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong> Enters global command mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>aaa new-model</strong> Creates a AAA authentication model.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)#aaa new-model</td>
</tr>
</tbody>
</table>

---

### Configuring RADIUS Authentication Server Group

<table>
<thead>
<tr>
<th>Step 2</th>
<th>radius server One Creates a radius server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch (config)# radius server One</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>address ipv4 address auth-port auth_port_number acct-port acct_port_number Configures the IPv4 address for the radius server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>address ipv6 address auth-port auth_port_number acct-port acct_port_number Configures the IPv6 address for the radius server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port 1813</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>key 0cisco Exits from the radius server mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch (config-radius-server)# key 0 cisco</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Example: Switch (config-radius-server)# exit</td>
</tr>
</tbody>
</table>
Creating a radius server-group.

**Step 3**

Command or Action: `aaa group server radius wcm_rad`  
Example:  
```
Switch(config)# aaa group server radius wcm_rad  
Switch(config-sg-radius)#
```
Purpose: Creates a radius server-group.

**Step 4**

Command or Action: `server <ip address> auth-port 1812 acct-port 1813`  
Example:  
```
Switch(config-sg-radius)# server One auth-port 1812 acct-port 1813  
Switch(config-sg-radius)# server Two auth-port 1812 acct-port 1813  
Switch(config-sg-radius)# server Three auth-port 1812 acct-port 1813
```
Purpose: Adds servers to the radius group created in Step 3. Configures the UDP port for RADIUS accounting server and authentication server.

**Step 5**

Command or Action: `aaa authentication dot1x method_list group wcm_rad`  
Example:  
```
Switch(config)# aaa authentication dot1x method_list group wcm_rad
```
Purpose: Maps the method list to the radius group.

**Step 6**

Command or Action: `dot1x system-auth-control`  
Example:  
```
Switch(config)# dot1x system-auth-control
```
Purpose: Enables the system authorization control for the radius group.

**Step 7**

Command or Action: `aaa session-id common`  
Example:  
```
Switch(config)# aaa session-id common
```
Purpose: Ensures that all session IDs information sent out, from the radius group, for a given call are identical.

---

Switch# configure terminal  
Switch(config)# aaa new-model  
Switch(config)# aaa group server radius wcm_rad  
Switch(config-sg-radius)# server One auth-port 1812 acct-port 1813  
Switch(config-sg-radius)# server Two auth-port 1812 acct-port 1813  
Switch(config-sg-radius)# server Three auth-port 1812 acct-port 1813  
Switch(config)# aaa authentication dot1x method_list group wcm_rad  
Switch(config)# dot1x system-auth-control  
Switch(config)# aaa session-id common  
Switch(config)#

---

Creating a Client VLAN

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global command mode.</td>
</tr>
</tbody>
</table>
| Example:  
```
Switch# configure terminal
```

---

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
Creating 802.1x WLAN Using an External RADIUS Server

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Creates a VLAN and associate it to the interface.</td>
</tr>
<tr>
<td><em>vlan 137</em></td>
<td></td>
</tr>
<tr>
<td><em>Example:</em> Switch(config)# vlan 137</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 3** | Exits from the VLAN mode. |
| *exit* | |
| *Example:* Switch (config-vlan)# exit | |

| **Step 4** | Assigns a VLAN to an interface. |
| *interface vlan 137* | |
| *Example:* Switch (config)# interface vlan 137 | |

| **Step 5** | Assigns an IPv4 address to the VLAN interface. |
| *ip address 10.7.137.10 255.255.255.0* | |
| *Example:* Switch(config-if)# ip address 10.7.137.10 255.255.255.0 | |

| **Step 6** | Assigns an IPv6 address to the VLAN interface. |
| *ipv6 address 2001:db8::30:1/64* | |
| *Example:* Switch(config-if)# ipv6 address 2001:db8::30:1/64 | |

| **Step 7** | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode. |
| *end* | |
| *Example:* Switch(config)# end | |

Switch# configure terminal
Switch(config)# vlan137
Switch(config-vlan)# exit
Switch(config)# interface vlan137
Switch(config-if)# ip address 10.7.137.10 255.255.255.0
Switch(config-if)# ipv6 address 2001:db8::30:1/64
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `Switch(config)# wlan ngwc_8021x 2 ngwc_8021x` | |}

**Step 3**  
**broadcast-ssid**  
**Example:**  
`Switch(config-wlan)# broadcast-ssid`  
Configures to broadcast the SSID on WLAN.

**Step 4**  
**no security wpa**  
**Example:**  
`Switch(config-wlan)# no security wpa`  
Disables the WPA for WLAN to enable 802.1x.

**Step 5**  
**security dot1x**  
**Example:**  
`Switch(config-wlan)# security dot1x`  
Configures the 802.1x encryption security for the WLAN.

**Step 6**  
**security dot1x authentication-list wcm-rad**  
**Example:**  
`Switch(config-wlan)# security dot1x authentication-list wcm-rad`  
Configures the server group mapping to the WLAN for dot1x authentication.

**Step 7**  
**client vlan 137**  
**Example:**  
`Switch(config-wlan)# client vlan 137`  
Associates the VLAN to a WLAN.

**Step 8**  
**no shutdown**  
**Example:**  
`Switch(config-wlan)# no shutdown`  
Enables the WLAN.

**Step 9**  
**end**  
**Example:**  
`Switch(config)# end`  
Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit the global configuration mode.

**Example**  
`Switch# configure terminal  
Switch(config)# wlan ngwc_8021x 2 ngwc_8021x  
Switch(config-wlan)# broadcast-ssid  
Switch(config-wlan)# no security wpa  
Switch(config-wlan)# security dot1x  
Switch(config-wlan)# security dot1x authentication-list wcm-rad  
Switch(config-wlan)# client vlan 137  
Switch(config-wlan)# no shutdown  
Switch(config-wlan)# end`
Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 command reference</td>
<td>IPv6 Command Reference (Catalyst 3850 Switches) IPv6 Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>WLAN command reference</td>
<td>WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series) WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
Feature Information for IPv6 WLAN Security

This table lists the features in this module and provides links to specific configuration information:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 WLAN Security Functionality</td>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Feature Information for IPv6 WLAN Security
Prerequisites for Configuring IPv6 ACL

You can filter IP Version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create and apply IP Version 4 (IPv4) named ACLs. You can also create and apply input router ACLs to filter Layer 3 management traffic when the switch is running the IP base feature set.

Related Topics
Creating an IPv6 ACL, on page 93

Restrictions for Configuring IPv6 ACL

With IPv4, you can configure standard and extended numbered IP ACLs, named IP ACLs, and MAC ACLs. IPv6 supports only named ACLs.

The switch supports most of the Cisco IOS-supported IPv6 ACLs with some exceptions:

- The controller does not support routing and only inbound ACLs are supported for wireless clients.
- The switch does not support matching on these keywords: flowlabel, routing header, and undetermined-transport.
- The switch does not support reflexive ACLs (the reflect keyword).
- The switch does not apply MAC-based ACLs on IPv6 frames.
When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware forwarding (physical ports or SVIs), the switch checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.

If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the switch does not allow the ACE to be added to the ACL that is currently attached to the interface.

Information About IPv6 ACL

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs are configured on the switch and applied to the management interface, the AP-manager interface, any of the dynamic interfaces, or a WLAN to control data traffic to and from wireless clients or to the controller central processing unit (CPU) to control all traffic destined for the CPU.

An access control list (ACL) is a set of rules used to limit access to a particular interface. ACLs are configured on the switch and applied to the management interface and to any of the dynamic interfaces.

You can also create a preauthentication ACL for web authentication. Such an ACL is used to allow certain types of traffic before authentication is complete.

IPv6 ACLs support the same options as IPv4 ACLs including source, destination, source and destination ports.

---

Note

You can enable only IPv4 traffic in your network by blocking IPv6 traffic. That is, you can configure an IPv6 ACL to deny all IPv6 traffic and apply it on specific or all WLANs.

Understanding IPv6 ACLs

Controller considers the local ACL configured on the WLAN as its client ACL. It supports:

- Client ACL
- port ACL
- vlan ACL
- router ACL

The ACL's are evaluated in the above order. By default, when there is no ACL configured on the WLAN, an implicit permit-all is configured.

---

Note

Port ACL is not applicable to the WLAN.

A switch supports two types of IPv6 ACLs:
• IPv6 router ACLs are supported on outbound or inbound traffic on Layer 3 interfaces, which can be routed ports, switch virtual interfaces (SVIs), or Layer 3 EtherChannels. IPv6 router ACLs apply only to IPv6 packets that are routed.

• IPv6 port ACLs are supported on inbound traffic on Layer 2 interfaces only. IPv6 port ACLs are applied to all IPv6 packets entering the interface.

A switch running the IP base feature set supports only input router IPv6 ACLs. It does not support port ACLs or output IPv6 router ACLs.

Note

If you configure unsupported IPv6 ACLs, an error message appears and the configuration does not take affect.

The switch does not support VLAN ACLs (VLAN maps) for IPv6 traffic.

You can apply both IPv4 and IPv6 ACLs to an interface. As with IPv4 ACLs, IPv6 port ACLs take precedence over router ACLs:

• When an input router ACL and input port ACL exist in an SVI, packets received on ports to which a port ACL is applied are filtered by the port ACL. Routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.

• When an output router ACL and input port ACL exist in an SVI, packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IPv6 packets are filtered by the router ACL. Other packets are not filtered.

Note

If any port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL is used to filter packets, and any router ACLs attached to the SVI of the port VLAN are ignored.

Related Topics

Creating an IPv6 ACL, on page 93
Applying an IPv6 to an Interface, on page 97
Creating WLAN IPv6 ACL, on page 99
Displaying IPv6 ACLs, on page 99

Types of ACL

Per User IPv6 ACL

For the per-user ACL, the full access control entries (ACE) as the text strings are configured on the ACS. The ACE is not configured on the Controller. The ACE is sent to the switch in the ACCESS-Accept attribute and applies it directly for the client. When a wireless client roams into a foreign switch, the ACEs are sent to the foreign switch as an AAA attribute in the mobility Handoff message. Output direction, using per-user ACL is not supported.
Filter ID IPv6 ACL

For the filter-id ACL, the full ACEs and the \texttt{acl name(filter-id)} is configured on the switch and only the \texttt{filter-id} is configured on the ACS.

The \texttt{filter-id} is sent to the switch in the ACCESS-Accept attribute, and the switch looks up the filter-id for the ACEs, and then applies the ACEs to the client. When the client L2 roams to the foreign switch, only the filter-id is sent to the foreign switch in the mobility Handoff message. Output filtered ACL, using per-user ACL is not supported. The foreign switch has to configure the filter-id and ACEs beforehand.

Downloadable IPv6 ACL

For the downloadable ACL(dACL), the full ACEs and the \texttt{dacl} name are all configured on the ACS only.

\textbf{Note}

The controller does not configure any ACL.

The ACS sends the \texttt{dacl} name to the switch in its \texttt{ACCESS-Accept} attribute, which takes the \texttt{dacl} name and sends the \texttt{dACL} name back to the ACS, for the ACEs, using the \texttt{access-request} attribute.

The ACS responds to the corresponding ACEs of the switch in the \texttt{access-accept} attribute. When the wireless client roams to an foreign switch, only the \texttt{dacl} name is sent to the foreign switch in the mobility Handoff message. The foreign switch contacts the ACS server with the \texttt{dacl} name to retrieve the ACEs.

Configuring IPv6 ACLs

To filter IPv6 traffic, you perform these steps:

\begin{tabular}{|l|l|}
\hline
\textbf{Procedure} & \textbf{Command or Action} & \textbf{Purpose} \\
\hline
\textbf{Step 1} & Create an IPv6 ACL, and enter IPv6 access list configuration mode. & \\
\hline
\textbf{Step 2} & Configure the IPv6 ACL to block (deny) or pass (permit) traffic. & \\
\hline
\textbf{Step 3} & Apply the IPv6 ACL to the interface where the traffic needs to be filtered. & \\
\hline
\textbf{Step 4} & Apply the IPv6 ACL to an interface. For router ACLs, you must also configure an IPv6 address on the Layer 3 interface to which the ACL is applied. & \\
\hline
\end{tabular}

Default IPv6 ACL Configuration

There are no IPv6 ACLs configured or applied.
Interaction with Other Features and Switches

- If an IPv6 router ACL is configured to deny a packet, the packet is not routed. A copy of the packet is sent to the Internet Control Message Protocol (ICMP) queue to generate an ICMP unreachable message for the frame.

- If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.

- You can create both IPv4 and IPv6 ACLs on a switch or switch stack, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.

  You use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 or Layer 3 interface. If you use the wrong command to attach an ACL (for example, an IPv4 command to attach an IPv6 ACL), you receive an error message.

- You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.

- If the hardware memory is full, for any additional configured ACLs, packets are dropped to the CPU, and the ACLs are applied in software. When the hardware is full a message is printed to the console indicating the ACL has been unloaded and the packets will be dropped on the interface.

  \[\text{Note}\] Only packets of the same type as the ACL that could not be added (ipv4, ipv6, MAC) will be dropped on the interface.

How To Configure an IPv6 ACL

Creating an IPv6 ACL

To create an IPv6 ACL, perform this procedure:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Creating an IPv6 ACL

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>ipv6 access-list <em>acl_name</em></td>
</tr>
<tr>
<td>Example:</td>
<td>Use a name to define an IPv6 access list and enter IPv6 access-list configuration mode.</td>
</tr>
<tr>
<td>Switch# ipv6 access-list <em>access-list-name</em></td>
<td></td>
</tr>
</tbody>
</table>

<p>| <strong>Step 4</strong> | {deny|permit} protocol  |
| Example: | Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions: |
| {deny | permit} protocol | • For protocol, enter the name or number of an Internet protocol: ahp, esp, icmp, ipv6, pcp, step, tcp, or udp, or an integer in the range 0 to 255 representing an IPv6 protocol number. |
| {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} | • The source-ipv6-prefix/prefix-length or destination-ipv6-prefix/ prefix-length is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373). |
| [operator | [port-number]] | • Enter any as an abbreviation for the IPv6 prefix ::/0. |
| [destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} | • For host source-ipv6-address or destination-ipv6-address, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons. |
| [operator | [port-number]] | • (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range. |
| [dscp value] | If the operator follows the source-ipv6-prefix/prefix-length argument, it must match the source port. If the operator follows the destination-ipv6-prefix/prefix-length argument, it must match the destination port. |
| [fragments] | • (Optional) The port-number is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You |
| [log] | |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>can use UDP port names only when filtering UDP.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter dscp value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter fragments to check noninitial fragments. This keyword is visible only if the protocol is ipv6.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter log to cause a logging message to be sent to the console about the packet that matches the entry. Enter log-input to include the input interface in the log entry. Logging is supported only for router ACLs.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter routing to specify that IPv6 packets be routed.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter sequence value to specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter time-range name to specify the time range that applies to the deny or permit statement.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

{deny|permit} tcp

**Example:**

```
(deny | permit) tcp
(source-ipv6-prefix | any | hostsource-ipv6-address) [operator [port-number]](destination-ipv6-prefix | any | hostdestination-ipv6-address) [operator [port-number]][ack] [dscp value][established] [fin]
[log][log-input] [neq {port | protocol}] [psh] [range{port | protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]
```

(Optional) Define a TCP access list and the access conditions.

Enter tcp for Transmission Control Protocol. The parameters are the same as those described in Step 3, with these additional optional parameters:

- ack—Acknowledgment bit set.
- established—An established connection. A match occurs if the TCP datagram has the ACK or RST bits set.
- fin—Finished bit set; no more data from sender.
- neq {port | protocol}—Matches only packets that are not on a given port number.
### Command or Action

| Step 6 | \{deny|permit\} udp |
|--------|---------------------|
| Example: | {deny | permit} udp \{source-ipv6-prefix/prefix-length | any \| hostsource-ipv6-address | [port-number]] \{destination-ipv6-prefix/prefix-length | any \| hostdestination-ipv6-address \} \[operator \[port-number\]] \{dscp value \| log \| log-input \| neq \[port | protocol\] \} \{range \{port | protocol\} \} \[dscp value \| log \| log-input \| [routing] \[sequence value \] \[time-range name \] |

(Optional) Define a UDP access list and the access conditions.

Enter udp for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the operator \[port\]] port number or name must be a UDP port number or name, and the established parameter is not valid for UDP.

| Step 7 | \{deny|permit\} icmp |
|--------|---------------------|
| Example: | {deny | permit} icmp \{source-ipv6-prefix/prefix-length | any \| hostsource-ipv6-address \} \[operator \[port-number\]] \{destination-ipv6-prefix/prefix-length | any \| hostdestination-ipv6-address \} \[operator \[port-number\]] \{icmp-type \| icmp-code \| icmp-message \} \[dscp value \| log \| log-input \] \[routing] \[sequence value \] \[time-range name \] |

(Optional) Define an ICMP access list and the access conditions.

Enter icmp for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 3a, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:

- icmp-type—Enter to filter by ICMP message type, a number from 0 to 255.
- icmp-code—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.
- icmp-message—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name. To see a list of ICMP message type names and code names, use the \? key or see command reference for this release.

<table>
<thead>
<tr>
<th>Step 8</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
</tr>
</tbody>
</table>

Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.
### Applying an IPv6 to an Interface

This section describes how to apply IPv6 ACLs to network interfaces. You can apply an IPv6 ACL to outbound or inbound traffic on layer 2 and Layer 3 interfaces. You can apply IPv6 ACLs only to inbound management traffic on Layer 3 interfaces.

To control access to an interface, perform this procedure:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface_id</td>
<td>Identifies a Layer 2 interface (for port ACLs) or Layer 3 Switch Virtual interface (for router ACLs) on which to apply an access list, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# interface interface-id</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>no switchport</td>
<td>Changes the interface from Layer 2 mode (the default) to Layer 3 mode (only if applying a router ACL).</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# no switchport</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command/Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>ipv6 address ipv6_address</td>
<td>Configures an IPv6 address on a Layer 3 interface (for router ACLs).</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# ipv6 address ipv6-address</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This command is not required on Layer 2 interfaces or if the interface has already been configured with an explicit IPv6 address.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>ipv6 traffic-filter acl_name</td>
<td>Applies the access list to incoming or outgoing traffic on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# ipv6 traffic-filter access-list-name {in</td>
<td>out}</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>show running-config interface</td>
<td>Shows the configuration summary.</td>
</tr>
<tr>
<td>tenGigabitEthernet 1/0/3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# show running-config interface</td>
<td></td>
</tr>
<tr>
<td>tenGigabitEthernet 1/0/3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Building configuration ..................</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Current configuration: 98 bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>!</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface TenGigabitEthernet 1/0/3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switchport mode trunk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ipv6 traffic-filter MyFilter out</td>
<td></td>
</tr>
<tr>
<td></td>
<td>end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td>copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics
- Creating an IPv6 ACL, on page 93
- Understanding IPv6 ACLs, on page 90
- Creating WLAN IPv6 ACL, on page 99
- Displaying IPv6 ACLs, on page 99
Creating WLAN IPv6 ACL

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
</tr>
<tr>
<td>Command or Action</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Switch(config-wlan)# ipv6 traffic-filter acl acl_name
Switch(config-wlan)#ipv6 traffic-filter acl acl_name-preauth

Related Topics
- Creating an IPv6 ACL, on page 93
- Applying an IPv6 to an Interface, on page 97
- Understanding IPv6 ACLs, on page 90
- Displaying IPv6 ACLs, on page 99

Verifying IPv6 ACL

Displaying IPv6 ACLs

To display IPv6 ACLs, perform this procedure:

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
</tr>
<tr>
<td>Command or Action</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
**Configuration Examples for IPv6 ACL**

**Example: Creating an IPv6 ACL**

This example configures the IPv6 access list named CISCO. The first deny entry in the list denies all packets that have a destination TCP port number greater than 5000. The second deny entry denies packets that have a source UDP port number less than 5000. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets. The second permit entry in the list permits all other traffic. The second permit entry is necessary because an implicit deny-all condition is at the end of each IPv6 access list.

**Note** Logging is supported only on Layer 3 interfaces.

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

**Example: Applying IPv6 ACLs**

This example shows how to apply the access list Cisco to outbound traffic on a Layer 3 interface.

```
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```
Example: Displaying IPv6 ACLs

This is an example of the output from the `show access-lists` privileged EXEC command. The output shows all access lists that are configured on the switch or switch stack.

```
Switch #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

This is an example of the output from the `show ipv6 access-lists` privileged EXEC command. The output shows only IPv6 access lists configured on the switch or switch stack.

```
Switch# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30
IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

Example: Configuring RA Throttling and NS Suppression

This task describes how to create an RA throttle policy in order to help the power-saving wireless clients from being disturbed by frequent unsolicited periodic RA's. The unsolicited multicast RA is throttled by the controller.

**Before you begin**

Enable IPv6 on the client machine.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | configure terminal  
   Example:  
   Switch# configure terminal | Enters global configuration mode. |
| **Step 2** | ipv6 nd ra-throttler policy Mythrottle  
   Example:  
   Switch (config)# ipv6 nd ra-throttler policy Mythrottle | Creates a RA throttler policy called Mythrottle. |
| **Step 3** | throttle-period 20  
   Example:  
   Switch (config-nd-ra-throttle)# throttle-period 20 | Determines the time interval segment during which throttling applies. |
| **Step 4** | max-through 5  
   Example: | Determines how many initial RA's are allowed. |
### Purpose Command or Action

**Step 5**

Switch (config-nd-ra-throttle)#
max-through 5

Determines how many RA's are allowed after the initial RAs have been transmitted, until the end of the interval segment.

**Step 6**

Switch (config)# vlan configuration 100

Creates a per vlan configuration.

**Step 7**

Switch (config)# ipv6 nd suppress

Disables the neighbor discovery on the Vlan.

**Step 8**

Switch (config)# ipv6 nd ra-throttle
attach-policy_name

Enables the router advertisement throttling.

**Step 9**

Switch (config)# end

Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

## Configuring RA Guard Policy

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 nd raguard policy policy name</td>
<td></td>
</tr>
</tbody>
</table>

---

**Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E**
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> trusted-port Example: Switch(config-nd-raguard)# trusted-port</td>
<td>Configures the trusted port for the policy created above.</td>
</tr>
<tr>
<td><strong>Step 5</strong> device-role router Example: Switch(config-nd-raguard)# device-role [host</td>
<td>monitor</td>
</tr>
<tr>
<td><strong>Step 6</strong> interface interface-id Example: Switch(config)# interface tenGigabitEthernet 1/0/1</td>
<td>Configures the interface to the trusted device.</td>
</tr>
<tr>
<td><strong>Step 7</strong> ipv6 nd raguard attach-policy policy name Example: Switch(config-if)# ipv6 nd raguard attach-policy Mypolicy</td>
<td>Configures and attaches the policy to trust the RA's received from the port.</td>
</tr>
<tr>
<td><strong>Step 8</strong> vlan vlan-id Example: Switch(config)# vlan configuration 19-21,23</td>
<td>Configures the wireless client vlans.</td>
</tr>
<tr>
<td><strong>Step 9</strong> ipv6 nd suppress Example: Switch(config-vlan-config)# ipv6 nd suppress</td>
<td>Suppresses the ND messages over wireless.</td>
</tr>
<tr>
<td><strong>Step 10</strong> ipv6 snooping Example: Switch(config-vlan-config)# ipv6 snooping</td>
<td>Captures IPv6 traffic.</td>
</tr>
<tr>
<td><strong>Step 11</strong> ipv6 nd raguard attach-policy policy name Example: Switch(config-vlan-config)# ipv6 nd raguard attach-policy Mypolicy</td>
<td>Attaches the RA Guard policy to the wireless client vlans.</td>
</tr>
<tr>
<td><strong>Step 12</strong> ipv6 nd ra-throttler attach-policy policy name Example: Switch(config-vlan-config)# ipv6 nd ra-throttler attach-policy Mythrottle</td>
<td>Attaches the RA throttling policy to the wireless client vlans.</td>
</tr>
</tbody>
</table>
Configuring IPv6 Neighbor Binding

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>ipv6 neighbor binding [vlan] 19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc</td>
<td>Sets and validates the neighbor 2001:db8::25:4 only valid when transmitting on VLAN 19 through interface te1/0/3 with the source mac-address as aaa.bbb.ccc.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ipv6 neighbor binding vlan 19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc</td>
<td></td>
</tr>
</tbody>
</table>

### Additional References

#### Related Documents

- Error Message Decoder
  - [Error Message Decoder](https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi) To help you research and resolve system error messages in this release, use the Error Message Decoder tool.

#### MIBs

- **MIB**: All the supported MIBs for this release.
  - **MIBs Link**: To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: [http://www.cisco.com/go/mibs](http://www.cisco.com/go/mibs)
**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

**Feature Information for IPv6 ACLs**

This table lists the features in this module and provides links to specific configuration information:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 ACL Functionality</td>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 6

Configuring IPv6 Web Authentication

- Prerequisites for IPv6 Web Authentication, on page 107
- Restrictions for IPv6 Web Authentication, on page 107
- Information About IPv6 Web Authentication, on page 108
- How to Configure IPv6 Web Authentication, on page 109
- Verifying IPv6 Web Authentication, on page 114
- Additional References, on page 115
- Feature Information for IPv6 Web Authentication, on page 116

Prerequisites for IPv6 Web Authentication

The following configurations must be in place before you start with IPv6 Web Authentication:

- IPv6 Device Tracking.
- IPv6 DHCP Snooping.
- Disable security of type 802.1x on the wlan.
- Each WLAN must have a vlan associated to it.
- Change the default wlan setting from shutdown to no shutdown.

Related Topics

Enabling Security on the WLAN, on page 110

Restrictions for IPv6 Web Authentication

The following restrictions are implied when using IPv6 web authentication:

Related Topics

Enabling Security on the WLAN, on page 110
Information About IPv6 Web Authentication

Web authentication is a Layer 3 security feature and the switch disallows IP traffic (except DHCP and DNS-related packets) from a particular client until it supplies a valid username and password. It is a simple authentication method without the need for a supplicant or client utility. Web authentication is typically used by customers who deploy a guest-access network. Traffic from both, HTTP and HTTPS, page is allowed to display the login page.

Note

Web authentication does not provide data encryption and is typically used as simple guest access for either a hot spot or campus atmosphere, where connectivity is always a factor.

A WLAN is configured as security webauth for web based authentication. The switch supports the following types of web based authentication:

• Web Authentication – The client enters the credentials in a web page which is then validated by the Wlan controller.

• Web Consent – The Wlan controller presents a policy page with Accept/Deny buttons. Click Accept button to access the network.

A Wlan is typically configured for open authentication, that is without Layer 2 authentication, when web-based authentication mechanism is used.

Web Authentication Process

The following events occur when a WLAN is configured for web authentication:

• The user opens a web browser and enters a URL address, for example, http://www.example.com. The client sends out a DNS request for this URL to get the IP address for the destination. The switch bypasses the DNS request to the DNS server, which in turn responds with a DNS reply that contains the IP address of the destination www.example.com. This, in turn, is forwarded to the wireless clients.

• The client then tries to open a TCP connection with the destination IP address. It sends out a TCP SYN packet destined to the IP address of www.example.com.

• The switch has rules configured for the client and cannot act as a proxy for www.example.com. It sends back a TCP SYN-ACK packet to the client with source as the IP address of www.example.com. The client sends back a TCP ACK packet in order to complete the three-way TCP handshake and the TCP connection is fully established.

• The client sends an HTTP GET packet destined to www.example.com. The switch intercepts this packet and sends it for redirection handling. The HTTP application gateway prepares an HTML body and sends it back as the reply to the HTTP GET requested by the client. This HTML makes the client go to the default web-page of the switch, for example, http://<Virtual-Server-IP>/login.html.

• The client closes the TCP connection with the IP address, for example, www.example.com.

• If the client wants to go to virtual IP, the client tries to open a TCP connection with the virtual IP address of the switch. It sends a TCP SYN packet for virtual IP to the switch.
• The switch responds back with a TCP SYN-ACK and the client sends back a TCP ACK to the switch in order to complete the handshake.

• The client sends an HTTP GET for /login.html destined to virtual IP in order to request for the login page.

• This request is allowed to the web server of the switch, and the server responds with the default login page. The client receives the login page in the browser window where the user can log in.

Related Topics
- Disabling WPA, on page 109
- Enabling Security on the WLAN, on page 110
- Enabling a Parameter Map on the WLAN, on page 110
- Enabling Authentication List on WLAN, on page 111
- Configuring a Global WebAuth WLAN Parameter Map, on page 111
- Configuring the WLAN, on page 112
- Enabling IPv6 in Global Configuration Mode, on page 113
- Verifying the Parameter Map, on page 114
- Verifying Authentication List, on page 114

How to Configure IPv6 Web Authentication

Disabling WPA

Before you begin

Disable 802.1x. A typical web authentication does not use Layer 2 security. Use this configuration to remove Layer 2 security.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Creates a WLAN and assign an SSID to it.</td>
</tr>
<tr>
<td>wlan test1 2 test1</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config)# wlan test1 2 test1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Disables the WPA support for Wlan.</td>
</tr>
<tr>
<td>no security wpa</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-wlan)# no security wpa</td>
<td></td>
</tr>
</tbody>
</table>
Enabling Security on the WLAN

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Applies the parameter map to all the web-auth wans.</td>
</tr>
<tr>
<td>parameter-map type web-auth global</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config)# parameter-map type web-auth global</td>
<td></td>
</tr>
</tbody>
</table>

| Step 2 | Defines the virtual gateway IPv4 address. |
| virtual-ip ipv4 192.0.2.1 | |
| Example: Switch(config-params-parameter-map)# virtual-ip ipv4 192.0.2.1 | |

| Step 3 | Defines the virtual gateway IPv6 address. |
| virtual-ip ipv6 2001:db8::24:2 | |
| Example: Switch(config-params-parameter-map)# virtual-ip ipv6 2001:db8::24:2 | |

**Related Topics**  
Prerequisites for IPv6 Web Authentication, on page 107  
Restrictions for IPv6 Web Authentication, on page 107  
Web Authentication Process, on page 108

Enabling a Parameter Map on the WLAN

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables web authentication for the wlan and creates a parameter map.</td>
</tr>
<tr>
<td>security web-auth parameter-map &lt;mapname&gt;</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Enabling Authentication List on WLAN

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch(config-wlan)# security web-auth parameter-map webauthlistlocal</code></td>
<td>Enables web authentication for the wlan and creates a local web authentication list.</td>
</tr>
</tbody>
</table>

**Related Topics**

Web Authentication Process, on page 108

Configuring a Global WebAuth WLAN Parameter Map

Use this example to configure a global web auth WLAN and add a parameter map to it.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configures a global webauth and adds a parameter map to it.</td>
</tr>
<tr>
<td><code>parameter-map type webauth global</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch (config)# parameter-map type webauth global</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Defines a virtual gateway IP address that appears to the wireless clients for authentication.</td>
</tr>
<tr>
<td><code>virtual-ip ipv6 2001:db8:4::1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch (config-params-parameter-map)# virtual-ip ipv6 2001:db8:4::1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the global ratelimit to limit the bandwidth that the web clients can use on the switch to avoid over-flooding attacks.</td>
</tr>
<tr>
<td><code>ratelimit init-state-sessions 120</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch (config-params-parameter-map)# ratelimit init-state-sessions 120</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the WLAN

**Before you begin**

- The WLAN must have a Vlan associated with it. By default, a new Wlan is always associated with Vlan 1, which can be changed as per the configuration requirements.

- Configure and enable the WLAN to `no shutdown`. By default, the Wlan is configured with the `shutdown` parameter and is disabled.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>wlan /</code></td>
<td>Creates a wlan and assign an SSID to it.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-wlan)# wlan 1 name vicweb</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ssid vicweb</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>client vlan</code> <em>interface ID</em></td>
<td>Assigns the client to vlan interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-wlan)# client vlan VLAN0136</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>security web-auth authentication list webauthlistlocal</code></td>
<td>Configures web authentication for the wlan.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-wlan)# security web-auth authentication-list webauthlistlocal</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>security web-auth parameter-map global</code></td>
<td>Configures the parameter map on the wlan.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-wlan)# security web-auth parameter-map global</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>no  security wpa</code></td>
<td>Configures the security policy for a wlan. This enables the wlan.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-wlan)# no  security wpa</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring and Enabling the WLAN

**Step 6**

**Command or Action:** `no shutdown`  
**Purpose:** Configures and enables the WLAN.

**Example:**

```
Switch(config-wlan)# no shutdown
```

**Step 7**

**Command or Action:** `end`  
**Purpose:** Returns to privileged EXEC mode. Alternatively, you can also press `Ctrl-Z` to exit global configuration mode.

**Example:**

```
Switch(config)# end
```

### Related Topics
- Configuring a Global WebAuth WLAN Parameter Map, on page 111
- Web Authentication Process, on page 108
- Enabling IPv6 in Global Configuration Mode, on page 113

---

### Enabling IPv6 in Global Configuration Mode

Enable IPv6 in global configuration for web authentication.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><code>web-auth global</code></td>
<td>Globally configures the parameter map type as web authentication.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# parameter-map type webauth global</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><code>virtual IPv6</code></td>
<td>Selects IPv6 as the virtual IP for web authentication.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-params-parameter-map)# virtual-ip ipv6</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You can also select IPv4 as the preferred IP for web authentication.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring the WLAN, on page 112
- Web Authentication Process, on page 108
- Verifying the Parameter Map, on page 114
Verifying IPv6 Web Authentication

Verifying the Parameter Map

Use the `show running configuration` command to verify the parameter map configured for Wlan.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show running config</td>
<td>Displays the entire running configuration for the switch. Grep for parameter map to view the result.</td>
</tr>
</tbody>
</table>

```
Step 1
wlan alpha 2 alpha
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauthlistlocal
security web-auth parameter-map webparalocal
```

**Related Topics**

- [Enabling IPv6 in Global Configuration Mode](#), on page 113
- [Web Authentication Process](#), on page 108
- [Verifying Authentication List](#), on page 114

Verifying Authentication List

Use the `show running configuration` command to verify the authentication list configured for the Wlan.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show running configuration</td>
<td>Displays the Wlan configuration.</td>
</tr>
</tbody>
</table>

```
Step 1
Switch# show running-config
```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

```
Step 2
Switch(config)# end
```

```
Switch# show running-config
..................................
..................................
..................................
..................................
wlan alpha 2 alpha
```

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauthlistlocal
security web-auth parameter-map webparalocal
..................................
..................................
..................................

Related Topics
Verifying the Parameter Map, on page 114
Web Authentication Process, on page 108

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 command reference</td>
<td>IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Feature Information for IPv6 Web Authentication

This table lists the features in this module and provides links to specific configuration information:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Web Authentication Functionality</td>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
</tr>
<tr>
<td>ID and password.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
IPv6 Client Mobility

Prerequisites for IPv6 Client Mobility

To enable wireless IPv6 client connectivity, the underlying wired network must support IPv6 routing and an address assignment mechanism such as SLAAC or DHCPv6. The switch must have L2 adjacency to the IPv6 router, and the VLAN needs to be tagged when the packets enter the switch. APs do not require connectivity on an IPv6 network, as all traffic is encapsulated inside the IPv4 CAPWAP tunnel between the AP and switch.

Restrictions For IPv6 Client Mobility

When using the IPv6 Client Mobility, clients must support IPv6 with either static stateless auto configuration (such as Windows XP clients) or stateful DHCPv6 IP addressing (such as Windows 7 clients).

To allow smooth operation of stateful DHCPv6 IP addressing, you must have a switch or router that supports the DHCP for IPv6 feature (such as the switch) that is configured to act like a DHCPv6 server, or you need a dedicated server such as a Windows 2008 server with a built-in DHCPv6 server.

Information About IPv6 Client Mobility

The Switch supports IPv6 mobility for IPv6-only or dual-stack nodes. The IPv6 Client Mobility is divided into:

- Link Layer and
• Network Layer

The link layer is handled by the 802.11 protocol which enables the client to roam to any AP in the same BSS (basic service set) identified by the same SSID without losing the link layer connectivity.

However, link layer mobility is not enough to make wireless client Layer 3 applications continue to work seamlessly while roaming. Cisco IOSd’s wireless mobility module uses mobility tunneling to retain seamless connectivity for the client’s Layer 3 PoP (point of presence) when the client roams across different subnets on different switches.

IPv6 is the next-generation network layer Internet protocol intended to replace IPv4 in the TCP/IP suite of protocols. This new version increases the internet global address space to accommodate users and applications that require unique global IP addresses. IPv6 incorporates 128-bit source and destination addresses, which provide significantly more addresses than the 32-bit IPv4 addresses.

To support IPv6 clients across controllers, ICMPv6 messages must be dealt with specially to ensure the IPv6 client remains on the same Layer 3 network. The switch keeps track of IPv6 clients by intercepting the ICMPv6 messages to provide seamless mobility and protect the network from network attacks. The NDP (neighbor discovery packets) packets are converted from multicast to unicast and delivered individually per client. This unique solution ensures that Neighbor Discovery and Router Advertisement packets are not leaked across VLANs. Clients can receive specific Neighbor Discovery and Router Advertisement packets ensuring correct IPv6 addressing to avoid unnecessary multicast traffic.

The configuration for IPv6 mobility is the same as IPv4 mobility and requires no separate software on the client side to achieve seamless roaming. The switch must be part of the same mobility group. Both IPv4 and IPv6 client mobility are enabled by default.

IPv6 client mobility is used for the following:

• Retaining the client IPv6 multiple addresses in Layer-2 and Layer-3 roaming.
• IPv6 Neighbor Discovery Protocol (NDP) packet management.
• Client IPv6 addresses learning.

The configuration for IPv6 mobility in SDA wireless and Local mode is the same as of IPv4 mobility and requires no different software configuration on the client side to achieve seamless roaming. Refer to IPv4 mobility section for configuration information.

Using Router Advertisement

The Neighbor Discovery Protocol (NDP) operates in the link-layer and is responsible for the discovery of other nodes on the link. It determines the link-layer addresses of other nodes, finds the available routers, and maintains reachability information about the paths to other active neighbor nodes.

Router Advertisement (RA) is one of the IPv6 Neighbor Discovery Protocol (NDP) packets that is used by the hosts to discover available routers, acquire the network prefix to generate the IPv6 addresses, link MTU, and so on. The routers send RA on a regular basis, or in response to hosts Router Solicitation messages.

IPv6 wireless client mobility manages the IPv6 RA packet. The converged access switch forwards the link-local all-nodes multicast RA packets to the local and roaming wireless nodes mapped on same VLAN the RA was received on.
Figure 1 illustrates the link-local all-nodes multicast RA forwarding issue in the wireless node mobility.

Figure 5: Roaming Client Receiving Invalid RA from Router 2

Figure 2 illustrates how a roaming client “MN” receives RA from VLAN 200 in a foreign switch and how it acquires a new IP address and breaks into L3 mobility's point of presence.

Figure 6: Roaming Client Receives Valid RA from Router 1

Related Topics
Verifying IPv6 Client Mobility, on page 120
Monitoring IPv6 Client Mobility, on page 121

RA Throttling and NS suppression
To safeguard the power-saving wireless clients from being disturbed by frequent unsolicited periodic RAs, the controller can throttle the unsolicited multicast RA.

Related Topics
Verifying IPv6 Client Mobility, on page 120
Monitoring IPv6 Client Mobility, on page 121

IPv6 Address Learning
There are three ways for IPv6 client to acquire IPv6 addresses:
• Stateless Address Auto-Configuration (SLAAC)
• Stateful DHCPv6
• Static configuration

For these methods, the IPv6 client always sends NS DAD (duplicate address detection) to ensure that there is no duplicated IP address on the network. The switch snoops the clients NDP and DHCPv6 packets to learn about its client IP addresses and then updates the controllers database. The database then informs the controller for the clients new IP address.

Related Topics
Verifying IPv6 Client Mobility, on page 120
Monitoring IPv6 Client Mobility, on page 121

Handling Multiple IP Addresses

In the case when the new IP address is received after RUN state, whether an addition or removal, the controller updates the new IP addresses on its local database for display purposes. Essentially, the IPv6 uses the existing or same PEM state machine code flow as in IPv4. When the IP addresses are requested by external entities, for example, from Prime Infrastructure, the controller will include all the available IP addresses, IPv4 and IPv6, in the API/SPI interface to the external entities.

An IPv6 client can acquire multiple IP addresses from stack for different purposes. For example, a link-local address for link local traffic, and a routable unique local or global address.

When the client is in the DHCP request state and the controller receives the first IP address notification from the database for either an IPv4 or IPv6 address, the PEM moves the client into the RUN state.

When a new IP address is received after the RUN state, either for addition or removal, the controller updates the new IP addresses on its local database for display purposes.

When the IP addresses are requested by external entities, for example, from Prime Infrastructure, the controller provides the available IP addresses, both IPv4 and IPv6, to the external entities.

Related Topics
Verifying IPv6 Client Mobility, on page 120
Monitoring IPv6 Client Mobility, on page 121

IPv6 Configuration

The switch supports IPv6 client as seamlessly as the IPv4 clients. The administrator must manually configure the VLANs to enable the IPv6, IPv6's snooping and throttling functionality. This will enable the NDP packets to throttle between the switch and its various clients.

Related Topics
Verifying IPv6 Client Mobility, on page 120
Monitoring IPv6 Client Mobility, on page 121

Verifying IPv6 Client Mobility

The commands listed in the Table 1 applies to the IPv6 client mobility.
Table 4: Commands for Verifying IPv6 Client Mobility on Cisco 5760 WLC

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug mobility ipv6</td>
<td>Enables all the wireless client IPv6 mobility debugs.</td>
</tr>
<tr>
<td>debug client mac-address</td>
<td>Displays wireless client debugging. Enter a MAC address for debugging information.</td>
</tr>
</tbody>
</table>

Related Topics
- Using Router Advertisement, on page 118
- RA Throttling and NS suppression, on page 119
- IPv6 Address Learning, on page 119
- Handling Multiple IP Addresses, on page 120
- IPv6 Configuration, on page 120
- Monitoring IPv6 Client Mobility, on page 121

Monitoring IPv6 Client Mobility

The commands in Table 2 are used to monitor IPv6 Client mobility on the switch.

Table 5: Monitoring IPv6 Client Mobility Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless client summary</td>
<td>Displays the wireless specific configuration of active clients.</td>
</tr>
<tr>
<td>show wireless client mac-address</td>
<td>Displays the wireless specific configuration of active clients based on their MAC address.</td>
</tr>
</tbody>
</table>

Related Topics
- Verifying IPv6 Client Mobility, on page 120
- Using Router Advertisement, on page 118
- RA Throttling and NS suppression, on page 119
- IPv6 Address Learning, on page 119
- Handling Multiple IP Addresses, on page 120
- IPv6 Configuration, on page 120
Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 command reference</td>
<td>IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

### Feature Information for IPv6 Client Mobility

This table lists the features in this module and provides links to specific configuration information:
<table>
<thead>
<tr>
<th>Feature</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Client Mobility Functionality</td>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

This feature was introduced.
Feature Information for IPv6 Client Mobility
Pre-requisites for IPv6 Mobility

The mobility and its related infrastructure must be configured and ready for use.

Information About IPv6 Mobility

Mobility, or roaming, is a wireless LAN client’s ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible. This section explains how mobility works when switch are included in a wireless network.

When a wireless client associates and authenticates to an access point, the access point’s switch places an entry for that client in its client database. This entry includes the client’s MAC and IP addresses, security context and associations, quality of service (QoS) contexts, the WLAN, and the associated access point. The switch uses this information to forward frames and manage traffic to and from the wireless client.

When the wireless client moves its association from one access point to another, the switch simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well. The process becomes more complicated, however, when a client roams from an access point joined to one switch to an access point joined to a different switch. It also varies based on whether the switch are operating on the same subnet.

Inter Controller Roaming

When the client associates to an access point joined to a new switch, the new switch exchanges mobility messages with the original switch, and the client database entry is moved to the new switch if sticky anchoring is disabled.
Intra Subnet Roaming with Sticky Anchoring, and Inter Subnet Roaming

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

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

For more information on configuring mobility see, the Cisco 5700 Wireless LAN Controller Mobility Configuration Guide, Cisco IOS XE, Release 3.2SE.

How to Configure IPv6 Mobility

Monitoring IPv6 Mobility

This chapter displays the mobility related IPv6 configuration. To see the mobility related configurations refer to the Cisco 5700 Wireless LAN Controller Mobility Configuration Guide, Cisco IOS XE 3.2SE.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show ipv6 neighbors binding mac C0C1.C06B.C4E2</td>
<td>Displays the IPv6 related mobility configurations.</td>
</tr>
</tbody>
</table>

Example

Switch# show ipv6 neighbors binding mac C0C1.C06B.C4E2

Binding Table has 45 entries, 37 dynamic (limit 100)

Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP, PKT - Other Packet, API - API created

Preflevel flags (prlvl):
0001:MAC and LLA match 0002:Orig trunk 0004:Orig access
0008:Orig trusted trunk 0010:Orig trusted access 0020:DHCP assigned
0040:Cga authenticated 0080:Cert authenticated 0100:Statically assigned
<table>
<thead>
<tr>
<th>IPv6 address</th>
<th>Link-Layer addr</th>
<th>Interface</th>
<th>vlan</th>
<th>prvl</th>
<th>age</th>
<th>state</th>
</tr>
</thead>
<tbody>
<tr>
<td>L FE80:20:25::16</td>
<td>2037.064.C.BA71</td>
<td>Vl25</td>
<td>25</td>
<td>0100</td>
<td>3137mn</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>L FE80:20:24::16</td>
<td>2037.064.C.BA41</td>
<td>Vl24</td>
<td>24</td>
<td>0100</td>
<td>3137mn</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>L FE80:20:23::16</td>
<td>2037.064.C.BA44</td>
<td>Vl23</td>
<td>23</td>
<td>0100</td>
<td>3137mn</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:23::13</td>
<td>2037.0653.6BC4</td>
<td>Te1/0/1</td>
<td>23</td>
<td>0005</td>
<td>83s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:22::17</td>
<td>2037.064D.06F6</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>3mn</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>L FE80:20:22::16</td>
<td>2037.064.C.BA76</td>
<td>Vl22</td>
<td>22</td>
<td>0100</td>
<td>3137mn</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:22::13</td>
<td>2037.0653.6BF6</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>163s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:22::12</td>
<td>2037.064.C.94F6</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>23s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:21::17</td>
<td>2037.064D.06E8</td>
<td>Te1/0/1</td>
<td>21</td>
<td>0005</td>
<td>4mn</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>L FE80:20:21::16</td>
<td>2037.064.C.BA68</td>
<td>Vl21</td>
<td>21</td>
<td>0100</td>
<td>3137mn</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:21::13</td>
<td>2037.0653.6BE8</td>
<td>Te1/0/1</td>
<td>21</td>
<td>0005</td>
<td>57s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:21::12</td>
<td>2037.064.C.94E8</td>
<td>Te1/0/1</td>
<td>21</td>
<td>0005</td>
<td>4s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:21::11</td>
<td>2037.0653.6BC1</td>
<td>Te1/0/1</td>
<td>21</td>
<td>0005</td>
<td>155s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:21::10</td>
<td>2001:20:23::16</td>
<td>2037.064.C.BA44</td>
<td>Vl23</td>
<td>23</td>
<td>0100</td>
<td>3137mn</td>
</tr>
<tr>
<td>ND FE80:20:21::9</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::16</td>
<td>2037.064.C.BA76</td>
<td>Vl22</td>
<td>22</td>
<td>0100</td>
<td>3137mn</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::15</td>
<td>2001:20:21::2504</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0024</td>
<td>509mn</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::14</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::13</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::12</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::11</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::10</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::9</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::8</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::7</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::6</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::5</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::4</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::3</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::2</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::1</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
<tr>
<td>ND FE80:20:20::0</td>
<td>2001:20:22::201:13</td>
<td>Te1/0/1</td>
<td>22</td>
<td>0005</td>
<td>49s</td>
<td>REACHABLE</td>
</tr>
</tbody>
</table>
REACHABLE 108 s try 0
REACHABLE 276 s
REACHABLE 87 s try 0
ND 2001:20:21:0:1016:A333:FAD5:6E68 0021.CC73.AA17 Te1/0/1 21 0005 4mn
REACHABLE 18 s try 0
REACHABLE 61 s try 0
ND 2001:20:21:0:985:8189:9937:BB05 8CA9.8295.09CC Ca0 21 0005 135s
REACHABLE 173 s try 0
ND 2001:20:21::201:20 0021.CC73.AA17 Te1/0/1 21 0005 4mn
REACHABLE 43 s try 0
ND 2001:20:21::17 2037.064D.06E8 Te1/0/1 21 0005 4mn
REACHABLE 50 s try 0
L 2001:20:21::16 2037.064C.BA68 Vl21 21 0100 3137mn
REACHABLE
ND 2001:20:21::13 2037.0653.6BE8 Te1/0/1 21 0005 67s
REACHABLE 237 s try 0
ND 2001:20:21::12 2037.064C.94E8 Te1/0/1 21 0005 5mn
REACHABLE 512 ms try 0
ND 2001:20:21::2 0022.550E.8FC2 Te1/0/1 21 0005 12s
REACHABLE 294 s try 0

Related Topics
- [Inter Controller Roaming](#), on page 125
- [Intra Subnet Roaming with Sticky Anchoring, and Inter Subnet Roaming](#), on page 126

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 command reference</td>
<td><em><a href="%7B%7D">IPv6 Command Reference (Catalyst 3850 Switches)</a></em>, <em><a href="%7B%7D">IPv6 Command Reference (Cisco WLC 5700 Series)</a></em></td>
</tr>
<tr>
<td>Mobility configurations</td>
<td><em><a href="%7B%7D">Mobility Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</a></em>, <em><a href="%7B%7D">Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</a></em></td>
</tr>
</tbody>
</table>

#### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
</tr>
<tr>
<td>Link</td>
</tr>
<tr>
<td><a href="#">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>
### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

### Feature Information for IPv6 Mobility

This table lists the features in this module and provides links to specific configuration information:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Mobility Functionality</td>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
PART IV

Layer 2/3

• Configuring EtherChannels, on page 133
• Configuring Flex Links and the MAC Address-Table Move Update Feature, on page 173
• Configuring UniDirectional Link Detection, on page 193
Configuring EtherChannels

- Finding Feature Information, on page 133
- Restrictions for EtherChannels, on page 133
- Information About EtherChannels, on page 134
- How to Configure EtherChannels, on page 151
- Monitoring EtherChannel, PAgP, and LACP Status, on page 167
- Configuration Examples for Configuring EtherChannels, on page 168
- Additional References for EtherChannels, on page 171
- Feature Information for EtherChannels, on page 172

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for EtherChannels

The following are restrictions for EtherChannels:

- All ports in an EtherChannel must be assigned to the same VLAN or they must be configured as trunk ports.
- Layer 3 EtherChannels are not supported if running the LAN Base license feature set.
- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.
Information About EtherChannels

EtherChannel Overview

EtherChannel provides fault-tolerant high-speed links between switches, routers, and servers. You can use the EtherChannel to increase the bandwidth between the wiring closets and the data center, and you can deploy it anywhere in the network where bottlenecks are likely to occur. EtherChannel provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, EtherChannel redirects traffic from the failed link to the remaining links in the channel without intervention.

An EtherChannel consists of individual Ethernet links bundled into a single logical link.

Figure 7: Typical EtherChannel Configuration

Each EtherChannel can consist of up to eight compatibly configured Ethernet ports.

The number of EtherChannels is limited to 128.

All ports in each EtherChannel must be configured as either Layer 2 or Layer 3 ports. The EtherChannel Layer 3 ports are made up of routed ports. Routed ports are physical ports configured to be in Layer 3 mode by using the `no switchport` interface configuration command. For more information, see the Configuring Interface Characteristics chapter.

Related Topics

- Configuring Layer 2 EtherChannels (CLI), on page 151
- EtherChannel Configuration Guidelines, on page 147
- Default EtherChannel Configuration, on page 146
- Layer 2 EtherChannel Configuration Guidelines, on page 148

EtherChannel Modes

You can configure an EtherChannel in one of these modes: Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or On. Configure both ends of the EtherChannel in the same mode:
• When you configure one end of an EtherChannel in either PAgP or LACP mode, the system negotiates with the other end of the channel to determine which ports should become active. If the remote port cannot negotiate an EtherChannel, the local port is put into an independent state and continues to carry data traffic as would any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.

• When you configure an EtherChannel in the on mode, no negotiations take place. The switch forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch) must also be configured in the on mode; otherwise, packet loss can occur.

Related Topics
Configuring Layer 2 EtherChannels (CLI), on page 151
EtherChannel Configuration Guidelines, on page 147
Default EtherChannel Configuration, on page 146
Layer 2 EtherChannel Configuration Guidelines, on page 148

EtherChannel on Switches

You can create an EtherChannel on a switch, on a single switch in the stack, or on multiple switches in the stack (known as cross-stack EtherChannel).

Figure 8: Single-Switch EtherChannel

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
This figure shows the recommended cross-stack EtherChannel configuration with three active links and three standby links.

Related Topics
Configuring Layer 2 EtherChannels (CLI), on page 151
EtherChannel Configuration Guidelines, on page 147
EtherChannel Link Failover

If a link within an EtherChannel fails, traffic previously carried over that failed link moves to the remaining links within the EtherChannel. If traps are enabled on the switch, a trap is sent for a failure that identifies the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

Related Topics
- Configuring Layer 2 EtherChannels (CLI), on page 151
- EtherChannel Configuration Guidelines, on page 147
- Default EtherChannel Configuration, on page 146
- Layer 2 EtherChannel Configuration Guidelines, on page 148

Channel Groups and Port-Channel Interfaces

An EtherChannel comprises a channel group and a port-channel interface. The channel group binds physical ports to the port-channel interface. Configuration changes applied to the port-channel interface apply to all the physical ports bound together in the channel group.

Figure 12: Relationship of Physical Ports, Channel Group and Port-Channel Interface

The **channel-group** command binds the physical port and the port-channel interface together. Each EtherChannel has a port-channel logical interface numbered from 1 to 128. This port-channel interface number corresponds to the one specified with the **channel-group** interface configuration command.

- With Layer 2 ports, use the **channel-group** interface configuration command to dynamically create the port-channel interface.

You also can use the **interface port-channel** port-channel-number global configuration command to manually create the port-channel interface, but then you must use the **channel-group** channel-group-number command to bind the logical interface to a physical port. The **channel-group-number** can be the same as the **port-channel-number**, or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.
• With Layer 3 ports, you should manually create the logical interface by using the `interface port-channel` global configuration command followed by the `no switchport` interface configuration command. You then manually assign an interface to the EtherChannel by using the `channel-group` interface configuration command.

• With Layer 3 ports, use the `no switchport` interface command to configure the interface as a Layer 3 interface, and then use the `channel-group` interface configuration command to dynamically create the port-channel interface.

Related Topics
- Creating Port-Channel Logical Interfaces (CLI)
- EtherChannel Configuration Guidelines, on page 147
- Default EtherChannel Configuration, on page 146
- Layer 2 EtherChannel Configuration Guidelines, on page 148
- Configuring the Physical Interfaces (CLI)

**Port Aggregation Protocol**

The Port Aggregation Protocol (PAgP) is a Cisco-proprietary protocol that can be run only on Cisco switches and on those switches licensed by vendors to support PAgP. PAgP facilitates the automatic creation of EtherChannels by exchanging PAgP packets between Ethernet ports. PAgP can be enabled on cross-stack EtherChannels.

By using PAgP, the switch or switch stack learns the identity of partners capable of supporting PAgP and the capabilities of each port. It then dynamically groups similarly configured ports (on a single switch in the stack) into a single logical link (channel or aggregate port). Similarly configured ports are grouped based on hardware, administrative, and port parameter constraints. For example, PAgP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, PAgP adds the group to the spanning tree as a single switch port.

**PAgP Modes**

PAgP modes specify whether a port can send PAgP packets, which start PAgP negotiations, or only respond to PAgP packets received.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Places a port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. This setting minimizes the transmission of PAgP packets.</td>
</tr>
<tr>
<td>desirable</td>
<td>Places a port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets. This mode is supported when the EtherChannel members are from different switches in the switch stack (cross-stack EtherChannel).</td>
</tr>
</tbody>
</table>

Switch ports exchange PAgP packets only with partner ports configured in the `auto` or `desirable` modes. Ports configured in the `on` mode do not exchange PAgP packets.

Both the `auto` and `desirable` modes enable ports to negotiate with partner ports to form an EtherChannel based on criteria such as port speed. and for Layer 2 EtherChannels, based on trunk state and VLAN numbers.
Ports can form an EtherChannel when they are in different PAgP modes as long as the modes are compatible. For example:

- A port in the **desirable** mode can form an EtherChannel with another port that is in the **desirable** or **auto** mode.
- A port in the **auto** mode can form an EtherChannel with another port in the **desirable** mode.

A port in the **auto** mode cannot form an EtherChannel with another port that is also in the **auto** mode because neither port starts PAgP negotiation.

### Related Topics
- Configuring Layer 2 EtherChannels (CLI), on page 151
- EtherChannel Configuration Guidelines, on page 147
- Default EtherChannel Configuration, on page 146
- Layer 2 EtherChannel Configuration Guidelines, on page 148
- Creating Port-Channel Logical Interfaces (CLI)
- Configuring the Physical Interfaces (CLI)

#### Silent Mode

If your switch is connected to a partner that is PAgP-capable, you can configure the switch port for nonsilent operation by using the **non-silent** keyword. If you do not specify **non-silent** with the **auto** or **desirable** mode, silent mode is assumed.

Use the silent mode when the switch is connected to a device that is not PAgP-capable and seldom, if ever, sends packets. An example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port connected to a silent partner prevents that switch port from ever becoming operational. However, the silent setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission.

### Related Topics
- Configuring Layer 2 EtherChannels (CLI), on page 151
- EtherChannel Configuration Guidelines, on page 147
- Default EtherChannel Configuration, on page 146
- Layer 2 EtherChannel Configuration Guidelines, on page 148
- Creating Port-Channel Logical Interfaces (CLI)
- Configuring the Physical Interfaces (CLI)

#### PAgP Learn Method and Priority

Network devices are classified as PAgP physical learners or aggregate-port learners. A device is a physical learner if it learns addresses by physical ports and directs transmissions based on that knowledge. A device is an aggregate-port learner if it learns addresses by aggregate (logical) ports. The learn method must be configured the same at both ends of the link.

When a device and its partner are both aggregate-port learners, they learn the address on the logical port-channel. The device sends packets to the source by using any of the ports in the EtherChannel. With aggregate-port learning, it is not important on which physical port the packet arrives.

PAgP cannot automatically detect when the partner device is a physical learner and when the local device is an aggregate-port learner. Therefore, you must manually set the learning method on the local device to learn
addresses by physical ports. You also must set the load-distribution method to source-based distribution, so that any given source MAC address is always sent on the same physical port.

You also can configure a single port within the group for all transmissions and use other ports for hot-standby. The unused ports in the group can be swapped into operation in just a few seconds if the selected single port loses hardware-signal detection. You can configure which port is always selected for packet transmission by changing its priority with the `pagp port-priority` interface configuration command. The higher the priority, the more likely that the port will be selected.

**Note**
The switch supports address learning only on aggregate ports even though the `physical-port` keyword is provided in the CLI. The `pagp learn-method` command and the `pagp port-priority` command have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner of the switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the `pagp learn-method physical-port` interface configuration command. Set the load-distribution method based on the source MAC address by using the `port-channel load-balance src-mac` global configuration command. The switch then sends packets to the physical learner using the same port in the EtherChannel from which it learned the source address. Only use the `pagp learn-method` command in this situation.

**Related Topics**
- Configuring the PAgP Learn Method and Priority (CLI), on page 158
- EtherChannel Configuration Guidelines, on page 147
- Default EtherChannel Configuration, on page 146
- Monitoring EtherChannel, PAgP, and LACP Status, on page 167
- Layer 2 EtherChannel Configuration Guidelines, on page 148

**PAgP Interaction with Other Features**

The Dynamic Trunking Protocol (DTP) and the Cisco Discovery Protocol (CDP) send and receive packets over the physical ports in the EtherChannel. Trunk ports send and receive PAgP protocol data units (PDUs) on the lowest numbered VLAN.

In Layer 2 EtherChannels, the first port in the channel that comes up provides its MAC address to the EtherChannel. If this port is removed from the bundle, one of the remaining ports in the bundle provides its MAC address to the EtherChannel. For Layer 3 EtherChannels, the MAC address is allocated by the active switch as soon as the interface is created (through the `interface port-channel` global configuration command).

PAgP sends and receives PAgP PDUs only from ports that are up and have PAgP enabled for the auto or desirable mode.

**Link Aggregation Control Protocol**

The LACP is defined in IEEE 802.3ad and enables Cisco switches to manage Ethernet channels between switches that conform to the IEEE 802.3ad protocol. LACP facilitates the automatic creation of EtherChannels by exchanging LACP packets between Ethernet ports.

By using LACP, the switch or switch stack learns the identity of partners capable of supporting LACP and the capabilities of each port. It then dynamically groups similarly configured ports into a single logical link (channel or aggregate port). Similarly configured ports are grouped based on hardware, administrative, and
port parameter constraints. For example, LACP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, LACP adds the group to the spanning tree as a single switch port.

The independent mode behavior of ports in a port channel is changed. With CSCtn96950, by default, standalone mode is enabled. When no response is received from an LACP peer, ports in the port channel are moved to suspended state.

**LACP Modes**

LACP modes specify whether a port can send LACP packets or only receive LACP packets.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Places a port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.</td>
</tr>
<tr>
<td>passive</td>
<td>Places a port into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation. This setting minimizes the transmission of LACP packets.</td>
</tr>
</tbody>
</table>

Both the *active* and *passive* LACP modes enable ports to negotiate with partner ports to an EtherChannel based on criteria such as port speed, and for Layer 2 EtherChannels, based on trunk state and VLAN numbers.

Ports can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- A port in the *active* mode can form an EtherChannel with another port that is in the *active* or *passive* mode.
- A port in the *passive* mode cannot form an EtherChannel with another port that is also in the *passive* mode because neither port starts LACP negotiation.

**Related Topics**

- Configuring Layer 2 EtherChannels (CLI), on page 151
- EtherChannel Configuration Guidelines, on page 147
- Default EtherChannel Configuration, on page 146
- Layer 2 EtherChannel Configuration Guidelines, on page 148

**LACP and Link Redundancy**

LACP port-channel operation, bandwidth availability, and link redundancy can be further refined with the LACP port-channel min-links and the LACP max-bundle features.

The LACP port-channel min-links feature:

- Configures the minimum number of ports that must be linked up and bundled in the LACP port channel.
- Prevents a low-bandwidth LACP port channel from becoming active.
- Causes an LACP port channel to become inactive if there are too few active members ports to supply the required minimum bandwidth.
The LACP max-bundle feature:

- Defines an upper limit on the number of bundled ports in an LACP port channel.
- Allows hot-standby ports with fewer bundled ports. For example, in an LACP port channel with five ports, you can specify a max-bundle of three, and the two remaining ports are designated as hot-standby ports.

**Related Topics**

- Configuring the LACP Max Bundle Feature (CLI), on page 160
- Configuring LACP Hot-Standby Ports: Example, on page 170
- Configuring the LACP Port Channel Min-Links Feature (CLI), on page 161

**LACP Interaction with Other Features**

The DTP and the CDP send and receive packets over the physical ports in the EtherChannel. Trunk ports send and receive LACP PDUs on the lowest numbered VLAN.

In Layer 2 EtherChannels, the first port in the channel that comes up provides its MAC address to the EtherChannel. If this port is removed from the bundle, one of the remaining ports in the bundle provides its MAC address to the EtherChannel. For Layer 3 EtherChannels, the MAC address is allocated by the active switch as soon as the interface is created through the `interface port-channel` global configuration command.

LACP sends and receives LACP PDUs only from ports that are up and have LACP enabled for the active or passive mode.

**EtherChannel On Mode**

EtherChannel `on` mode can be used to manually configure an EtherChannel. The `on` mode forces a port to join an EtherChannel without negotiations. The `on` mode can be useful if the remote device does not support PAgP or LACP. In the `on` mode, a usable EtherChannel exists only when the switches at both ends of the link are configured in the `on` mode.

Ports that are configured in the `on` mode in the same channel group must have compatible port characteristics, such as speed and duplex. Ports that are not compatible are suspended, even though they are configured in the `on` mode.

**Caution**

You should use care when using the `on` mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

**Load-Balancing and Forwarding Methods**

EtherChannel balances the traffic load across the links in a channel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel. You can specify one of several different load-balancing modes, including load distribution based on MAC addresses, IP addresses, source addresses, destination addresses, or both source and destination addresses. The selected mode applies to all EtherChannels configured on the switch.
Layer 3 Equal-cost multi path (ECMP) load balancing is based on source IP address, destination IP address, source port, destination port, and layer 4 protocol. Fragmented packets will be treated on two different links based on the algorithm calculated using these parameters. Any changes in one of these parameters will result in load balancing.

You configure the load-balancing and forwarding method by using the `port-channel load-balance` and the `port-channel load-balance extended` global configuration commands.

### Related Topics
- Configuring EtherChannel Load-Balancing (CLI), on page 155
- EtherChannel Configuration Guidelines, on page 147
- Layer 2 EtherChannel Configuration Guidelines, on page 148
- Default EtherChannel Configuration, on page 146
- Layer 3 EtherChannel Configuration Guidelines, on page 149

### MAC Address Forwarding

With source-MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the source-MAC address of the incoming packet. Therefore, to provide load-balancing, packets from different hosts use different ports in the channel, but packets from the same host use the same port in the channel.

With destination-MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the destination host’s MAC address of the incoming packet. Therefore, packets to the same destination are forwarded over the same port, and packets to a different destination are sent on a different port in the channel.

With source-and-destination MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on both the source and destination MAC addresses. This forwarding method, a combination source-MAC and destination-MAC address forwarding methods of load distribution, can be used if it is not clear whether source-MAC or destination-MAC address forwarding is better suited on a particular switch. With source-and-destination MAC-address forwarding, packets sent from host A to host B, host A to host C, and host C to host B could all use different ports in the channel.

### Related Topics
- Configuring EtherChannel Load-Balancing (CLI), on page 155
- EtherChannel Configuration Guidelines, on page 147
- Layer 2 EtherChannel Configuration Guidelines, on page 148
- Default EtherChannel Configuration, on page 146
- Layer 3 EtherChannel Configuration Guidelines, on page 149

### IP Address Forwarding

With source-IP address-based forwarding, packets are distributed across the ports in the EtherChannel based on the source-IP address of the incoming packet. To provide load balancing, packets from different IP addresses use different ports in the channel, and packets from the same IP address use the same port in the channel.

With destination-IP address-based forwarding, packets are distributed across the ports in the EtherChannel based on the destination-IP address of the incoming packet. To provide load balancing, packets from the same IP source address sent to different IP destination addresses could be sent on different ports in the channel.
Packets sent from different source IP addresses to the same destination IP address are always sent on the same port in the channel.

With source-and-destination IP address-based forwarding, packets are distributed across the ports in the EtherChannel based on both the source and destination IP addresses of the incoming packet. This forwarding method, a combination of source-IP and destination-IP address-based forwarding, can be used if it is not clear whether source-IP or destination-IP address-based forwarding is better suited on a particular switch. In this method, packets sent from the IP address A to IP address B, from IP address A to IP address C, and from IP address C to IP address B could all use different ports in the channel.

**Related Topics**

- Configuring EtherChannel Load-Balancing (CLI), on page 155
- EtherChannel Configuration Guidelines, on page 147
- Layer 2 EtherChannel Configuration Guidelines, on page 148
- Default EtherChannel Configuration, on page 146
- Layer 3 EtherChannel Configuration Guidelines, on page 149

### Load-Balancing Advantages

Different load-balancing methods have different advantages, and the choice of a particular load-balancing method should be based on the position of the switch in the network and the kind of traffic that needs to be load-distributed.

**Figure 13: Load Distribution and Forwarding Methods**

In the following figure, an EtherChannel of four workstations communicates with a router. Because the router is a single MAC-address device, source-based forwarding on the switch EtherChannel ensures that the switch uses all available bandwidth to the router. The router is configured for destination-based forwarding because the large number of workstations ensures that the traffic is evenly distributed from the router EtherChannel.
In the figure below the controller does source MAC-based forwarding over the EtherChannel links and evenly distributes the traffic over multiple links of the EtherChannel.

Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel is going only to a single MAC address, using the destination-MAC address always chooses the same link in the channel. Using source addresses or IP addresses might result in better load-balancing.

**Related Topics**
- Configuring EtherChannel Load-Balancing (CLI), on page 155
- EtherChannel Configuration Guidelines, on page 147
- Layer 2 EtherChannel Configuration Guidelines, on page 148
- Default EtherChannel Configuration, on page 146
- Layer 3 EtherChannel Configuration Guidelines, on page 149

**EtherChannel and Switch Stacks**

If a stack member that has ports participating in an EtherChannel fails or leaves the stack, the active switch removes the failed stack member switch ports from the EtherChannel. The remaining ports of the EtherChannel, if any, continue to provide connectivity.

When a switch is added to an existing stack, the new switch receives the running configuration from the active switch and updates itself with the EtherChannel-related stack configuration. The stack member also receives the operational information (the list of ports that are up and are members of a channel).

When two stacks merge that have EtherChannels configured between them, self-looped ports result. Spanning tree detects this condition and acts accordingly. Any PAgP or LACP configuration on a winning switch stack is not affected, but the PAgP or LACP configuration on the losing switch stack is lost after the stack reboots.

**Switch Stack and PAgP**

With PAgP, if the active switch fails or leaves the stack, the standby switch becomes the new active switch. A spanning-tree reconvergence is not triggered unless there is a change in the EtherChannel bandwidth. The new active switch synchronizes the configuration of the stack members to that of the active switch. The PAgP
configuration is not affected after an active switch change unless the EtherChannel has ports residing on the old active switch.

**Switch Stacks and LACP**

With LACP, the system ID uses the stack MAC address from the active switch. When an active switch fails or leaves the stack and the standby switch becomes the new active switch change, the LACP system ID is unchanged. By default, the LACP configuration is not affected after the active switch changes.

**Default EtherChannel Configuration**

The default EtherChannel configuration is described in this table.

*Table 8: Default EtherChannel Configuration*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel groups</td>
<td>None assigned.</td>
</tr>
<tr>
<td>Port-channel logical interface</td>
<td>None defined.</td>
</tr>
<tr>
<td>PAgP mode</td>
<td>No default.</td>
</tr>
<tr>
<td>PAgP learn method</td>
<td>Aggregate-port learning on all ports.</td>
</tr>
<tr>
<td>PAgP priority</td>
<td>128 on all ports.</td>
</tr>
<tr>
<td>LACP mode</td>
<td>No default.</td>
</tr>
<tr>
<td>LACP learn method</td>
<td>Aggregate-port learning on all ports.</td>
</tr>
<tr>
<td>LACP port priority</td>
<td>32768 on all ports.</td>
</tr>
<tr>
<td>LACP system priority</td>
<td>32768.</td>
</tr>
<tr>
<td>LACP system ID</td>
<td>LACP system priority and the switch or stack MAC address.</td>
</tr>
<tr>
<td>Load-balancing</td>
<td>Load distribution on the switch is based on the source-MAC address of the incoming packet.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring Layer 2 EtherChannels (CLI), on page 151
- EtherChannel Overview, on page 134
- EtherChannel Modes, on page 134
- EtherChannel on Switches, on page 135
- EtherChannel Link Failover, on page 137
- LACP Modes, on page 141
- PAgP Modes, on page 138
- Silent Mode, on page 139
- Creating Port-Channel Logical Interfaces (CLI)
- Channel Groups and Port-Channel Interfaces, on page 137
EtherChannel Configuration Guidelines

If improperly configured, some EtherChannel ports are automatically disabled to avoid network loops and other problems. Follow these guidelines to avoid configuration problems:

- Configure a PAgP EtherChannel with up to eight Ethernet ports of the same type.
- Configure a LACP EtherChannel with up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.
- Configure all ports in an EtherChannel to operate at the same speeds and duplex modes.
- Enable all ports in an EtherChannel. A port in an EtherChannel that is disabled by using the `shutdown` interface configuration command is treated as a link failure, and its traffic is transferred to one of the remaining ports in the EtherChannel.
- When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, you must also make the changes to all ports in the group:
  - Allowed-VLAN list
  - Spanning-tree path cost for each VLAN
  - Spanning-tree port priority for each VLAN
  - Spanning-tree Port Fast setting
- Do not configure a port to be a member of more than one EtherChannel group.
- Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch or on different switches in the stack. Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.
- Do not configure a secure port as part of an EtherChannel or the reverse.
- Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x on an EtherChannel port, an error message appears, and IEEE 802.1x is not enabled.
- If EtherChannels are configured on switch interfaces, remove the EtherChannel configuration from the interfaces before globally enabling IEEE 802.1x on a switch by using the `dot1x system-auth-control` global configuration command.
• If cross-stack EtherChannel is configured and the switch stack partitions, loops and forwarding issues can occur.

Related Topics
- Configuring Layer 2 EtherChannels (CLI), on page 151
- EtherChannel Overview, on page 134
- EtherChannel Modes, on page 134
- EtherChannel on Switches, on page 135
- EtherChannel Link Failover, on page 137
- LACP Modes, on page 141
- PAgP Modes, on page 138
- Silent Mode, on page 139
- Creating Port-Channel Logical Interfaces (CLI)
- Channel Groups and Port-Channel Interfaces, on page 137
- Configuring the Physical Interfaces (CLI)
- Configuring EtherChannel Load-Balancing (CLI), on page 155
- Load-Balancing and Forwarding Methods, on page 142
- MAC Address Forwarding, on page 143
- IP Address Forwarding, on page 143
- Load-Balancing Advantages, on page 144
- Configuring the PAgP Learn Method and Priority (CLI), on page 158
- PAgP Learn Method and Priority, on page 139
- Configuring the LACP System Priority (CLI), on page 162
- Configuring the LACP Port Priority (CLI), on page 163

Layer 2 EtherChannel Configuration Guidelines

When configuring Layer 2 EtherChannels, follow these guidelines:
• Assign all ports in the EtherChannel to the same VLAN, or configure them as trunks. Ports with different native VLANs cannot form an EtherChannel.

• An EtherChannel supports the same allowed range of VLANs on all the ports in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the ports do not form an EtherChannel even when PAgP is set to the auto or desirable mode.

• Ports with different spanning-tree path costs can form an EtherChannel if they are otherwise compatibly configured. Setting different spanning-tree path costs does not, by itself, make ports incompatible for the formation of an EtherChannel.

Related Topics
- Configuring Layer 2 EtherChannels (CLI), on page 151
- EtherChannel Overview, on page 134
- EtherChannel Modes, on page 134
- EtherChannel on Switches, on page 135
- EtherChannel Link Failover, on page 137
- LACP Modes, on page 141
- PAgP Modes, on page 138
Layer 3 EtherChannel Configuration Guidelines

- For Layer 3 EtherChannels, assign the Layer 3 address to the port-channel logical interface, not to the physical ports in the channel.

Related Topics
- Configuring EtherChannel Load-Balancing (CLI), on page 155
- Load-Balancing and Forwarding Methods, on page 142
- MAC Address Forwarding, on page 143
- IP Address Forwarding, on page 143
- Load-Balancing Advantages, on page 144

Auto-LAG

The auto-LAG feature provides the ability to auto create EtherChannels on ports connected to a switch. By default, auto-LAG is disabled globally and is enabled on all port interfaces. The auto-LAG applies to a switch only when it is enabled globally.

On enabling auto-LAG globally, the following scenarios are possible:

- All port interfaces participate in creation of auto EtherChannels provided the partner port interfaces have EtherChannel configured on them. For more information, see the "The supported auto-LAG configurations between the actor and partner devices" table below.

- Ports that are already part of manual EtherChannels cannot participate in creation of auto EtherChannels.

- When auto-LAG is disabled on a port interface that is already a part of an auto created EtherChannel, the port interface will unbundle from the auto EtherChannel.

The following table shows the supported auto-LAG configurations between the actor and partner devices:

<table>
<thead>
<tr>
<th>Actor/Partner</th>
<th>Active</th>
<th>Passive</th>
<th>Auto</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Auto-LAG Configuration Guidelines

<table>
<thead>
<tr>
<th>Passive</th>
<th>Yes</th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

On disabling auto-LAG globally, all auto created Etherchannels become manual EtherChannels.

You cannot add any configurations in an existing auto created EtherChannel. To add, you should first convert it into a manual EtherChannel by executing the `port-channel <channel-number> persistent`.

---

**Note**

Auto-LAG uses the LACP protocol to create auto EtherChannel. Only one EtherChannel can be automatically created with the unique partner devices.

---

**Related Topics**

- Configuring Auto-LAG Globally, on page 164
- Configuring Auto LAG: Examples, on page 170
- Configuring Auto-LAG on a Port Interface, on page 165
- Configuring Persistence with Auto-LAG, on page 166
- Auto-LAG Configuration Guidelines, on page 150

---

**Auto-LAG Configuration Guidelines**

Follow these guidelines when configuring the auto-LAG feature.

- When auto-LAG is enabled globally and on the port interface, and if you do not want the port interface to become a member of the auto EtherChannel, disable the auto-LAG on the port interface.

- A port interface will not bundle to an auto EtherChannel when it is already a member of a manual EtherChannel. To allow it to bundle with the auto EtherChannel, first unbundle the manual EtherChannel on the port interface.

- When auto-LAG is enabled and auto EtherChannel is created, you can create multiple EtherChannels manually with the same partner device. But by default, the port tries to create auto EtherChannel with the partner device.

- The auto-LAG is supported only on Layer 2 EtherChannel. It is not supported on Layer 3 interface and Layer 3 EtherChannel.

- The auto-LAG is supported on cross-stack EtherChannel.

---

**Related Topics**

- Configuring Auto-LAG Globally, on page 164
- Configuring Auto LAG: Examples, on page 170
- Configuring Auto-LAG on a Port Interface, on page 165
- Configuring Persistence with Auto-LAG, on page 166
- Auto-LAG, on page 149
# How to Configure EtherChannels

After you configure an EtherChannel, configuration changes applied to the port-channel interface apply to all the physical ports assigned to the port-channel interface, and configuration changes applied to the physical port affect only the port where you apply the configuration.

## Configuring Layer 2 EtherChannels (CLI)

You configure Layer 2 EtherChannels by assigning ports to a channel group with the `channel-group` interface configuration command. This command automatically creates the port-channel logical interface.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies a physical port, and enters interface configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Valid interfaces are physical ports. For a PAgP EtherChannel, you can configure up to eight ports of the same type and speed for the same group. For a LACP EtherChannel, you can configure up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Assigns all ports as static-access ports in the same VLAN, or configure them as trunks. If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.</td>
</tr>
<tr>
<td>`switchport mode {access</td>
<td>trunk}`</td>
</tr>
<tr>
<td>Example: Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.</td>
</tr>
<tr>
<td><code>switchport access vlan vlan-id</code></td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# switchport access vlan 22</td>
<td></td>
</tr>
</tbody>
</table>
Step 5

channel-group channel-group-number mode
{auto [non-silent] | desirable [non-silent] | on} | {active | passive}

Example:

Switch(config-if)# channel-group 5 mode auto

Assigns the port to a channel group, and specifies the PAgP or the LACP mode.

For channel-group-number, the range is 1 to 128.

For mode, select one of these keywords:

- **auto** — Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. This keyword is not supported when EtherChannel members are from different switches in the switch stack.

- **desirable** — Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets. This keyword is not supported when EtherChannel members are from different switches in the switch stack.

- **on** — Forces the port to channel without PAgP or LACP. In the on mode, an EtherChannel exists only when a port group in the on mode is connected to another port group in the on mode.

- **non-silent** — (Optional) If your switch is connected to a partner that is PAgP-capable, configures the switch port for nonsilent operation when the port is in the auto or desirable mode. If you do not specify non-silent, silent is assumed. The silent setting is for connections to file servers or packet analyzers. This setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission.

- **active** — Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.

- **passive** — Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets.
### Configuring Layer 3 EtherChannels (CLI)

Follow these steps to assign an Ethernet port to a Layer 3 EtherChannel. This procedure is required.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch&gt; <code>enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Switch# <code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies a physical port, and enters interface configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Valid interfaces include physical ports.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>interface gigabitethernet</code></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>1/0/2</td>
<td>For a PAgP EtherChannel, you can configure up to eight ports of the same type and speed for the same group. For a LACP EtherChannel, you can configure up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.</td>
</tr>
</tbody>
</table>

**Step 4**

no ip address

*Example:*

Switch(config-if)# no ip address

Ensures that there is no IP address assigned to the physical port.

**Step 5**

no switchport

*Example:*

Switch(config-if)# no switchport

Puts the port into Layer 3 mode.

**Step 6**

channel-group  channel-group-number  [ auto  [ non-silent ] ]  [ desirable [ non-silent ] ]  [ on ]  [ active | passive ]

*Example:*

Switch(config-if)# channel-group 5 mode auto

Assigns the port to a channel group, and specifies the PAgP or the LACP mode.

For **mode**, select one of these keywords:

- **auto**—Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. This keyword is not supported when EtherChannel members are from different switches in the switch stack.

- **desirable**—Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets. This keyword is not supported when EtherChannel members are from different switches in the switch stack.

- **on**—Forces the port to channel without PAgP or LACP. In the **on** mode, an EtherChannel exists only when a port group in the **on** mode is connected to another port group in the **on** mode.

- **non-silent**—(Optional) If your switch is connected to a partner that is PAgP
Configuring EtherChannel Load-Balancing (CLI)

You can configure EtherChannel load-balancing to use one of several different forwarding methods. This task is optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>port-channel load-balance</td>
<td>Configures an EtherChannel load-balancing method.</td>
</tr>
<tr>
<td>{ dst-ip</td>
<td>dst-mac</td>
</tr>
<tr>
<td>Select one of these load-distribution methods:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>src-dst-ip</td>
<td>Specifies destination-host IP address.</td>
</tr>
<tr>
<td>src-dst-mac</td>
<td>Specifies the destination-host MAC address of the incoming packet.</td>
</tr>
<tr>
<td>src-dst-mixed-ip-port</td>
<td>Specifies the host IP address and TCP/UDP port.</td>
</tr>
<tr>
<td>src-port</td>
<td>Specifies the destination TCP/UDP port.</td>
</tr>
<tr>
<td>dst-mac</td>
<td>Specifies the destination host MAC address.</td>
</tr>
<tr>
<td>dst-mixed-ip-port</td>
<td>Specifies extended load balance methods--combinations of source and destination methods beyond those available with the standard command.</td>
</tr>
<tr>
<td>dst-port</td>
<td>Specifies the destination TCP/UDP port.</td>
</tr>
<tr>
<td>ipv6-label</td>
<td>Specifies the IPv6 flow label.</td>
</tr>
<tr>
<td>l3-proto</td>
<td>Specifies the Layer 3 protocol.</td>
</tr>
</tbody>
</table>

Example:

```
Switch(config)# port-channel load-balance src-mac
```

Step 3

Example:

```
Switch(config)# end
```

Returns to privileged EXEC mode.

Related Topics

Load-Balancing and Forwarding Methods, on page 142
Configuring EtherChannel Extended Load-Balancing (CLI)

Configure EtherChannel extended load-balancing when you want to use a combination of load-balancing methods.

This task is optional.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 2</strong></th>
<th>Configures an EtherChannel extended load-balancing method. The default is src-mac. Select one of these load-distribution methods:</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-channel load-balance extended [ dst-ip</td>
<td>dst-mac dst-port</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# port-channel load-balance extended dst-ip dst-mac src-ip</td>
<td></td>
</tr>
</tbody>
</table>

Mac Address Forwarding, on page 143
IP Address Forwarding, on page 143
Load-Balancing Advantages, on page 144
EtherChannel Configuration Guidelines, on page 147
Layer 2 EtherChannel Configuration Guidelines, on page 148
Default EtherChannel Configuration, on page 146
Layer 3 EtherChannel Configuration Guidelines, on page 149
Configuring the PAgP Learn Method and Priority (CLI)

This task is optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Example:</td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies the port for transmission, and enters interface configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Example:</td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Selects the PAgP learning method.</td>
</tr>
<tr>
<td><code>pagp learn-method physical-port</code></td>
<td>Example:</td>
</tr>
<tr>
<td>Switch(config-if)# pagp learn-method physical port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Assigns a priority so that the selected port is chosen for packet transmission.</td>
</tr>
<tr>
<td><code>pagp port-priority priority</code></td>
<td>Example:</td>
</tr>
</tbody>
</table>
### Configuring LACP Hot-Standby Ports

When LACP is enabled, the software, by default, tries to configure the maximum number of LACP-compatible ports in a channel, up to a maximum of 16 ports. Only eight LACP links can be active at one time; the remaining eight links are placed in hot-standby mode. If one of the active links becomes inactive, a link that is in the hot-standby mode becomes active in its place.

You can override the default behavior by specifying the maximum number of active ports in a channel, in which case, the remaining ports become hot-standby ports. For example, if you specify a maximum of five ports in a channel, up to 11 ports become hot-standby ports.

If you configure more than eight links for an EtherChannel group, the software automatically decides which of the hot-standby ports to make active based on the LACP priority. To every link between systems that operate LACP, the software assigns a unique priority made up of these elements (in priority order):

- LACP system priority
- System ID (the switch MAC address)
- LACP port priority
- Port number

In priority comparisons, numerically lower values have higher priority. The priority decides which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Determining which ports are active and which are hot standby is a two-step procedure. First the system with a numerically lower system priority and system ID is placed in charge of the decision. Next, that system decides which ports are active and which are hot standby, based on its values for port priority and port number. The port priority and port number values for the other system are not used.

You can change the default values of the LACP system priority and the LACP port priority to affect how the software selects active and standby links.

---

### Related Topics

- PAgP Learn Method and Priority, on page 139
- EtherChannel Configuration Guidelines, on page 147
- Default EtherChannel Configuration, on page 146
- Monitoring EtherChannel, PAgP, and LACP Status, on page 167
- Layer 2 EtherChannel Configuration Guidelines, on page 148

---

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config-if)# pagp port-priority 200</code></td>
<td>For priority, the range is 0 to 255. The default is 128. The higher the priority, the more likely that the port will be used for PAgP transmission.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>Switch(config-if)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Configuring the LACP Max Bundle Feature (CLI)

When you specify the maximum number of bundled LACP ports allowed in a port channel, the remaining ports in the port channel are designated as hot-standby ports.

Beginning in privileged EXEC mode, follow these steps to configure the maximum number of LACP ports in a port channel. This procedure is optional.

Procedure

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface port-channel channel-number</td>
<td>Enters interface configuration mode for a port channel. The range is 1 to 128.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface port-channel 2</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>lACP max-bundle max-bundle-number</td>
<td>Specifies the maximum number of LACP ports in the port-channel bundle. The range is 1 to 8.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# lACP max-bundle 3</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics
- LACP and Link Redundancy, on page 141
- Configuring LACP Hot-Standby Ports: Example, on page 170

Configuring LACP Port-Channel Standalone Disable

To disable the standalone EtherChannel member port state on a port channel, perform this task on the port channel interface:
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface port-channel channel-group</td>
<td>Selects a port channel interface to configure.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface port-channel channel-group</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> port-channel standalone-disable</td>
<td>Disables the standalone mode on the port-channel interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# port-channel standalone-disable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show etherchannel</td>
<td>Verifies the configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show etherchannel channel-group port-channel detail</td>
<td></td>
</tr>
</tbody>
</table>

## Related Topics

- Configuring LACP Hot-Standby Ports: Example, on page 170

## Configuring the LACP Port Channel Min-Links Feature (CLI)

You can specify the minimum number of active ports that must be in the link-up state and bundled in an EtherChannel for the port channel interface to transition to the link-up state. Using EtherChannel min-links, you can prevent low-bandwidth LACP EtherChannels from becoming active. Port channel min-links also cause LACP EtherChannels to become inactive if they have too few active member ports to supply the required minimum bandwidth.

To configure the minimum number of links that are required for a port channel. Perform the following tasks.

## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the LACP System Priority (CLI)

You can configure the system priority for all the EtherChannels that are enabled for LACP by using the `lacp system-priority` global configuration command. You cannot configure a system priority for each LACP-configured channel. By changing this value from the default, you can affect how the software selects active and standby links.

You can use the `show etherchannel summary` privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

Follow these steps to configure the LACP system priority. This procedure is optional.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

---

**Configuring the LACP System Priority (CLI)**

You can configure the system priority for all the EtherChannels that are enabled for LACP by using the `lacp system-priority` global configuration command. You cannot configure a system priority for each LACP-configured channel. By changing this value from the default, you can affect how the software selects active and standby links.

You can use the `show etherchannel summary` privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

Follow these steps to configure the LACP system priority. This procedure is optional.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring the LACP Port Priority (CLI)

By default, all ports use the same port priority. If the local system has a lower value for the system priority and the system ID than the remote system, you can affect which of the hot-standby links become active first by changing the port priority of LACP EtherChannel ports to a lower value than the default. The hot-standby ports that have lower port numbers become active in the channel first. You can use the `show etherchannel summary` privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

**configure terminal**

**Example:**

`Switch# configure terminal`

| **Step 3** |  |
| lacp system-priority **priority** | Configures the LACP system priority. |
| **Example:** | The range is 1 to 65535. The default is 32768. |
| `Switch(config)# lacp system-priority 32000` | The lower the value, the higher the system priority. |

**Step 4**

**end**

**Example:**

`Switch(config)# end`

**Related Topics**

- EtherChannel Configuration Guidelines, on page 147
- Default EtherChannel Configuration, on page 146
- Layer 2 EtherChannel Configuration Guidelines, on page 148
- Monitoring EtherChannel, PAgP, and LACP Status, on page 167

**Note**

If LACP is not able to aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), all the ports that cannot be actively included in the EtherChannel are put in the hot-standby state and are used only if one of the channeled ports fails.

Follow these steps to configure the LACP port priority. This procedure is optional.
## Configuring Auto-LAG Globally

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**        | **enable**<br><br>Example:  
Switch> enable  |
|                   | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Step 2**        | **configure terminal**<br><br>Example:  
Switch# configure terminal  |
|                   | Enters global configuration mode. |
| **Step 3**        | **interface interface-id**<br><br>Example:  
Switch(config)# interface gigabitethernet  |
|                   | Specifies the port to be configured, and enters interface configuration mode. |
| **Step 4**        | **lacp port-priority priority**<br><br>Example:  
Switch(config-if)# lacp port-priority 32000  |
|                   | Configures the LACP port priority.  
The range is 1 to 65535. The default is 32768.  
The lower the value, the more likely that the port will be used for LACP transmission. |
| **Step 5**        | **end**<br><br>Example:  
Switch(config-if)# end  |
|                   | Returns to privileged EXEC mode. |

### Related Topics

- [EtherChannel Configuration Guidelines](#), on page 147
- [Default EtherChannel Configuration](#), on page 146
- [Layer 2 EtherChannel Configuration Guidelines](#), on page 148
- [Monitoring EtherChannel, PAgP, and LACP Status](#), on page 167

---

### Configuring Auto-LAG Globally

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring Auto-LAG on a Port Interface

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**
- Auto-LAG, on page 149
- Auto-LAG Configuration Guidelines, on page 150
- Configuring Auto LAG: Examples, on page 170
- Configuring Auto-LAG on a Port Interface, on page 165
- Configuring Persistence with Auto-LAG, on page 166

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>port-channel auto</strong></td>
<td>Enables the auto-LAG feature on a switch globally. Use the <code>no</code> form of this command to disable the auto-LAG feature on the switch globally.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# port-channel auto</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note**
By default, the auto-LAG feature is enabled on the port.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><strong>end</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><strong>show etherchannel auto</strong></td>
<td>Displays that EtherChannel is created automatically.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show etherchannel auto</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Persistence with Auto-LAG

You use the persistence command to convert the auto created EtherChannel into a manual one and allow you to add configuration on the existing EtherChannel.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

---

### What to do next

**Related Topics**
- Configuring Auto-LAG Globally, on page 164
- Auto-LAG, on page 149
- Auto-LAG Configuration Guidelines, on page 150
- Configuring Persistence with Auto-LAG, on page 166
- Configuring Auto LAG: Examples, on page 170
Purpose

Command or Action

Example:

Switch> enable

• Enter your password if prompted.

Step 2

port-channel channel-number persistent

Example:

Switch# port-channel 1 persistent

Converts the auto created EtherChannel into a manual one and allows you to add configuration on the EtherChannel.

Step 3

show etherchannel summary

Example:

Switch# show etherchannel summary

Displays the EtherChannel information.

Related Topics

Configuring Auto-LAG Globally, on page 164
Auto-LAG, on page 149
Auto-LAG Configuration Guidelines, on page 150
Configuring Auto-LAG on a Port Interface, on page 165
Configuring Auto LAG: Examples, on page 170

Monitoring EtherChannel, PAgP, and LACP Status

You can display EtherChannel, PAgP, and LACP status using the commands listed in this table.

Table 10: Commands for Monitoring EtherChannel, PAgP, and LACP Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear lacp { channel-group-number counters</td>
<td>Clears LACP channel-group information and traffic counters.</td>
</tr>
<tr>
<td>counters }</td>
<td></td>
</tr>
<tr>
<td>clear pagp { channel-group-number counters</td>
<td>Clears PAgP channel-group information and traffic counters.</td>
</tr>
<tr>
<td>counters }</td>
<td></td>
</tr>
<tr>
<td>show etherchannel [ channel-group-number { detail</td>
<td>Displays EtherChannel information in a brief, detailed,</td>
</tr>
<tr>
<td>load-balance</td>
<td>port</td>
</tr>
<tr>
<td>protocol</td>
<td>summary } [ detail</td>
</tr>
<tr>
<td>show pagp [ channel-group-number ] { counters</td>
<td>Displays PAgP information such as traffic</td>
</tr>
<tr>
<td>internal</td>
<td>neighbor }</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>show pagp [ channel-group-number ] dual-active</td>
<td>Displays the dual-active detection status.</td>
</tr>
</tbody>
</table>
**Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show lacp [channel-group-number] {counters</td>
<td>Displays LACP information such as traffic information, the internal LACP configuration, and neighbor information.</td>
</tr>
<tr>
<td>internal</td>
<td>neighbor sys-id}</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verifies your configuration entries.</td>
</tr>
<tr>
<td><code>show etherchannel load-balance</code></td>
<td>Displays the load balance or frame distribution scheme among ports in the port channel.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring the PAgP Learn Method and Priority (CLI), on page 158
- PAgP Learn Method and Priority, on page 139
- Configuring the LACP System Priority (CLI), on page 162
- Configuring the LACP Port Priority (CLI), on page 163

---

**Configuration Examples for Configuring EtherChannels**

**Configuring Layer 2 EtherChannels: Examples**

This example shows how to configure an EtherChannel on a single switch in the stack. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the PAgP mode `desirable:`

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet -2
Switch(config)# switchport mode access
Switch(config)# switchport access vlan 10
Switch(config)# channel-group 5 mode desirable non-silent
Switch(config)# end
```

This example shows how to configure an EtherChannel on a single switch in the stack. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the LACP mode `active`:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet -2
Switch(config)# switchport mode access
Switch(config)# switchport access vlan 10
Switch(config)# channel-group 5 mode active
Switch(config)# end
```

This example shows how to configure a cross-stack EtherChannel. It uses LACP passive mode and assigns two ports on stack member 1 and one port on stack member 2 as static-access ports in VLAN 10 to channel 5:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet -5
Switch(config)# switchport mode access
```
PoE or LACP negotiation errors may occur if you configure two ports from switch to the access point (AP). This scenario can be avoided if the port channel configuration is on the switch side. For more details, see the following example:

interface Port-channel1
  switchport access vlan 20
  switchport mode access
  switchport nonegotiate
  no port-channel standalone-disable <--this one
  spanning-tree portfast

Note: If the port reports LACP errors on port flap, you should include the following command as well: no errdisable
detect cause pagp-flap

**Configuring Layer 3 EtherChannels: Examples**

This example shows how to configure a Layer 3 EtherChannel. It assigns two ports to channel 5 with the LACP mode active:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

This example shows how to configure a cross-stack Layer 3 EtherChannel. It assigns two ports on stack member 2 and one port on stack member 3 to channel 7 using LACP active mode:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 7 mode active
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# no ip address
Switch(config-if)# no switchport
Switch(config-if)# channel-group 7 mode active
Switch(config-if)# exit
```
Configuring LACP Hot-Standby Ports: Example

This example shows how to configure an Etherchannel (port channel 2) that will be active when there are at least three active ports, will comprise up to seven active ports and the remaining ports (up to nine) as hot-standby ports:

```
Switch# configure terminal
Switch(config)# interface port-channel 2
Switch(config-if)# port-channel min-links 3
Switch(config-if)# lACP max-bundle 7
```

This example shows how to disable the standalone EtherChannel member port state on port channel 42:

```
Switch(config)# interface port-channel channel-group
Switch(config-if)# port-channel standalone-disable
```

This example shows how to verify the configuration:

```
Switch# show etherchannel 42 port-channel | include Standalone
Standalone Disable = enabled
Switch# show etherchannel 42 detail | include Standalone
Standalone Disable = enabled
```

Related Topics
- Configuring the LACP Max Bundle Feature (CLI), on page 160
- LACP and Link Redundancy, on page 141
- Configuring LACP Port-Channel Standalone Disable, on page 160
- Configuring the LACP Port Channel Min-Links Feature (CLI), on page 161

Configuring Auto LAG: Examples

This example shows how to configure Auto-LAG on a switch

```
switch> enable
switch# configure terminal
switch (config)# port-channel auto
switch (config-if)# end
switch# show etherchannel auto
```

The following example shows the summary of EtherChannel that was created automatically.

```
switch# show etherchannel auto
Flags:  D - down   P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3   S - Layer2
        U - in use   f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol  Ports
```
The following example shows the summary of auto EtherChannel after executing the `port-channel 1 persistent` command.

```
switch# port-channel 1 persistent
switch# show etherchannel summary
Switch# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
       I - stand-alone  S - suspended
       H - Hot-standby (LACP only)
       R - Layer3      S - Layer2
       U - in use      f - failed to allocate aggregator
       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
       A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol  Ports
-------+------------+-----------+-----------------------------------------------
1      Po1(SU)    LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

**Related Topics**
- Configuring Auto-LAG Globally, on page 164
- Auto-LAG, on page 149
- Auto-LAG Configuration Guidelines, on page 150
- Configuring Persistence with Auto-LAG, on page 166
- Configuring Auto-LAG on a Port Interface, on page 165
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature Information for EtherChannels

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>Support for the LACP max-bundle feature and the port channel min-links features was added.</td>
</tr>
<tr>
<td>Cisco IOS 15.2(3)E2, Cisco IOS XE 3.7.2E</td>
<td>Auto-LAG feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 10

Configuring Flex Links and the MAC Address-Table Move Update Feature

• Finding Feature Information, on page 173
• Restrictions for Configuring Flex Links and MAC Address-Table Move Update, on page 173
• Information About Flex Links and MAC Address-Table Move Update, on page 174
• How to Configure Flex Links and the MAC Address-Table Move Update Feature, on page 180
• Monitoring Flex Links, Multicast Fast Convergence, and MAC Address-Table Move Update, on page 186
• Configuration Examples for Flex Links, on page 186
• Additional References for Flex Links and MAC Address-Table Move Update, on page 191
• Feature Information for Flex Links and MAC Address-Table Move Update, on page 192

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring Flex Links and MAC Address-Table Move Update

• Flex Links are supported only on Layer 2 ports and port channels.
• You can configure up to 16 backup links.
• You can configure only one Flex Links backup link for any active link, and it must be a different interface from the active interface.
• An interface can belong to only one Flex Links pair. An interface can be a backup link for only one active link. An active link cannot belong to another Flex Links pair.

• Neither of the links can be a port that belongs to an EtherChannel. However, you can configure two port channels (EtherChannel logical interfaces) as Flex Links, and you can configure a port channel and a physical interface as Flex Links, with either the port channel or the physical interface as the active link.

• A backup link does not have to be the same type (Gigabit Ethernet or port channel) as the active link. However, you should configure both Flex Links with similar characteristics so that there are no loops or changes in behavior if the standby link begins to forward traffic.

• STP is disabled on Flex Links ports. A Flex Links port does not participate in STP, even if the VLANs present on the port are configured for STP. When STP is not enabled, be sure that there are no loops in the configured topology.

• You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

Related Topics
- Configuring a Preemption Scheme for a Pair of Flex Links (CLI), on page 181
- Configuring Flex Links (CLI), on page 180
- Configuring Flex Links: Examples, on page 186
- Configuring VLAN Load Balancing on Flex Links (CLI), on page 183
- Configuring VLAN Load Balancing on Flex Links: Examples, on page 187
- Configuring a Switch to Obtain and Process MAC Address-Table Move Update Messages (CLI), on page 185
- Configuring MAC Address-Table Move Update (CLI), on page 184
- Configuring the MAC Address-Table Move Update: Examples, on page 188

Information About Flex Links and MAC Address-Table Move Update

Flex Links

Flex Links are a pair of a Layer 2 interfaces (switch ports or port channels) where one interface is configured to act as a backup to the other. The feature provides an alternative solution to the Spanning Tree Protocol (STP). Users can disable STP and still retain basic link redundancy. Flex Links are typically configured in service provider or enterprise networks where customers do not want to run STP on the switch. If the switch is running STP, Flex Links are not necessary because STP already provides link-level redundancy or backup.

You configure Flex Links on one Layer 2 interface (the active link) by assigning another Layer 2 interface as the Flex Links or backup link. On switches, the Flex Links can be on the same switch or on another switch in the stack. When one of the links is up and forwarding traffic, the other link is in standby mode, ready to begin forwarding traffic if the other link shuts down. At any given time, only one of the interfaces is in the link up state and forwarding traffic. If the primary link shuts down, the standby link starts forwarding traffic. When the active link comes back up, it goes into standby mode and does not forward traffic. STP is disabled on Flex Links interfaces.

Related Topics
- Configuring a Preemption Scheme for a Pair of Flex Links (CLI), on page 181
Flex Links Configuration

In the following figure, ports 1 and 2 on switch A are connected to uplink switches B and C. Because they are configured as Flex Links, only one of the interfaces is forwarding traffic; the other is in standby mode. If port 1 is the active link, it begins forwarding traffic between port 1 and switch B; the link between port 2 (the backup link) and switch C is not forwarding traffic. If port 1 goes down, port 2 comes up and starts forwarding traffic to switch C. When port 1 comes back up, it goes into standby mode and does not forward traffic; port 2 continues forwarding traffic.

You can also configure a preemption function, specifying the preferred port for forwarding traffic. For example, you can configure the Flex Links pair with preemption mode. In the scenario shown, when port 1 comes back up and has more bandwidth than port 2, port 1 begins forwarding traffic after 60 seconds. Port 2 becomes the standby port. You do this by entering the `switchport backup interface preemption mode bandwidth` and `switchport backup interface preemption delay` interface configuration commands.

If a primary (forwarding) link goes down, a trap notifies the network management stations. If the standby link goes down, a trap notifies the users.

Flex Links are supported only on Layer 2 ports and port channels, not on VLANs or on Layer 3 ports.

Related Topics
- Configuring a Preemption Scheme for a Pair of Flex Links (CLI), on page 181
- Configuring Flex Links (CLI), on page 180

VLAN Flex Links Load Balancing and Support

VLAN Flex Links load balancing allows users to configure a Flex Links pair so that both ports simultaneously forward the traffic for some mutually exclusive VLANs. For example, if Flex Links ports are configured for 1 to 100 VLANs, the traffic of the first 50 VLANs can be forwarded on one port and the rest on the other.
Multicast Fast Convergence with Flex Links Failover

Multicast fast convergence reduces the multicast traffic convergence time after a Flex Links failure. Multicast fast convergence is implemented by a combination of learning the backup link as an mrouter port, generating IGMP reports, and leaking IGMP reports.

Related Topics

Configuring Multicast Fast Convergence with Flex Links Failover: Examples, on page 189

Learning the Other Flex Links Port as the mrouter Port

In a typical multicast network, there is a querier for each VLAN. A switch deployed at the edge of a network has one of its Flex Links ports receiving queries. Flex Links ports are also always forwarding at any given time.

A port that receives queries is added as an mrouter port on the switch. An mrouter port is part of all the multicast groups learned by the switch. After a changeover, queries are received by the other Flex Links port. The other Flex Links port is then learned as the mrouter port. After changeover, multicast traffic then flows through the other Flex Links port. To achieve faster convergence of traffic, both Flex Links ports are learned as mrouter ports whenever either Flex Links port is learned as the mrouter port. Both Flex Links ports are always part of multicast groups.

Although both Flex Links ports are part of the groups in normal operation mode, all traffic on the backup port is blocked. The normal multicast data flow is not affected by the addition of the backup port as an mrouter port.
Generating IGMP Reports

When the backup link comes up after the changeover, the upstream new distribution switch does not start forwarding multicast data, because the port on the upstream router, which is connected to the blocked Flex Links port, is not part of any multicast group. The reports for the multicast groups were not forwarded by the downstream switch because the backup link is blocked. The data does not flow on this port, until it learns the multicast groups, which occurs only after it receives reports.

The reports are sent by hosts when a general query is received, and a general query is sent within 60 seconds in normal scenarios. When the backup link starts forwarding, to achieve faster convergence of multicast data, the downstream switch immediately sends proxy reports for all the learned groups on this port without waiting for a general query.

Leaking IGMP Reports

To achieve multicast traffic convergence with minimal loss, a redundant data path must be set up before the Flex Links active link goes down. This can be achieved by leaking only IGMP report packets on the Flex Links backup link. These leaked IGMP report messages are processed by upstream distribution routers, so multicast data traffic gets forwarded to the backup interface. Because all incoming traffic on the backup interface is dropped at the ingress of the access switch, no duplicate multicast traffic is received by the host. When the Flex Links active link fails, the access switch starts accepting traffic from the backup link immediately. The only disadvantage of this scheme is that it consumes bandwidth on the link between the distribution switches and on the backup link between the distribution and access switches. This feature is disabled by default and can be configured by using the `switchport backup interface interface-id multicast fast-convergence` command.

When this feature has been enabled at changeover, the switch does not generate the proxy reports on the backup port, which became the forwarding port.

MAC Address-Table Move Update

The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence when a primary (forwarding) link goes down and the standby link begins forwarding traffic.

Figure 19: MAC Address-Table Move Update Example

In the following figure, switch A is an access switch, and ports 1 and 2 on switch A are connected to uplink switches B and D through a Flex Links pair. Port 1 is forwarding traffic, and port 2 is in the backup state. Traffic from the PC to the server is forwarded from port 1 to port 3. The MAC address of the PC has been...
learned on port 3 of switch C. Traffic from the server to the PC is forwarded from port 3 to port 1.

If the MAC address-table move update feature is not configured and port 1 goes down, port 2 starts forwarding traffic. However, for a short time, switch C keeps forwarding traffic from the server to the PC through port 3, and the PC does not get the traffic because port 1 is down. If switch C removes the MAC address of the PC on port 3 and relearns it on port 4, traffic can then be forwarded from the server to the PC through port 2.

If the MAC address-table move update feature is configured and enabled on the switches, and port 1 goes down, port 2 starts forwarding traffic from the PC to the server. The switch sends a MAC address-table move update packet from port 2. Switch C gets this packet on port 4 and immediately learns the MAC address of the PC on port 4, which reduces the reconvergence time.

You can configure the access switch, switch A, to send MAC address-table move update messages. You can also configure the uplink switches B, C, and D to get and process the MAC address-table move update messages. When switch C gets a MAC address-table move update message from switch A, switch C learns the MAC address of the PC on port 4. Switch C updates the MAC address table, including the forwarding table entry for the PC.

Switch A does not need to wait for the MAC address-table update. The switch detects a failure on port 1 and immediately starts forwarding server traffic from port 2, the new forwarding port. This change occurs in less than 100 milliseconds (ms). The PC is directly connected to switch A, and the connection status does not change. Switch A does not need to update the PC entry in the MAC address table.
Figure 20: MAC Address-Table Move Update Example

In the following figure, the controller and switches B and C form the Flexlink through a Flex Links pair. Port 3 is forwarding traffic, and port 4 is in the backup state. Switch A is an access switch, and ports 1 and 2 on switch A are connected to uplink switches B and C. The MAC addresses of the wireless clients have been learnt on port 1 of the switch A.

In the above figure, three wireless clients connect to an access point and communicate to the controller. The PC connected to switch A communicates with the wireless clients through the data path from port 3 to port 1. If the MAC address-table move update feature is not configured on the controller and port 3 goes down, port 4 starts forwarding traffic. However, for a short time the wireless clients will not be able to pass any traffic to the PC as port 3 is down.

If the MAC address-table move update feature is configured and enabled on the controller, and port 3 goes down, the controller sends a MAC address-table move update packet (MMU) from port 4. This MMU packet carries all the MAC addresses of the wireless clients. Switch C gets this packet on port 4 and immediately learns the MAC addresses of the wireless clients, which reduces the reconvergence time. The PC transmits data to the wireless clients using the path from port 2 to port 4. Switch C also bridges the same MMU packet in the VLAN so that all the switches in the network will update the MAC address table to ensure that the next packet to any wireless client towards controller comes on the right path. The controller learns only the MAC addresses of the wireless clients.

Related Topics
- Configuring a Switch to Obtain and Process MAC Address-Table Move Update Messages (CLI), on page 185
- Configuring MAC Address-Table Move Update (CLI), on page 184
- Configuring the MAC Address-Table Move Update: Examples, on page 188

**Flex Links VLAN Load Balancing Configuration Guidelines**

- For Flex Links VLAN load balancing, you must choose the preferred VLANs on the backup interface.
- You cannot configure a preemption mechanism and VLAN load balancing for the same Flex Links pair.

Related Topics
- Configuring VLAN Load Balancing on Flex Links (CLI), on page 183
- Configuring VLAN Load Balancing on Flex Links: Examples, on page 187
MAC Address-Table Move Update Configuration Guidelines

- You can enable and configure this feature on the access switch to send the MAC address-table move updates.
- You can enable and configure this feature on the uplink switches to get the MAC address-table move updates.

Default Flex Links and MAC Address-Table Move Update Configuration

- Flex Links is not configured, and there are no backup interfaces defined.
- The preemption mode is off.
- The preemption delay is 35 seconds.
- The MAC address-table move update feature is not configured on the switch.

Related Topics
- Configuring a Preemption Scheme for a Pair of Flex Links (CLI), on page 181
- Configuring Flex Links (CLI), on page 180
- Configuring Flex Links: Examples, on page 186

How to Configure Flex Links and the MAC Address-Table Move Update Feature

Configuring Flex Links (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Step 2  
interface interface-id  
Example:  
Switch(conf)# interface gigabitethernet1/0/1  
Specifications the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 128.

Step 3  
switchport backup interface interface-id  
Example:  
Configures a physical Layer 2 interface (or port channel) as part of a Flex Links pair with the
Configuring a Preemption Scheme for a Pair of Flex Links (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
<td></td>
</tr>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code></td>
<td>Specifies the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 128.</td>
<td>Specify the Layer 2 interface configured for a Flex Link. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 128.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(conf)# interface gigabitethernet1/0/1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>switchport backup interface interface-id</code></td>
<td>Configures a physical Layer 2 interface (or port channel) as part of a Flex Links pair with the interface. When one link is forwarding traffic, the other interface is in standby mode.</td>
<td>Specify the interface configured for a Flex Link. When one link is forwarding traffic, the other interface is in standby mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(conf-if)# switchport backup interface gigabitethernet1/0/2</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Preemption Scheme for a Pair of Flex Links (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>switchport backup interface <em>interface-id</em> preemption mode [forced</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(conf-if)#</td>
<td></td>
</tr>
<tr>
<td>switchport backup</td>
<td></td>
</tr>
<tr>
<td>interface gigabit</td>
<td></td>
</tr>
<tr>
<td>ethernet1/0/2</td>
<td></td>
</tr>
<tr>
<td>preemption mode</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>switchport backup interface <em>interface-id</em> preemption delay <em>delay-time</em></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(conf-if)#</td>
<td></td>
</tr>
<tr>
<td>switchport backup</td>
<td></td>
</tr>
<tr>
<td>interface gigabit</td>
<td></td>
</tr>
<tr>
<td>ethernet1/0/2</td>
<td></td>
</tr>
<tr>
<td>preemption delay</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(conf-if)#</td>
<td></td>
</tr>
<tr>
<td><strong>end</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show interface [interface-id] switchport backup</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch#</td>
<td></td>
</tr>
<tr>
<td>gigabitethernet1/0/2 switchport backup</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup config</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch#</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**
- Flex Links, on page 174
- Default Flex Links and MAC Address-Table Move Update Configuration, on page 180
- Restrictions for Configuring Flex Links and MAC Address-Table Move Update, on page 173
- Configuring Flex Links: Examples, on page 186
### Configuring VLAN Load Balancing on Flex Links (CLI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
<td>Specifies the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 128.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch (config)# interface gigabitethernet2/0/6</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switchport backup interface interface-id prefer vlan vlan-range</td>
<td>Configures a physical Layer 2 interface (or port channel) as part of a Flex Links pair with the interface and specifies the VLANs carried on the interface. The VLAN ID range is 1 to 4094.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch (config-if)# switchport backup interface gigabitethernet2/0/8 prefer vlan 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch (config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**
- Flex Links VLAN Load Balancing Configuration Guidelines, on page 179
- Restrictions for Configuring Flex Links and MAC Address-Table Move Update, on page 173
- Configuring VLAN Load Balancing on Flex Links: Examples, on page 187
- Monitoring Flex Links, Multicast Fast Convergence, and MAC Address-Table Move Update, on page 186
## Configuring MAC Address-Table Move Update (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code></td>
<td>Specifies the interface, and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch#interface gigabitethernet1/0/1</code></td>
<td>The interface can be a physical Layer 2 interface or a port channel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(logical interface). The port-channel range is 1 to 128.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Use one of the following:</td>
<td>Configures a physical Layer 2 interface (or port channel), as part of</td>
</tr>
<tr>
<td></td>
<td>• <code>switchport backup interface interface-id</code></td>
<td>a Flex Links pair with the interface. The MAC address-table move update</td>
</tr>
<tr>
<td></td>
<td>• <code>switchport backup interface interface-id mmu primary vlan vlan-id</code></td>
<td>VLAN is the lowest VLAN ID on the interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# switchport backup interface</code></td>
<td>Configure a physical Layer 2 interface (or port channel) and specifies</td>
</tr>
<tr>
<td></td>
<td><code>gigabitethernet0/2 mmu primary vlan 2</code></td>
<td>the VLAN ID on the interface, which is used for sending the MAC address-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>table-move update.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When one link is forwarding traffic, the other interface is in standby</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# end</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>mac address-table move update transmit</code></td>
<td>Enables the access switch to send MAC address-table move updates to</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>other switches in the network if the primary link goes down and the</td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# mac address-table move update transmit</code></td>
<td>switch starts forwarding traffic through the standby link.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter command <code>mac address-table move update</code> on the switch, for MMU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>packets to update MAC tables. When the primary link comes back up, the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAC tables need to reconverge and this command will transmit the MMU,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>that will establish the behavior.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Switch to Obtain and Process MAC Address-Table Move Update Messages (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>mac address-table move update receive</td>
<td>Enables the switch to obtain and processes the MAC address-table move updates.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch (config)# mac address-table move update receive</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch (config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics
- Monitoring Flex Links, Multicast Fast Convergence, and MAC Address-Table Move Update, on page 186
- Configuring the MAC Address-Table Move Update: Examples, on page 188
- MAC Address-Table Move Update, on page 177
- Restrictions for Configuring Flex Links and MAC Address-Table Move Update, on page 173
Monitoring Flex Links, Multicast Fast Convergence, and MAC Address-Table Move Update

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface [interface-id] switchport backup</td>
<td>Displays the Flex Links backup interface configured for an interface or all the configured Flex Links and the state of each active and backup interface (up or standby mode).</td>
</tr>
<tr>
<td>show ip igmp profile address-table move update profile-id</td>
<td>Displays the specified IGMP profile or all the IGMP profiles defined on the switch.</td>
</tr>
<tr>
<td>show mac address-table move update</td>
<td>Displays the MAC address-table move update information on the switch.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring a Preemption Scheme for a Pair of Flex Links (CLI), on page 181
- Configuring Flex Links (CLI), on page 180

Configuration Examples for Flex Links

Configuring Flex Links: Examples

This example shows how to verify the configuration after you configure an interface with a backup interface:

```
Switch# show interface switchport backup

Switch Backup Interface Pairs:
Active Interface Backup Interface State
---------------------------------------------------------------------------------
GigabitEthernet1/0/1 GigabitEthernet1/0/2 Active Up/Backup Standby
```

This example shows how to verify the configuration after you configure the preemption mode as forced for a backup interface pair:

```
Switch# show interface switchport backup detail

Switch Backup Interface Pairs:
Active Interface Backup Interface State
---------------------------------------------------------------------------------
GigabitEthernet1/0/211 GigabitEthernet1/0/2 Active Up/Backup Standby
Interface Pair : Gi1/0/1, Gi1/0/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (Gi1/0/1), 100000 Kbit (Gi1/0/2)
Mac Address Move Update Vlan : auto
```
Configuring VLAN Load Balancing on Flex Links: Examples

In the following example, VLANs 1 to 50, 60, and 100 to 120 are configured on the switch:

Switch(config)#  interface gigabitethernet 2/0/6
Switch(config-if)#  switchport backup interface gigabitethernet 2/0/8 prefer vlan 60,100-120

When both interfaces are up, Gi2/0/8 forwards traffic for VLANs 60 and 100 to 120 and Gi2/0/6 forwards traffic for VLANs 1 to 50.

Switch#  show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface    Backup Interface    State
------------------------------------------------------------------------
GigabitEthernet2/0/6        GigabitEthernet2/0/8    Active Up/Backup Standby
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120

When a Flex Links interface goes down (LINK_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Links pair. In this example, if interface Gi2/0/6 goes down, Gi2/0/8 carries all VLANs of the Flex Links pair.

Switch#  show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface    Backup Interface    State
------------------------------------------------------------------------
GigabitEthernet2/0/6        GigabitEthernet2/0/8    Active Down/Backup Up
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120

When a Flex Links interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface Gi2/0/6 comes up, VLANs preferred on this interface are blocked on the peer interface Gi2/0/8 and forwarded on Gi2/0/6.

Switch#  show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface    Backup Interface    State
Configuring the MAC Address-Table Move Update: Examples

This example shows how to verify the configuration after you configure an access switch to send MAC address-table move updates:

Switch# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 5
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 000b.462d.c502
Rcv last switch-ID : 0403.fd6a.8700
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None

Related Topics
- Configuring MAC Address-Table Move Update (CLI), on page 184
- Configuring a Switch to Obtain and Process MAC Address-Table Move Update Messages (CLI), on page 185
- MAC Address-Table Move Update, on page 177
Configuring Multicast Fast Convergence with Flex Links Failover: Examples

These are configuration examples for learning the other Flex Links port as the mrouter port when Flex Links is configured on GigabitEthernet1/0/11 and GigabitEthernet1/0/12, and output for the `show interfaces switchport backup` command:

```plaintext
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet1/0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport backup interface GigabitEthernet1/0/12
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/0/12
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
Switch(config)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
GigabitEthernet1/0/11 GigabitEthernet1/0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : Off
Bandwidth : 100000 Kbit (Gi1/0/11), 100000 Kbit (Gi1/0/12)
Mac Address Move Update Vlan : auto
```

This output shows a querier for VLANs 1 and 401, with their queries reaching the switch through GigabitEthernet1/0/11:

```plaintext
Switch# show ip igmp snooping querier
Vlan  IP Address  IGMP Version  Port
-----------------------------------------------
1     1.1.1.1     v2          Gi1/0/11
401   41.41.41.1  v2          Gi1/0/11
```

This example is output for the `show ip igmp snooping mrouter` command for VLANs 1 and 401:

```plaintext
Switch# show ip igmp snooping mrouter
Vlan  ports
----- ----
1     Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401   Gi1/0/11(dynamic), Gi1/0/12(dynamic)
```

Similarly, both Flex Links ports are part of learned groups. In this example, GigabitEthernet2/0/11 is a receiver/host in VLAN 1, which is interested in two multicast groups:

```plaintext
Switch# show ip igmp snooping groups
Vlan  Group  Type  Version  Port List
---------------------------------------------
1     228.1.5.1  igmp  v2  Gi1/0/11, Gi1/0/12, Gi2/0/11
```
When a host responds to the general query, the switch forwards this report on all the mrouter ports. In this example, when a host sends a report for the group 228.1.5.1, it is forwarded only on GigabitEthernet1/0/11, because the backup port GigabitEthernet1/0/12 is blocked. When the active link, GigabitEthernet1/0/11, goes down, the backup port, GigabitEthernet1/0/12, begins forwarding.

As soon as this port starts forwarding, the switch sends proxy reports for the groups 228.1.5.1 and 228.1.5.2 on behalf of the host. The upstream router learns the groups and starts forwarding multicast data. This is the default behavior of Flex Links. This behavior changes when the user configures fast convergence using the switchport backup interface gigabitEthernet 1/0/12 multicast fast-convergence command. This example shows turning on this feature:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet 1/0/11
Switch(config-if)# switchport backup interface gigabitEthernet 1/0/12 multicast fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
----------------------------------------------------------------------
GigabitEthernet1/0/11 GigabitEthernet1/0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
Bandwidth : 100000 Kbit (Gi1/0/11), 100000 Kbit (Gi1/0/12)
Mac Address Move Update Vlan : auto

This output shows a querier for VLAN 1 and 401 with their queries reaching the switch through GigabitEthernet1/0/11:

```
Switch# show ip igmp snooping querier
Vlan    IP Address    IGMP Version Port
--------------------------------------------
1       1.1.1.1       v2   Gi1/0/11
401     41.41.41.1    v2   Gi1/0/11

This is output for the show ip igmp snooping mrouter command for VLAN 1 and 401:

```
Switch# show ip igmp snooping mrouter
Vlan    ports
---- -----
1       Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401     Gi1/0/11(dynamic), Gi1/0/12(dynamic)

Similarly, both the Flex Links ports are a part of the learned groups. In this example, GigabitEthernet2/0/11 is a receiver/host in VLAN 1, which is interested in two multicast groups:

```
Switch# show ip igmp snooping groups
Vlan    Group    Type    Version Port List
--------------------------------------------
```
Whenever a host responds to the general query, the switch forwards this report on all the router ports. When you turn on this feature through the command-line port, and when a report is forwarded by the switch on GigabitEthernet1/0/11, it is also leaked to the backup port GigabitEthernet1/0/12. The upstream router learns the groups and starts forwarding multicast data, which is dropped at the ingress because GigabitEthernet1/0/12 is blocked. When the active link, GigabitEthernet1/0/11, goes down, the backup port, GigabitEthernet1/0/12, begins forwarding. You do not need to send any proxy reports as the multicast data is already being forwarded by the upstream router. By leaking reports to the backup port, a redundant multicast path has been set up, and the time taken for the multicast traffic convergence is very minimal.

**Related Topics**

-Multicast Fast Convergence with Flex Links Failover, on page 176

---

### Additional References for Flex Links and MAC Address-Table Move Update

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 command reference</td>
<td>Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2/3 Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>switchport backup interface command</td>
<td>Interface and Hardware Component Command Reference (Catalyst 3850 Switches)Interface Command Reference (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

**Error Message Decoder**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

**Standards and RFCs**

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases,</td>
</tr>
<tr>
<td></td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you</td>
<td></td>
</tr>
<tr>
<td>can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for Flex Links and MAC Address-Table Move Update

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>Support for multicast fast convergence with Flex Links failover was added.</td>
</tr>
</tbody>
</table>
CHAPTER 11

Configuring UniDirectional Link Detection

• Finding Feature Information, on page 193
• Restrictions for Configuring UDLD, on page 193
• Information About UDLD, on page 194
• How to Configure UDLD, on page 197
• Monitoring and Maintaining UDLD, on page 199
• Additional References for UDLD, on page 199
• Feature Information for UDLD, on page 200

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring UDLD

The following are restrictions for configuring UniDirectional Link Detection (UDLD):

• A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.

• When configuring the mode (normal or aggressive), make sure that the same mode is configured on both sides of the link.

• You can configure UDLD in interface configuration mode and the configuration is accepted by the device; however, this configuration is not displayed in the running configuration, nor is it saved.

Caution

Loop guard works only on point-to-point links. We recommend that each end of the link has a directly connected device that is running STP.
Information About UDLD

UniDirectional Link Detection (UDLD) is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it disables the affected port and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

Modes of Operation

UDLD has two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected ports on fiber-optic connections. In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected ports on fiber-optic links.

In normal and aggressive modes, UDLD works with the Layer 1 mechanisms to learn the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports. When you enable both autonegotiation and UDLD, the Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.

Normal Mode

In normal mode, UDLD detects a unidirectional link when fiber strands in a fiber-optic port are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the ports are connected correctly but the traffic is one way, UDLD does not detect the unidirectional link because the Layer 1 mechanism, which is supposed to detect this condition, does not do so. In this case, the logical link is considered undetermined, and UDLD does not disable the port.

When UDLD is in normal mode, if one of the fiber strands in a pair is disconnected, as long as autonegotiation is active, the link does not stay up because the Layer 1 mechanisms detect a physical problem with the link. In this case, UDLD does not take any action and the logical link is considered undetermined.

Related Topics

- Enabling UDLD Globally (CLI), on page 197
- Enabling UDLD on an Interface (CLI), on page 198

Aggressive Mode

In aggressive mode, UDLD detects a unidirectional link by using the previous detection methods. UDLD in aggressive mode can also detect a unidirectional link on a point-to-point link on which no failure between the two devices is allowed. It can also detect a unidirectional link when one of these problems exists:

- On fiber-optic or twisted-pair links, one of the ports cannot send or receive traffic.
- On fiber-optic or twisted-pair links, one of the ports is down while the other is up.
- One of the fiber strands in the cable is disconnected.
In these cases, UDLD disables the affected port.

In a point-to-point link, UDLD hello packets can be considered as a heartbeat whose presence guarantees the health of the link. Conversely, the loss of the heartbeat means that the link must be shut down if it is not possible to reestablish a bidirectional link.

If both fiber strands in a cable are working normally from a Layer 1 perspective, UDLD in aggressive mode detects whether those fiber strands are connected correctly and whether traffic is flowing bidirectionally between the correct neighbors. This check cannot be performed by autonegotiation because autonegotiation operates at Layer 1.

---

**Note**

UDLD is enabled with udld aggressive mode globally. When Rx cable or Tx is cable from switch1, then the switch1 and switch2 ports will go into **Not connected** state. They do not go to **error disabled** state. Also the port does not show any light if you check the physical connection.

Switch1 (Tx) __________________________ (Rx) Switch2
Switch1 (Rx) __________________________ (Tx) Switch2

**Related Topics**

- Enabling UDLD Globally (CLI), on page 197
- Enabling UDLD on an Interface (CLI), on page 198

---

**Methods to Detect Unidirectional Links**

UDLD operates by using two methods:

- Neighbor database maintenance
- Event-driven detection and echoing

**Related Topics**

- Enabling UDLD Globally (CLI), on page 197
- Enabling UDLD on an Interface (CLI), on page 198

**Neighbor Database Maintenance**

UDLD learns about other UDLD-capable neighbors by periodically sending a hello packet (also called an advertisement or probe) on every active port to keep each device informed about its neighbors.

When the switch receives a hello message, it caches the information until the age time (hold time or time-to-live) expires. If the switch receives a new hello message before an older cache entry ages, the switch replaces the older entry with the new one.

Whenever a port is disabled and UDLD is running, whenever UDLD is disabled on a port, or whenever the switch is reset, UDLD clears all existing cache entries for the ports affected by the configuration change. UDLD sends at least one message to inform the neighbors to flush the part of their caches affected by the status change. The message is intended to keep the caches synchronized.
Event-Driven Detection and Echoing

UDLD relies on echoing as its detection operation. Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-sync neighbor, it restarts the detection window on its side of the connection and sends echo messages in reply. Because this behavior is the same on all UDLD neighbors, the sender of the echoes expects to receive an echo in reply.

If the detection window ends and no valid reply message is received, the link might shut down, depending on the UDLD mode. When UDLD is in normal mode, the link might be considered undetermined and might not be shut down. When UDLD is in aggressive mode, the link is considered unidirectional, and the port is disabled.

Related Topics
- Enabling UDLD Globally (CLI), on page 197
- Enabling UDLD on an Interface (CLI), on page 198

UDLD Reset Options

If an interface becomes disabled by UDLD, you can use one of the following options to reset UDLD:

- The `udld reset` interface configuration command.
- The `shutdown` interface configuration command followed by the `no shutdown` interface configuration command restarts the disabled port.
- The `no udld {aggressive | enable}` global configuration command followed by the `udld {aggressive | enable}` global configuration command reenables the disabled ports.
- The `no udld port` interface configuration command followed by the `udld port [aggressive]` interface configuration command reenables the disabled fiber-optic port.
- The `errdisable recovery cause udld` global configuration command enables the timer to automatically recover from the UDLD error-disabled state, and the `errdisable recovery interval interval` global configuration command specifies the time to recover from the UDLD error-disabled state.

Related Topics
- Enabling UDLD Globally (CLI), on page 197
- Enabling UDLD on an Interface (CLI), on page 198

Default UDLD Configuration

Table 11: Default UDLD Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDLD global enable state</td>
<td>Globally disabled</td>
</tr>
<tr>
<td>UDLD per-port enable state for fiber-optic media</td>
<td>Disabled on all Ethernet fiber-optic ports</td>
</tr>
<tr>
<td>UDLD per-port enable state for twisted-pair (copper) media</td>
<td>Disabled on all Ethernet 10/100 and 1000BASE-TX ports</td>
</tr>
<tr>
<td>UDLD aggressive mode</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
How to Configure UDLD

Enabling UDLD Globally (CLI)

Follow these steps to enable UDLD in the aggressive or normal mode and to set the configurable message timer on all fiber-optic ports on the switch.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 2</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>udl {aggressive</td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# udl enable message time 10</td>
<td></td>
</tr>
</tbody>
</table>

- **aggressive**—Enables UDLD in aggressive mode on all fiber-optic ports.
- **enable**—Enables UDLD in normal mode on all fiber-optic ports on the switch. UDLD is disabled by default.

An individual interface configuration overrides the setting of the udl enable global configuration command.

- **message time**

message-timer-interval—Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are detected to be bidirectional. The range is from 1 to 90 seconds; the default value is 15.

**Note**

This command affects fiber-optic ports only. Use the udl interface configuration command to enable UDLD on other port types.

Use the no form of this command, to disable UDLD.
### Enabling UDLD on an Interface (CLI)

Follow these steps either to enable UDLD in the aggressive or normal mode or to disable UDLD on a port.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# interface gigabitethernet</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>udld port [aggressive]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# udld port aggressive</td>
</tr>
</tbody>
</table>

**UDLD is disabled by default.**

- **udld port**—Enables UDLD in normal mode on the specified port.
- **udld port aggressive**—(Optional) Enables UDLD in aggressive mode on the specified port.
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>Use the <em>no udl port</em> interface configuration command to disable UDLD on a specified fiber-optic port.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>end</th>
</tr>
</thead>
</table>

**Example:**

```
Switch(config-if)# end
```

### Related Topics

- Monitoring and Maintaining UDLD
- Aggressive Mode, on page 194
- Normal Mode, on page 194
- Methods to Detect Unidirectional Links, on page 195
- Event-Driven Detection and Echoing, on page 196
- UDLD Reset Options, on page 196
- Default UDLD Configuration, on page 196

### Monitoring and Maintaining UDLD

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show udl [interface-id</td>
<td>neighbors]`</td>
</tr>
</tbody>
</table>

### Additional References for UDLD

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>For complete syntax and usage information for the commands used in this chapter.</td>
<td>Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2 Command Reference (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

#### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>
### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

### Feature Information for UDLD

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
PART V

Lightweight Access Point

• Configuring the Switch for Access Point Discovery, on page 203
• Configuring Data Encryption, on page 211
• Configuring Retransmission Interval and Retry Count, on page 215
• Configuring Adaptive Wireless Intrusion Prevention System, on page 221
• Configuring Authentication for Access Points, on page 227
• Converting Autonomous Access Points to Lightweight Mode, on page 235
• Using Cisco Workgroup Bridges, on page 247
• Configuring Probe Request Forwarding, on page 251
• Optimizing RFID Tracking, on page 253
• Country Codes, on page 257
• Configuring Link Latency, on page 263
• Configuring Power over Ethernet, on page 273
CHAPTER 12

Configuring the Switch for Access Point Discovery

• Finding Feature Information, on page 203
• Prerequisites for Configuring the Switch for Access Point Discovery, on page 203
• Restrictions for Configuring the Switch for Access Point Discovery, on page 204
• Information About Configuring the Switch for Access Point Discovery, on page 204
• How to Configure Access Point Discovery, on page 206
• Configuration Examples for Configuring the Switch for Access Point Discovery, on page 207
• Configuring AP Pass Through, on page 209

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring the Switch for Access Point Discovery

⚠️ Caution
You should connect APs directly to the Cisco Catalyst 3850 switch ports to use its wireless functionality.

• Ensure that the Control and Provisioning of Wireless Access Points (CAPWAP) UDP ports 5246 and 5247 (similar to the Lightweight Access Point Protocol (LWAPP) UDP ports 12222 and 12223) are enabled and are not blocked by an intermediate device that could prevent an access point from joining the switch.

• If access control lists (ACLs) are in the control path between the switch and its access points, you must open new protocol ports to prevent access points from being stranded.
• If an access point is in the UP state and its IP address changes, the access point tears down the existing CAPWAP tunnel and rejoins the switch.

• Access points must be discovered by a switch before they can become an active part of the network. The lightweight access points support the following switch discovery processes:
  • Layer 3 CAPWAP discovery—You can enable this feature on different subnets from the access point. This feature uses IP addresses and UDP packets rather than MAC addresses used by Layer 2 discovery.
  • Locally stored switch IP address discovery—If the access point was previously associated to a switch, the IP addresses of the primary, secondary, and tertiary switches are stored in the access point’s nonvolatile memory. This process of storing switch IP addresses on an access point for later deployment is called *priming the access point*.
  • DHCP server discovery—This feature uses DHCP option 43 to provide switch IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability.
  • DNS discovery—The access point can discover switches through your domain name server (DNS). You must configure your DNS to return switch IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the access point domain name. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of switch IP addresses, the access point sends discovery requests to the switches.

### Restrictions for Configuring the Switch for Access Point Discovery

• Ensure that the switches are configured with the correct date and time. If the date and time configured on the switch precedes the creation and installation date of certificates on the access points, the access point fails to join the switch.

• During the discovery process, access points that are supported by the Cisco switch, such as the 1140, 1260, 3500, 1040, 1600, 2600, or 3600 query only for Cisco switches.

• Do not configure same VLAN for both wireless management and wireless clients.

### Information About Configuring the Switch for Access Point Discovery

In a CAPWAP environment, a lightweight access point discovers a switch by using CAPWAP discovery mechanisms and then sends a CAPWAP join request to the switch. The switch sends a CAPWAP join response to the access point that allows the access point to join the switch. When the access point joins the switch, the switch manages its configuration, firmware, control transactions, and data transactions.
Access Point Communication Protocols

Cisco lightweight access points use the IETF standard CAPWAP to communicate with the switch and other lightweight access points on the network.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a switch to manage a collection of wireless access points. CAPWAP is implemented in switch for these reasons:

- To provide an upgrade path from Cisco products that use LWAPP to next-generation Cisco products that use CAPWAP
- To manage RFID readers and similar devices
- To enable switches to interoperate with third-party access points in the future

Viewing Access Point Join Information

Join statistics for an access point that sends a CAPWAP discovery request to the switch at least once are maintained on the switch even if the access point is rebooted or disconnected. These statistics are removed only when the switch is rebooted or when you choose to clear the statistics.

Troubleshooting the Access Point Join Process

Access points can fail to join a switch for many reasons such as a RADIUS authorization is pending, self-signed certificates are not enabled on the switch, the access point and switch’s regulatory domains do not match, and so on.

You can configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the switch because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the switch until it receives a CAPWAP join request from the access point, so it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining issues without enabling CAPWAP debug commands on the switch, the switch collects information for all access points that send a discovery message to this switch and maintains information for any access points that have successfully joined this switch.

The switch collects all join-related information for each access point that sends a CAPWAP discovery request to the switch. Collection begins when the first discovery message is received from the access point and ends when the last configuration payload is sent from the switch to the access point.

When the switch is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

You can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all syslog messages to this IP address.

You can configure the syslog server IP address through the access point CLI, if the access point is not connected to the switch by entering the `capwap ap log-server syslog_server_IP_address` command.

When the access point joins a switch for the first time, the switch pushes the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address, until it is overridden by one of the following scenarios:
• The access point is still connected to the same switch, and you changed the global syslog server IP address configuration on the switch by using the `ap syslog host Syslog_Server_IP_Address` command. In this case, the switch pushes the new global syslog server IP address to the access point.

• The access point is still connected to the same switch, and you configured a specific syslog server IP address for the access point on the switch by using the `ap name Cisco_AP syslog host Syslog_Host_IP_Address` command. In this case, the switch pushes the new specific syslog server IP address to the access point.

• The access point gets disconnected from the switch, and you configured the syslog server IP address from the access point CLI by using the `capwap ap log-server syslog_server_IP_address` command. This command works only if the access point is not connected to any switch.

• The access point gets disconnected from the switch and joins another switch. In this case, the new switch pushes its global syslog server IP address to the access point.

Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all syslog messages to the new IP address, if the access point can reach the syslog server IP address.

How to Configure Access Point Discovery

Configuring the Syslog Server for Access Points (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show ap config global</td>
<td>Displays the global syslog server settings for all access points that join the switch.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show ap config global</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> show ap name Cisco_AP</td>
<td>Displays the syslog server settings for a specific access point.</td>
</tr>
<tr>
<td>config general</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show ap name AP03 config</td>
<td></td>
</tr>
<tr>
<td>general</td>
<td></td>
</tr>
</tbody>
</table>

Monitoring Access Point Join Information (CLI)

⚠️ Note

The procedure to perform this task using the switch GUI is not currently available.
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> show ap join stats summary</td>
<td>Displays the MAC addresses of all the access points that are joined to the switch or that have tried to join.</td>
</tr>
<tr>
<td>Example: Switch# show ap join stats summary</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show ap mac-address mac_address join stats summary</td>
<td>Displays all the statistics for the AP including the last join error detail.</td>
</tr>
<tr>
<td>Example: Switch# show ap mac-address 000.2000.0400 join stats summary</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> show ap mac-address mac_address join stats detailed</td>
<td>Displays all join-related statistics collected for a specific access point.</td>
</tr>
<tr>
<td>Example: Switch# show ap mac-address 000.2000.0400 join stats detailed</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> clear ap join statistics</td>
<td>Clears the join statistics for all access points.</td>
</tr>
<tr>
<td>Example: Switch# clear ap join statistics</td>
<td>Note To clear the join statistics that correspond to specific access points, enter the clear ap mac-address mac_address join statistics command.</td>
</tr>
</tbody>
</table>

## Related Topics
- Displaying the MAC Addresses of all Access Points: Example, on page 207
- DHCP Option 43 for Lightweight Cisco Aironet Access Points Configuration Example, on page 209

## Configuration Examples for Configuring the Switch for Access Point Discovery

### Displaying the MAC Addresses of all Access Points: Example

This example shows how to display MAC addresses of all the access points that are joined to the switch:

```
Switch# show ap join stats summary
Number of APs.......................................... 4

Base Mac EthernetMac AP Name IP Address Status
----------------- ----------------- ------- ------------- ----------
```

---

[Note]: #207

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
This example shows how to display the last join error details for a specific access point:

```
Switch# show ap mac-address 000.2000.0400 join stats summary
Is the AP currently connected to controller........... Yes
Time at which the AP joined this controller last time........ Aug 21 12:50:36.061
Type of error that occurred last..................... AP got or has been disconnected
Reason for error that occurred last................. The AP has been reset by the controller
Time at which the last join error occurred......... Aug 21 12:50:34.374
```

This example shows how to display all join-related statistics collected for a specific access point:

```
Switch# show ap mac-address 000.2000.0400 join stats detailed
Discovery phase statistics
- Discovery requests received.......................... 2
- Successful discovery responses sent.................. 2
- Unsuccessful discovery request processing......... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt.......... Aug 21 12:50:23.335
- Time at last unsuccessful discovery attempt......... Not applicable

Join phase statistics
- Join requests received................................ 1
- Successful join responses sent ..................... 1
- Unsuccessful join request processing ............. 1
- Reason for last unsuccessful join attempt .......... RADIUS authorization is pending for the AP
- Time at last successful join attempt............... Aug 21 12:50:34.481
- Time at last unsuccessful join attempt .......... Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received..................... 1
- Successful configuration responses sent ............ 1
- Unsuccessful configuration request processing...... 0
- Reason for last unsuccessful configuration attempt. Not applicable
- Time at last successful configuration attempt...... Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt.... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure.......... Not applicable

Last AP disconnect details
- Reason for last AP connection failure .............. The AP has been reset by the controller

Last join error summary
- Type of error that occurred last.................... AP got or has been disconnected
- Reason for error that occurred last................. The AP has been reset by the controller
- Time at which the last join error occurred.......... Aug 21 12:50:34.374
```
DHCP Option 43 for Lightweight Cisco Aironet Access Points Configuration Example

For more information about the AP join process, see DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example.

Configuring AP Pass Through

Information About AP Pass Through

AP pass through allows all the access points connected to Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches to join another controller on the network.

Prior to this release, all access points connected Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches would be terminated on the switch when the wireless management vlan is turned on. Unsupported access points connected to the switch were unable join a controller on a different vlan. AP pass through allows the connected AP to join another wireless controller on the network by assigning different vlan.

The advantages of AP pass through are:

- Allows partial deployment of Cisco New Generation Wireless Controllers where some APs are connected to Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches but other APs continue to join other controllers on the network.

- The APs that are not supported on the Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches are allowed to join other controllers on the network.

- The wireless LAN controller is used to provide access to both wired and wireless guests. AP Pass through allows the AP to pass through Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches to join any other controller when wired guest accessing is turned on.

Configuring AP Pass Through

All access points on VLANs other than the one with supported access points will be put into the AP pass-through mode and will not terminate on the Switch.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless management interface vlan vlan_id</td>
<td>Configures the ports that are connected to the supported access points with the wireless management VLAN</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring AP Pass Through

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# wireless management interface vlan10</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

<table>
<thead>
<tr>
<th>Step 3</th>
<th>interface GigabitEthernet1/0/1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# interface TenGigabitEthernet1/0/1</td>
</tr>
<tr>
<td></td>
<td>Sets the 10-Gigabit Ethernet interface. The command prompt changes from (config)# to (config-if)#.</td>
</tr>
</tbody>
</table>

**Step 4**

<table>
<thead>
<tr>
<th>Step 4</th>
<th>description Supported AP switchport access vlan_id</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# switchport access vlan10</td>
</tr>
<tr>
<td></td>
<td>Specifies the VLAN for which this access port will carry traffic</td>
</tr>
</tbody>
</table>

**Step 5**

<table>
<thead>
<tr>
<th>Step 5</th>
<th>description Unsupported AP switchport access vlan_id</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# switchport access vlan20</td>
</tr>
<tr>
<td></td>
<td>Configures the ports that are connected to the unsupported access points with a vlan other than the wireless management VLAN.</td>
</tr>
</tbody>
</table>
Configuring Data Encryption

- Finding Feature Information, on page 211
- Prerequisites for Configuring Data Encryption, on page 211
- Restrictions for Configuring Data Encryption, on page 211
- Information About Data Encryption, on page 212
- How to Configure Data Encryption, on page 212
- Configuration Examples for Configuring Data Encryption, on page 213

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Data Encryption

- Cisco 1260, 3500, 3600, 801, 1140, 1310, and 1520 series access points support Datagram Transport Layer Security (DTLS) data encryption.
- You can use the switch to enable or disable DTLS data encryption for a specific access point or for all access points.
- Non-Russian customers who use the Cisco switch do not need a data DTLS license.

Restrictions for Configuring Data Encryption

- Encryption limits throughput at both the switch and the access point, and maximum throughput is desired for most enterprise networks.
- If your switch does not have a data DTLS license and if the access point associated with the switch has DTLS enabled, the data path will be unencrypted.
Information About Data Encryption

The switch enables you to encrypt Control and Provisioning of Wireless Access Points (CAPWAP) control packets (and optionally, CAPWAP data packets) that are sent between the access point and the switch using DTLS. DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS. CAPWAP control packets are management packets exchanged between a switch and an access point while CAPWAP data packets encapsulate forwarded wireless frames. CAPWAP control and data packets are sent over separate UDP ports: 5246 (control) and 5247 (data). If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.

How to Configure Data Encryption

Configuring Data Encryption (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap link-encryption</td>
<td>Enables data encryption for all access points or a specific access point by entering this command. The default value is disabled. Changing the data encryption mode requires the access points to rejoin the switch.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# ap link-encryption</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show ap link-encryption</td>
<td>Displays the encryption state of all access points or a specific access point. This command also shows authentication errors, which track the number of integrity check failures and replay errors. Relay errors help in tracking the number of times the access point receives the same packet.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show ap link-encryption</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show wireless dtls connections</td>
<td>Displays a summary of all active DTLS connections.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- In images that do not have a DTLS license, the DTLS commands are not available.
Switch# show wireless dtls connections

If you experience any problems with DTLS data encryption, enter the debug dtls ap {all | event | trace} command to debug all DTLS messages, events, or traces.

Related Topics
Displaying Data Encryption States for all Access Points: Examples, on page 213

Configuring Data Encryption (GUI)

Procedure

Step 1 Choose Configuration > Wireless > Access Points > All APs.
The All APs page is displayed.

Step 2 Click the name of the access point for which you want to enable data encryption.
The AP > Edit page is displayed.

Step 3 Click the Advanced tab.

Step 4 Select or unselect the Data Encryption check box.

Note Changing the data encryption mode requires the access points to reassociate with the switch.

Step 5 Click Apply.

Step 6 Click Save Configuration.

Configuration Examples for Configuring Data Encryption

Displaying Data Encryption States for all Access Points: Examples

This example shows how to display the encryption state of all access points or a specific access point. This command also shows authentication errors, which track the number of integrity check failures and replay errors. Relay errors help in tracking the number of times the access point receives the same packet:

Switch# show ap link-encryption

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Encryption</th>
<th>Dnstream</th>
<th>Upstream</th>
<th>Last</th>
</tr>
</thead>
<tbody>
<tr>
<td>3602a</td>
<td>Enabled</td>
<td>0</td>
<td>0</td>
<td>Never</td>
</tr>
</tbody>
</table>

This example shows how to display a summary of all active DTLS connections:
Switch# show wireless dtls connections

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Local Port</th>
<th>Peer IP</th>
<th>Peer Port</th>
<th>Ciphersuite</th>
</tr>
</thead>
<tbody>
<tr>
<td>3602a</td>
<td>Capwap_Ctrl</td>
<td>10.10.21.213</td>
<td>46075</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>3602a</td>
<td>Capwap_Data</td>
<td>10.10.21.213</td>
<td>46075</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
</tbody>
</table>
Configuring Retransmission Interval and Retry Count

- Finding Feature Information, on page 215
- Prerequisites for Configuring the Access Point Retransmission Interval and Retry Count, on page 215
- Information About Retransmission Interval and Retry Count, on page 216
- How to Configure Access Point Retransmission Interval and Retry Count, on page 216
- Viewing CAPWAP Maximum Transmission Unit Information (CLI), on page 218
- Viewing CAPWAP Maximum Transmission Unit Information (GUI), on page 218
- Configuration Examples for Configuring Access Point Retransmission Interval and Retry Count, on page 219

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring the Access Point Retransmission Interval and Retry Count

- You can configure the retransmission intervals and retry count both at a global and a specific access point level. A global configuration applies these configuration parameters to all the access points. Alternatively, when you configure the retransmission level and retry count at a specific access point level, the values are applied to that particular access point. The access point specific configuration has a higher precedence than the global configuration.
Information About Retransmission Interval and Retry Count

The switch and the access points exchange packets using the Control and Provisioning of Wireless Access Points (CAPWAP) reliable transport protocol. For each request, a response is defined. This response is used to acknowledge the receipt of the request message. Response messages are not explicitly acknowledged; therefore, if a response message is not received, the original request message is retransmitted after the retransmit interval. If the request is not acknowledged after a maximum number of retransmissions, the session is closed and the access points reassociate with another switch.

How to Configure Access Point Retransmission Interval and Retry Count

Configuring the Access Point Retransmission Interval and Retry Count (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch# enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ap capwap retransmit interval interval_time</code></td>
<td>Configures the control packet retransmit interval for all access points globally. Note: The range for the interval parameter is from 2 to 5.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# ap capwap retransmit interval 2</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ap capwap retransmit count count_value</code></td>
<td>Configures the control packet retry count for all access points globally. Note: The range for the count is from 3 to 8.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# ap capwap retransmit count 3</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>ap name Cisco_AP capwap retransmit interval interval_time</code></td>
<td>Configures the control packet retransmit interval for the individual access point that you specify.</td>
</tr>
</tbody>
</table>
### Configuring the Access Point Retransmission Interval and Retry Count (GUI)

**Procedure**

- Global configuration applicable to all APs:
  a) Choose **Configuration > Wireless > Access Points > Global AP Configuration**.
     
     The **Global Configuration** page is displayed.
  
  b) In the **AP Retransmit Config Parameters** area, enter the values for the following parameters:
    
    • **AP Retransmit Count**—Number of times you want the access point to retransmit the request to the switch. The valid range is between 3 and 8.
    
    • **AP Retransmit Interval**—Duration between the retransmission of requests. The valid range is between 2 and 5.

  c) Click **Apply**.
  
  d) Click **Save Configuration**.

- Configuration that is applicable to a specific AP:
  a) Choose **Configuration > Wireless > Access Points > All APs**.
     
     The **All APs** page is displayed with a list of access points.
  
  b) Click the access point name.
     
     The **AP > Edit** page is displayed.
  
  c) Click the **Advanced** tab.
  
  d) In the **AP Retransmit Config Parameters** area, enter the values for the following **AP Retransmit Count** and **AP Retransmit Interval** parameters:
• **AP Retransmit Count**—Number of times you want the access point to retransmit the request to the switch. The valid range is between 3 and 8.

• **AP Retransmit Interval**—Duration between the retransmission of requests. The valid range is between 2 and 5.

e) Click **Apply**.
f) Click **Save Configuration**.

# Viewing CAPWAP Maximum Transmission Unit Information (CLI)

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# enable</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>show ap name Cisco_AP config general</code></td>
<td>Displays the maximum transmission unit (MTU) for the CAPWAP path on the switch. The MTU specifies the maximum size of any packet (in bytes) in a transmission.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>`Switch# show ap name Maria-1250 config general</td>
<td>include MTU`</td>
</tr>
</tbody>
</table>

## Related Topics

- Viewing the CAPWAP Retransmission Details: Example, on page 219
- Viewing Maximum Transmission Unit Information: Example, on page 219

# Viewing CAPWAP Maximum Transmission Unit Information (GUI)

## Procedure

1. Choose **Configuration > Wireless > Access Points > All APs**.
   - The **All APs** page is displayed.
2. Click the AP name.
   - The **AP > Edit** page is displayed.
3. Click the **Advanced** tab.
The CAPWAP MTU field shows the CAPWAP maximum retransmission unit information.

Configuration Examples for Configuring Access Point Retransmission Interval and Retry Count

Viewing the CAPWAP Retransmission Details: Example

Enter the following command:

```
Switch# show ap capwap retransmit
Global control packet retransmit interval : 3
Global control packet retransmit count : 5
```

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Retransmit Interval</th>
<th>Retransmit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>3602a</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

Viewing Maximum Transmission Unit Information: Example

This example shows how to view the maximum transmission unit (MTU) for the CAPWAP path on the switch. The MTU specifies the maximum size of any packet (in bytes) in a transmission:

```
Switch# show ap name cisco-ap-name config general | include MTU
CAPWAP Path MTU................................. 1500
```
Lightweight Access Point

Viewing Maximum Transmission Unit Information: Example
CHAPTER 15

Configuring Adaptive Wireless Intrusion Prevention System

- Finding Feature Information, on page 221
- Prerequisites for Configuring wIPS, on page 221
- How to Configure wIPS on Access Points, on page 222
- Monitoring wIPS Information, on page 224
- Configuration Examples for Configuring wIPS on Access Points, on page 224

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring wIPS

- The regular local mode access point has been extended with a subset of Wireless Intrusion Prevention System (wIPS) capabilities. This feature enables you to deploy your access points to provide protection without needing a separate overlay network.
# How to Configure wIPS on Access Points

## Configuring wIPS on an Access Point (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>ap name <em>Cisco_AP</em> mode local</td>
<td>Configures an access point for monitor mode. A message appears that indicates that changing the AP's mode causes the access point to reboot. This message also displays a prompt that enables you to specify whether or not you want to continue with changing the AP mode. Enter y at the prompt to continue.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# ap name AP01 mode local</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap name <em>Cisco_AP</em> dot11 5ghz shutdown</td>
<td>Enables the 802.11a radio on the access point.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# ap name AP01 dot11 5ghz shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ap name <em>Cisco_AP</em> dot11 24ghz shutdown</td>
<td>Enables the 802.11b radio on the access point.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# ap name AP02 dot11 24ghz shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ap name <em>Cisco_AP</em> mode monitor submode wips</td>
<td>Configures the wIPS submode on the access point.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# ap name AP01 mode monitor submode wips</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To disable wIPS on the access point, enter the ap name <em>Cisco_AP</em> modemonitor submode none command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ap name <em>Cisco_AP</em> monitor-mode wips-optimized</td>
<td>Enables wIPS optimized channel scanning for the access point. The access point scans each channel for 250 milliseconds. It derives the list of channels to be scanned from the monitor configuration. You can choose the following options:</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# ap name AP01 monitor-mode wips-optimized</td>
<td>- <strong>All</strong>—All channels supported by the access point’s radio.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Country</strong>—Only the channels supported by the access point’s country of operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>DCA</strong>—Only the channel set used by the dynamic channel assignment (DCA)</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz monitor</td>
<td>Displays the monitor configuration channel set.</td>
<td></td>
</tr>
<tr>
<td>Switch# show ap dot11 24ghz monitor</td>
<td><strong>Note</strong> The 802.11b Monitor Channels value in the output of the command indicates the monitor configuration channel set.</td>
<td></td>
</tr>
<tr>
<td>ap name Cisco_AP no dot11 5ghz shutdown</td>
<td>Enables the 802.11a radio on the access point.</td>
<td></td>
</tr>
<tr>
<td>Switch# ap name AP01 no dot11 5ghz shutdown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ap name Cisco_AP no dot11 24ghz shutdown</td>
<td>Enables the 802.11b radio on the access point.</td>
<td></td>
</tr>
<tr>
<td>Switch# ap name AP01 no dot11 24ghz shutdown</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring wIPS on an Access Point (GUI)

**Procedure**

**Step 1** Choose **Configuration > Wireless > Access Points > All APs**

The **All APs** page is displayed.

**Step 2** Click the access point name.

The **AP > Edit** page is displayed.

**Step 3** From the **AP Mode** drop-down list, choose one of the following options to configure the AP mode parameters:

- Local
- Monitor

**Step 4** From the **AP Sub Mode** drop-down list, choose **WIPS**.

**Step 5** Click **Apply**.

**Step 6** Click **Save Configuration**.
Monitoring wIPS Information

The procedure to perform this task using the switch GUI is not currently available.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>show ap name Cisco_AP config general</code></td>
<td>Displays information on the wIPS submode on the access point.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Switch# show ap name AP01 config general</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>show ap monitor-mode summary</code></td>
<td>Displays the wIPS optimized channel scanning configuration on the access point.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Switch# show ap monitor-mode summary</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>show wireless wps wips summary</code></td>
<td>Displays the wIPS configuration forwarded by NCS or Prime to the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Switch# show wireless wps wips summary</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>show wireless wps wips statistics</code></td>
<td>Displays the current state of wIPS operation on the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Switch# show wireless wps wips statistics</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>clear wireless wips statistics</code></td>
<td>Clears the wIPS statistics on the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Switch# clear wireless wips statistics</code></td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics
- Displaying the Monitor Configuration Channel Set: Example, on page 224
- Displaying wIPS Information: Examples, on page 225

### Configuration Examples for Configuring wIPS on Access Points

#### Displaying the Monitor Configuration Channel Set: Example

This example shows how to display the monitor configuration channel set:

```
Switch# show ap dot11 24ghz monitor
Default 802.11b AP monitoring
802.11b Monitor Mode............................. enable
802.11b Monitor Channels......................... Country channels
802.11b AP Coverage Interval.................... 180 seconds
```
Displaying wIPS Information: Examples

This example shows how to display information on the wIPS submode on the access point:

```
Switch# show ap name AP01 config general
Cisco AP Identifier.................... 3
Cisco AP Name........................ AP1131:46f2.98ac
...  
AP Mode ......................... Monitor
Public Safety ................... Disabled Disabled
AP SubMode ...................... WIPS
```

This example shows how to display the wIPS optimized channels scanning configuration on the access point:

```
Switch# show ap monitor-mode summary
AP Name Ethernet MAC Status Scanning
------------- -------------- -------- ---------
AP1131:4f2.9a 00:16:4:f2:9:a WIPS 1,6,NA,NA
```

This example shows how to display the wIPS configuration forwarded by WCS to the switch:

```
Switch# show wireless wps wips summary
Policy Name .................... Default
Policy Version................ 3
```

This example shows how to display the current state of wIPS operation on the switch:

```
Switch# show wireless wps wips statistics
Policy Assignment Requests............ 1
Policy Assignment Responses........... 1
Policy Update Requests................ 0
Policy Update Responses............... 0
Policy Delete Requests............... 0
Policy Delete Responses............... 0
Alarm Updates....................... 13572
Device Updates........................ 8376
Device Update Requests............ 0
Device Update Responses............ 0
Forensic Updates..................... 1001
Invalid WIPS Payloads............... 0
Invalid Messages Received........... 0
CAPWAP Enqueue Failed................ 0
NMSP Enqueue Failed.................. 0
NMSP Transmitted Packets........... 22950
NMSP Transmit Packets Dropped....... 0
NMSP Largest Packet.................. 1377
```
Displaying wiPS Information: Examples
Configuring Authentication for Access Points

• Finding Feature Information, on page 227
• Prerequisites for Configuring Authentication for Access Points, on page 227
• Restrictions for Configuring Authentication for Access Points, on page 228
• Information about Configuring Authentication for Access Points, on page 228
• How to Configure Authentication for Access Points, on page 228
• Configuration Examples for Configuring Authentication for Access Points, on page 234

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Authentication for Access Points

• You can set a global username, password, and enable password for all access points that are currently joined to the switch and any that join in the future inherit as they join the switch. If desired, you can override the global credentials and assign a unique username, password, and enable password for a specific access point.

• After an access point joins the switch, the access point enables console port security, and you are prompted for your username and password whenever you log into the access point’s console port. When you log in, you are in nonprivileged mode, and you must enter the enable password in order to use the privileged mode.

• The global credentials that you configure on the switch are retained across switch and access point reboots. They are overwritten only if the access point joins a new switch that is configured with a global username and password. If the new switch is not configured with global credentials, the access point retains the global username and password configured for the first switch.

• You must track the credentials used by the access points. Otherwise, you might not be able to log into an access point’s console port. If you need to return the access points to the default Cisco/Cisco username
and password, you must clear the switch’s configuration and the access point’s configuration to return them to factory-default settings. To reset the default access point configuration, enter the `ap name Cisco_AP mgmtuser username Cisco password Cisco` command. Entering the command does not clear the static IP address of the access point. Once the access point rejoins a switch, it adopts the default Cisco/Cisco username and password.

- You can configure global authentication settings for all access points that are currently joined to the switch and any that join in the future. If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.

- This feature is supported on the following hardware:
  - All Cisco switches that support authentication.
  - Cisco Aironet 1140, 1260, 1310, 1520, 1600, 2600, 3500, and 3600 access points

### Restrictions for Configuring Authentication for Access Points

- The switch name in the AP configuration is case sensitive. Therefore, make sure to configure the exact system name on the AP configuration. Failure to do this results in the AP fallback not working.

### Information about Configuring Authentication for Access Points

Cisco IOS access points are shipped from the factory with `Cisco` as the default enable password. This password allows users to log into the nonprivileged mode and enter the `show` and `debug` commands that pose a security threat to your network. You must change the default enable password to prevent unauthorized access and to enable users to enter configuration commands from the access point’s console port.

You can configure 802.1X authentication between a lightweight access point and a Cisco switch. The access point acts as an 802.1X supplicant and is authenticated by the switch where it uses EAP-FAST with anonymous PAC provisioning.

### How to Configure Authentication for Access Points

#### Configuring Global Credentials for Access Points (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch# enable</code></td>
</tr>
<tr>
<td></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td></td>
<td>Enter privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring Global Credentials for Access Points (CLI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>ap mgmtuser username user_name password 0 password secret 0 secret_value</code></td>
<td>Configures the global username and password and enables the password for all access points that are currently joined to the switch and any access points that join the switch in the future. In the command, the parameter 0 specifies that an unencrypted password will follow and 8 specifies that an AES encrypted password will follow.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>ap mgmtuser apusr1 password appass 0 secret 0 appass1</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>ap name Cisco_AP mgmtuser username user_name password password secret secret</code></td>
<td>Overrides the global credentials for a specific access point and assigns a unique username and password and enables password to this access point. The credentials that you enter in this command are retained across switch and access point reboots and if the access point joins a new switch.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>ap name TSIM_AP-2 mgmtuser apusr1 password appass secret secret</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you want to force this access point to use the switch’s global credentials, enter the <code>ap name Cisco_AP no mgmtuser</code> command. The following message appears after you execute this command: “AP reverted to global username configuration.”</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>show ap summary</code></td>
<td>Displays a summary of all connected Cisco APs.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# <code>show ap summary</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>show ap name Cisco_AP config general</code></td>
<td>Displays the global credentials configuration for a specific access point.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# <code>show ap name AP02 config general</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If this access point is configured for global credentials, the AP User Mode text boxes shows “Automatic.” If the global credentials have been overwritten for this access point, the AP User Mode text box shows “Customized.”</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring Authentication for Access Points (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ap dot1x username user_name_value password 0 password_value</code></td>
<td>Configures the global authentication username and password for all access points that are currently joined to the switch and any access points that join the switch in the future. This command contains the following keywords and arguments:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>ap dot1x username AP3 password 0 password</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>You must enter a strong password for the password parameter. Strong passwords are at least eight characters long, contain a combination of uppercase and lowercase letters, numbers, and symbols, and are not a word in any language.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>ap name Cisco_AP dot1x-user username username_value password password_value</code></td>
<td>Overrides the global authentication settings and assigns a unique username and password to a specific access point. This command</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| Switch# ap name AP03 dot1x-user username apuser1 password appass | contains the following keywords and arguments:  
- **username**—Specifies to add a username.  
- **user-id**—Username.  
- **password**—Specifies to add a password.  
- **0**—Specifies an unencrypted password.  
- **8**— Specifies an AES encrypted password.  
- **passwd**—Password. |

**Note** You must enter a strong password for the password parameter. See the note in Step 2 for the characteristics of strong passwords.

The authentication settings that you enter in this command are retained across switch and access point reboots and whenever the access point joins a new switch.

| Step 6 | **configure terminal**  
Example:  
Switch# configure terminal | Enters global configuration mode. |

| Step 7 | **no ap dot1x username user_name_value password 0 password_value**  
Example:  
Switch(config)# no ap dot1x username dot1xusr password 0 dot1xpass | Disables 802.1X authentication for all access points or for a specific access point.  
The following message appears after you execute this command: “AP reverted to global username configuration.” |

**Note** You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

| Step 8 | **end**  
Example:  
Switch(config)# end | Returns to privileged EXEC mode.  
Alternatively, you can also press Ctrl-Z to exit global configuration mode. |

| Step 9 | **show ap summary**  
Example: | Displays the authentication settings for all access points that join the switch. |
### Configuring the Switch for Authentication (CLI)

#### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# show ap summary</td>
<td>Note If global authentication settings are not configured, the Global AP Dot1x User Name text box shows “Not Configured.”</td>
</tr>
</tbody>
</table>

**Step 10**

**show ap name Cisco_AP** config general  
**Example:**  
Switch# show ap name AP02 config general

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the authentication settings for a specific access point.</td>
<td></td>
</tr>
</tbody>
</table>

**Note** If this access point is configured for global authentication, the AP Dot1x User Mode text boxes shows “Automatic.” If the global authentication settings have been overwritten for this access point, the AP Dot1x User Mode text box shows “Customized.”

### Related Topics

- Displaying the Authentication Settings for Access Points: Examples, on page 234

---

**Note**

The procedure to perform this task using the switch GUI is not currently available.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
</tbody>
</table>
| Example:  
Switch# enable | |
| Step 2 configure terminal | Enters global configuration mode. |
| Example:  
Switch# configure terminal | |
| Step 3 dot1x system-auth-control | Enables system authentication control. |
| Example:  
Switch(config)# dot1x system-auth-control | |
| Step 4 aaa new-model | Enables new access control commands and functions. |
| Example:  
Switch(config)# aaa new-model | |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> aaa authentication dot1x default group radius</td>
<td>Sets the default authentications lists for IEEE 802.1X by using all the radius hosts in a server group.</td>
</tr>
<tr>
<td><strong>Step 6</strong> radius server server name</td>
<td>(Optional) Specifies the RADIUS server parameters. For <strong>auth-port port_number</strong>, specify the UDP destination port for authentication requests. The default is 1645. The range is 0 to 65536. For <strong>acct-port port_number</strong>, specify the UDP destination port for authentication requests. The default is 1646.</td>
</tr>
<tr>
<td><strong>Step 7</strong> address {ipv4</td>
<td>ipv6} ip_address {auth-port port_number</td>
</tr>
<tr>
<td><strong>Step 8</strong> key unencrypted_server_key</td>
<td>Exits the RADIUS server mode and enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 9</strong> exit</td>
<td>Sets the 10-Gigabit Ethernet interface. The command prompt changes from Controller(config)# to Controller(config-if)#.</td>
</tr>
<tr>
<td><strong>Step 10</strong> interface TenGigabitEthernet1/0/1</td>
<td>Sets the unconditional trunking mode access to the interface.</td>
</tr>
<tr>
<td><strong>Step 11</strong> switch mode access</td>
<td>Sets the 802.1X interface PAE type as the authenticator.</td>
</tr>
<tr>
<td><strong>Step 12</strong> dot1x pae authenticator</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 13</strong> end</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

Switch(config)# aaa authentication dot1x default group radius

Switch(config)# radius server rsim

Switch(config)# address ipv4 124.2.2.12 auth-port 1612

Switch(config)# key encryptkey

Switch(config)# exit

Switch(config)# interface TenGigabitEthernet1/0/1

Switch(config)# switch mode access

Switch(config)# dot1x pae authenticator

Switch(config)# end
Configuration Examples for Configuring Authentication for Access Points

Displaying the Authentication Settings for Access Points: Examples

This example shows how to display the authentication settings for all access points that join the switch:

Switch# show ap summary
Number of APs................................. 1
Global AP User Name.......................... globalap
Global AP Dot1x User Name.................. globalDot1x

This example shows how to display the authentication settings for a specific access point:

Switch# show ap name AP02 config dot11 24ghz general
Cisco AP Identifier.......................... 0
Cisco AP Name.................................. TSIM_AP2
AP Dot1x User Mode............................ AUTOMATIC
AP Dot1x User Name............................ globalDot1x
CHAPTER 17

Converting Autonomous Access Points to Lightweight Mode

- Finding Feature Information, on page 235
- Guidelines for Converting Autonomous Access Points to Lightweight Mode, on page 235
- Information About Autonomous Access Points Converted to Lightweight Mode, on page 236
- How to Convert a Lightweight Access Point Back to an Autonomous Access Point, on page 238
- Authorizing Access Points (CLI), on page 239
- Authorizing Access Points (GUI), on page 240
- Disabling the Reset Button on Converted Access Points (CLI), on page 240
- Monitoring the AP Crash Log Information, on page 241
- How to Configure a Static IP Address on an Access Point, on page 242
- Recovering the Access Point Using the TFTP Recovery Procedure, on page 244
- Configuration Examples for Converting Autonomous Access Points to Lightweight Mode, on page 244

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Guidelines for Converting Autonomous Access Points to Lightweight Mode

- Access points that are converted to lightweight mode do not support Wireless Domain Services (WDS). Converted access points communicate only with Cisco wireless LAN switches and cannot communicate with WDS devices. However, the switch provides functionality that is equivalent to WDS when an access point is associated to it.
• All Cisco lightweight access points support 16 Basic Service Set Identifiers (BSSIDs) per radio and a total of 16 wireless LANs per access point. When a converted access point is associated to a switch, only wireless LANs with IDs 1 through 16 are pushed to the access point, unless the access point is a member of an access point group.

• Access points that are converted to lightweight mode must get an IP address and discover the switch using DHCP, DNS, or IP subnet broadcast.

Information About Autonomous Access Points Converted to Lightweight Mode

You can convert autonomous Cisco Aironet access points to lightweight mode. When you upgrade the access points to lightweight mode, the access point communicates with the switch and receives a configuration and software image from the switch.

Reverting from Lightweight Mode to Autonomous Mode

After you convert an autonomous access point to lightweight mode, you can convert the access point from a lightweight unit back to an autonomous unit by loading a Cisco IOS release that supports autonomous mode (Cisco IOS Release 12.3(7)JA or earlier releases). If the access point is associated with a switch, you can use the switch to load the Cisco IOS release. If the access point is not associated to a switch, you can load the Cisco IOS release using TFTP. In either method, the access point must be able to access a TFTP server that contains the Cisco IOS release to be loaded.

Using DHCP Option 43 and DHCP Option 60

Cisco Aironet Access Points use the type-length-value (TLV) format for DHCP option 43. You must program the DHCP servers to return the option based on the access point’s DHCP Vendor Class Identifier (VCI) string (DHCP option 60).

See the product documentation for your DHCP server for instructions on configuring DHCP option 43. The Converting Autonomous Access Points to Lightweight Mode document contains example steps for configuring option 43 on a DHCP server.

If the access point is ordered with the Service Provider Option - AIR-OPT60-DHCP selected, the VCI string for that access point will be different than those strings listed in the previous table. The VCI string has the following suffix: ServiceProvider, for example, a 1260 with this option returns the VCI string Cisco AP c1260-ServiceProvider.

Note

Ensure that the switch IP address that you obtain from the DHCP server is a unicast IP address. Do not configure the switch IP address as a multicast address when configuring DHCP option 43.

Restrictions for DHCP Option 60

• Cisco Wave2 APs support strings with length up to 256 characters only.
When the string length exceeds the limit, the default value is sent during the DHCP discover process.

How Converted Access Points Send Crash Information to the Switch

When a converted access point unexpectedly reboots, the access point stores a crash file on its local flash memory at the time of the crash. After the unit reboots, it sends the reason for the reboot to the switch. If the unit rebooted because of a crash, the switch pulls up the crash file using existing CAPWAP messages and stores it in the switch flash memory. The crash information copy is removed from the access point flash memory when the switch pulls it from the access point.

Uploading Memory Core Dumps from Converted Access Points

By default, access points converted to lightweight mode do not send memory core dumps to the switch. This section provides instructions to upload access point core dumps using the switch GUI or CLI.

Displaying MAC Addresses for Converted Access Points

There are some differences in the way that controllers display the MAC addresses of converted access points on information pages in the controller GUI:

- On the AP Summary window, the controller lists the Ethernet MAC addresses of the converted access points.
- On the AP Detail window, the controller lists the BSS MAC addresses and Ethernet MAC addresses of the converted access points.
- On the Radio Summary page, the switch lists converted access points by the radio MAC address.

Configuring a Static IP Address for a Lightweight Access Point

If you want to specify an IP address for an access point rather than having one assigned automatically by a DHCP server, you can use the controller GUI or CLI to configure a static IP address for the access point. Static IP addresses are generally used only for deployments with a limited number of APs.

An access point cannot discover the switch using domain name system (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs. You can configure these parameters using either the switch CLI or the GUI.

If you configure an access point to use a static IP address that is not on the same subnet on which the access point’s previous DHCP address was, the access point falls back to a DHCP address after the access point reboots. If the access point falls back to a DHCP address, enter the show ap config general Cisco AP CLI command to show that the access point is using a fallback IP address. However, the GUI shows both the static IP address and the DHCP address, but it does not identify the DHCP address as a fallback address.
How to Convert a Lightweight Access Point Back to an Autonomous Access Point

Converting a Lightweight Access Point Back to an Autonomous Access Point (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# enable</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2** ap name Cisco_AP tftp-downgrade tftp_server_ip_address tftp_server_image_filename

**Example:**

Switch# ap name AP02 tftp-downgrade 10.0.0.1 tsrvname

**Converting a Lightweight Access Point Back to an Autonomous Access Point (Using the Mode Button and a TFTP Server)**

**Procedure**

1. Configure the PC on which your TFTP server software runs with a static IP address in the range of 10.0.0.2 to 10.0.0.30.
2. Make sure that the PC contains the access point image file (such as c1140-k9w7-tar.123-7.JA.tar for a 1140 series access point) in the TFTP server folder and that the TFTP server is activated.
3. Rename the access point image file in the TFTP server folder to c1140-k9w7-tar.default for a 1140 series access point.
4. Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.
5. Disconnect power from the access point.
6. Press and hold the **MODE** button while you reconnect power to the access point.

**Note** The **MODE** button on the access point must be enabled.

7. Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the **MODE** button.
Step 8  Wait until the access point reboots as indicated by all the LEDs turning green followed by the Status LED blinking green.
Step 9  After the access point reboots, reconfigure the access point using the GUI or the CLI.

## Authorizing Access Points (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ap auth-list ap-policy authorize-ap</code></td>
<td>Configures an access point authorization policy.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ap auth-list ap-policy authorize-ap</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>username user_name mac aaa attribute list list_name</code></td>
<td>Configures the MAC address of an access point locally.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# username aaa.bbb.ccc mac aaa attribute list attrlist</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>aaa new-model</code></td>
<td>Enables new access control commands and functions.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>aaa authorization credential-download auth_list local</code></td>
<td>Downloads EAP credentials from the local server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa authorization credential-download auth_download local</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>aaa attribute list list</code></td>
<td>Configures AAA attribute list definitions.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa attribute list alist</td>
<td></td>
</tr>
</tbody>
</table>
## Authorizing Access Points (GUI)

### Procedure

**Step 1**
Choose **Configuration > Security > AAA > AP Policy**.

The **AP Policy** page is displayed.

**Step 2**
In the Policy Configuration area, enable or disable the following parameters:

- Authorize LSC APs against Auth-List
- AP with Self-Signed Certificate
- Authorize MIC APs against AAA
- AP with Manufacturing Installed Certificate

**Step 3**
Click **Apply**.

**Step 4**
Click **Save Configuration**.

## Disabling the Reset Button on Converted Access Points (CLI)

You can enable or disable the **Reset** button on access points that are converted to lightweight mode. The **Reset** button is labeled **MODE** on the outside of the access point.

### Note
The procedure to perform this task using the controller GUI is not currently available.
### Monitoring the AP Crash Log Information

The procedure to perform this task using the switch GUI is not currently available.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# enable</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal | Enters global configuration mode.  |
| **Example:** Switch# configure terminal | |

| **Step 3** no ap reset-button | Disables the Reset buttons on all converted access points that are associated to the switch.  |
| **Example:** Switch(config)# no ap reset-button | **Note** To enable the Reset buttons on all the converted access points that are associated to the switch, enter the ap reset-button command. |

| **Step 4** end | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.  |
| **Example:** Switch(config)# end | |

| **Step 5** ap name cisco_ap reset-button | Enables the Reset button on the converted access point that you specify.  |
| **Example:** Switch# ap name AP02 reset-button | |
## How to Configure a Static IP Address on an Access Point

### Configuring a Static IP Address on an Access Point (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# enable</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>ap name Cisco_AP static-ip ip-address</code></td>
<td>Configures a static IP address on the access point. This command contains the following keywords and arguments:</td>
</tr>
<tr>
<td></td>
<td><code>static_ip_address netmask static_ip_netmask</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>gateway static_ip_gateway</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# ap name AP03 static-ip ip-address</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# enable</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>ap static-ip name-server nameserver_ip_address</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><em>Switch(config)# ap static-ip name-server 10.10.10.205</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configures a DNS server so that a specific access point or all access points can discover the switch using DNS resolution.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To undo the DNS server configuration, enter the <strong>no ap static-ip name-server nameserver_ip_address</strong> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>ap static-ip domain static_ip_domain</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><em>Switch(config)# ap static-ip domain domain1</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configures the domain to which a specific access point or all access points belong.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To undo the domain name configuration, enter the <strong>no ap static-ip domain static_ip_domain</strong> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>end</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><em>Switch(config)# end</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>show ap name Cisco_AP config general</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><em>Switch# show ap name AP03 config general</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Displays the IP address configuration for the access point.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring a Static IP Address on an Access Point (GUI)

**Procedure**

1. **Step 1** Choose **Configuration > Wireless > Access Points > All APs.**
   
The **All APs** page is displayed.

2. **Step 2** Click the name of the access point.
   
The **AP > Edit** page is displayed.

3. **Step 3** In the **General** tab, in the **IP Config** area, select the **Static IP** check box if you want to assign a static IP address to the access point.

4. **Step 4** Enter the following details:
   
   • **Static IP**
   • **Netmask**
   • **Gateway**

5. **Step 5** Click **Apply**.
The access point reboots and rejoins the switch, and the static IP address that you specified is sent to the access point.

**Step 6** After the static IP address has been sent to the access point, configure the **DNS IP Address** and **Domain Name**.

**Step 7** Click **Apply**.

**Step 8** Click **Save Configuration**.

---

**Recovering the Access Point Using the TFTP Recovery Procedure**

**Procedure**

**Step 1** Download the required recovery image from Cisco.com (ap3g2-k9w8-tar.152-2.JA.tar) and install it in the root directory of your TFTP server.

**Step 2** Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the switch to download the oversized access point image and complete the upgrade procedure.

**Step 3** After the access point has been recovered, you can remove the TFTP server.

---

**Configuration Examples for Converting Autonomous Access Points to Lightweight Mode**

**Example: Displaying the IP Address Configuration for Access Points**

This example shows how to display the IP address configuration for an access point:

```
Switch# show ap name AP03 dot11 24ghz config general
Cisco AP Identifier.............. 4
Cisco AP Name............................. AP6
IP Address Configuration.............. Static IP assigned
IP Address................................ 10.10.10.118
IP NetMask................................ 255.255.255.0
Gateway IP Addr........................... 10.10.10.1
Domain.................................... Domain1
Name Server............................... 10.10.10.205
...
```

---
Example: Displaying Access Point Crash File Information

This example shows how to display access point crash file information. Using this command, you can verify whether the file is downloaded to the switch.

Switch# `show ap crash-file`
Local Core Files:
lrad_AP1130.rdump0 (156)

The number in parentheses indicates the size of the file. The size should be greater than zero if a core dump file is available.
Example: Displaying Access Point Crash File Information
CHAPTER 18

Using Cisco Workgroup Bridges

• Finding Feature Information, on page 247
• Information About Cisco Workgroup Bridges and non-Cisco Workgroup bridges, on page 247
• Monitoring the Status of Workgroup Bridges, on page 248
• Debugging WGB Issues (CLI), on page 248
• Configuration Examples for Configuring Workgroup Bridges, on page 249

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Cisco Workgroup Bridges and non-Cisco Workgroup bridges

A WGB is a mode that can be configured on an autonomous Cisco IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging. The WGB provides wireless access connectivity to wired clients by establishing a single wireless connection to the lightweight access point.

When a Cisco WGB is used, the WGB informs the access points of all the clients that it is associated with. The switch is aware of the clients that are associated with the access point. When non-Cisco WGBs are used, the switch has no information about the IP address of the clients on the wired segment behind the WGB. Without this information, the switch drops the following types of messages:

• ARP REQ from the distribution system for the WGB client.
• ARP RPLY from the WGB client.
• DHCP REQ from the WGB client.
• DHCP RPLY for the WGB client.

Monitoring the Status of Workgroup Bridges

The procedure to perform this task using the switch GUI is not currently available.

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command or Action</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
</tbody>
</table>

Debugging WGB Issues (CLI)

The procedure to perform this task using the switch GUI is not currently available.

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command or Action</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Command or Action</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td><strong>Step 3</strong> debug iapp error</td>
</tr>
<tr>
<td>Example: Switch# debug iapp error</td>
</tr>
<tr>
<td><strong>Step 4</strong> debug iapp packet</td>
</tr>
<tr>
<td>Example: Switch# debug iapp packet</td>
</tr>
<tr>
<td><strong>Step 5</strong> debug mobility handoff [switch switch_number]</td>
</tr>
<tr>
<td>Example: Switch# debug mobility handoff</td>
</tr>
<tr>
<td><strong>Step 6</strong> debug dhcp</td>
</tr>
<tr>
<td>Example: Switch# debug dhcp</td>
</tr>
<tr>
<td><strong>Step 7</strong> debug dot11 mobile</td>
</tr>
<tr>
<td>Example: Switch# debug dot11 mobile</td>
</tr>
<tr>
<td><strong>Step 8</strong> debug dot11 state</td>
</tr>
<tr>
<td>Example: Switch# debug dot11 state</td>
</tr>
</tbody>
</table>
Verify that the WGB is associated to an access point by entering this command on the WGB:

**show dot11 association**

Information similar to the following appears:

```
Switch# show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address  IP address  Device  Name  Parent  State
000b.8581.6aee  10.11.12.1  WGB-client  map1  -  Assoc
ap#  
```
CHAPTER 19

Configuring Probe Request Forwarding

- Finding Feature Information, on page 251
- Information About Configuring Probe Request Forwarding, on page 251
- How to Configure Probe Request Forwarding (CLI), on page 251

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Probe Request Forwarding

Probe requests are 802.11 management frames that are sent by clients to request information about the capabilities of Service Set Identifiers (SSIDs). By default, access points forward acknowledged probe requests to the switch for processing. Acknowledged probe requests are probe requests for SSIDs that are supported by the access point. If desired, you can configure access points to forward both acknowledged and unacknowledged probe requests to the switch. The switch can use the information from unacknowledged probe requests to improve the location accuracy.

How to Configure Probe Request Forwarding (CLI)

Note
The procedure to perform this task using the switch GUI is not currently available.
## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless probe filter</td>
<td>Enables or disables the filtering of probe requests forwarded from an access point to the switch.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# wireless probe filter</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>If you enable probe filtering, the default filter setting, the access point forwards only acknowledged probe requests to the switch. If you disable probe filtering, the access point forwards both acknowledged and unacknowledged probe requests to the switch.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>wireless probe limit num_probes interval</td>
<td>Limits the number of probe requests sent to the switch per client per access point radio in a given interval. You must specify the following arguments with this command:</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# wireless probe limit 10 1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• num_probes—Number of probe requests forwarded to the switch per client per access point radio in a given interval. The range is from 1 to 100.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• interval—Probe limit interval in milliseconds. The range is from 100 to 10000.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>show wireless probe</td>
<td>Displays the advanced probe request configuration.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# show wireless probe</td>
<td></td>
</tr>
</tbody>
</table>
Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Optimizing RFID Tracking on Access Points

To optimize the monitoring and location calculation of RFID tags, you can enable tracking optimization on up to four channels within the 2.4-GHz band of an 802.11b/g access point radio. This feature allows you to scan only the channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

How to Optimize RFID Tracking on Access Points

Optimizing RFID Tracking on Access Points (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>ap name Cisco_AP mode monitor submode none</td>
<td>Specifies the monitor submode for the access point as none.</td>
</tr>
</tbody>
</table>

Example:
### Configuration Examples for Optimizing RFID Tracking

#### Displaying all the Access Points in Monitor Mode: Example

This example shows how to display all the access points in monitor mode:

1. **Step 2**
   - `ap name Cisco_AP dot11 24ghz shutdown`
   - Example:
     - `Switch# ap name AP01 dot11 24ghz shutdown`
   - Disables the access point radio.

2. **Step 3**
   - `ap name Cisco_AP monitor-mode tracking-opt`
   - Example:
     - `Switch# ap name TSIM_AP1 monitor-mode tracking-opt`
   - Configures the access point to scan only the Dynamic Channel Assignment (DCA) channels supported by its country of operation.

3. **Step 4**
   - `ap name Cisco_AP monitor-mode dot11b {fast-channel [first_channel second_channel third_channel fourth_channel]}`
   - Example:
     - `Switch# ap name AP01 monitor-mode dot11b fast-channel 1 2 3 4`
   - Chooses up to four specific 802.11b channels to be scanned by the access point.

4. **Step 5**
   - `ap name Cisco_AP no dot11 24ghz shutdown`
   - Example:
     - `Switch# ap name AP01 no dot11 24ghz shutdown`
   - Enables the access point radio.

5. **Step 6**
   - `show ap monitor-mode summary`
   - Example:
     - `Switch# show ap monitor-mode summary`
   - Displays all the access points in monitor mode.
Switch# `show ap monitor-mode summary`

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Ethernet MAC</th>
<th>Status</th>
<th>Scanning Channel List</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP113:4f2.9a 00:16:4:f2:9:a</td>
<td>Tracking 1,6,NA,NA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Displaying all the Access Points in Monitor Mode: Example
CHAPTER 21

Country Codes

- Finding Feature Information, on page 257
- Information About Country Codes, on page 257
- Prerequisites for Configuring Country Codes, on page 258
- How to Configure Country Codes, on page 258
- Configuration Examples for Configuring Country Codes, on page 260

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Country Codes

Controllers and access points are designed for use in many countries with varying regulatory requirements. The radios within the access points are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation (such as FR for France or ES for Spain). Configuring a country code ensures that each radio’s broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

Information About Japanese Country Codes

Country codes define the channels that can be used legally in each country. These country codes are available for Japan:

- JP—Allows only -J radios to join the controller
- J2—Allows only -P radios to join the controller
- J3—Uses the -U frequencies, but allows -U, -P, and -Q (other than 1550/1600/2600/3600) radios to join the WLC
- J4—Allows 2.4G JPQU and 5G PQU to join the controller.
Prerequisites for Configuring Country Codes

• Generally, you should configure one country code per switch; you configure one code that matches the physical location of the switch and its access points. You can configure up to 20 country codes per switch. This multiple-country support enables you to manage access points in various countries from a single switch.

• When the multiple-country feature is used, all the switches that are going to join the same RF group must be configured with the same set of countries, configured in the same order.

• Access points are capable of using all the available legal frequencies. However, access points are assigned to the frequencies that are supported in their relevant domains.

• The country list configured on the RF group leader determines which channels the members will operate on. This list is independent of which countries have been configured on the RF group members.

• For switches in the Japan regulatory domain, you should have one or more Japan country codes (JP, J2, or J3) configured on your switch at the time you last booted your switch.

• For switches in the Japan regulatory domain, you must have at least one access point with a -J regulatory domain joined to your switch.

How to Configure Country Codes

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>show wireless country supported</td>
<td>Displays a list of all the available country codes.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# show wireless country supported</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
## How to Configure Country Codes

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td><code>ap dot11 24ghz shutdown</code></td>
<td>Disables the 802.11b/g network.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# ap dot11 5ghz shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>ap dot11 5ghz shutdown</code></td>
<td>Disables the 802.11a network.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# ap dot11 24ghz shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>ap country country_code</code></td>
<td>Assigns access points to a specific country. <strong>Note</strong> Make sure that the country code you choose is compatible with the regulatory domain of at least one of the access point’s radios.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# ap country IN</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>show wireless country channels</code></td>
<td>Displays the list of available channels for the country codes configured on your switch. <strong>Note</strong> Perform Steps 9 through 17 only if you have configured multiple country codes in Step 6.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show wireless country channels</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>no ap dot11 5ghz shutdown</code></td>
<td>Enables the 802.11a network.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# no ap dot11 5ghz shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><code>no ap dot11 24ghz shutdown</code></td>
<td>Enables the 802.11b/g network.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# no ap dot11 24ghz shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><code>ap name cisco-ap shutdown</code></td>
<td>Disables the access point.</td>
</tr>
</tbody>
</table>
### Configuration Examples for Configuring Country Codes

#### Displaying Channel List for Country Codes: Example

This example shows how to display the list of available channels for the country codes configured on your switch:

```
Switch# show wireless country channels
```

Configured Country.........................: US - United States
KEY: * = Channel is legal in this country and may be configured manually.
    A = Channel is the Auto-RF default in this country.
<table>
<thead>
<tr>
<th>Wireless Standard</th>
<th>Channels</th>
<th>(-A , -AB) US</th>
<th>Auto-RF</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11bg</td>
<td>1 1 1 1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 2 3 4 5 6 7 8 9 0 1 2 3 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11a</td>
<td>3 3 4 4 4 4 4 4 5 5 6 6 0 0 0 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.9GHz 802.11a</td>
<td>1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Explanation:
- `.` = Channel is not legal in this country.
- `C` = Channel has been configured for use by Auto-RF.
- `x` = Channel is available to be configured for use by Auto-RF.
- `(-,)` = (indoor, outdoor) regulatory domain allowed by this country.
Displaying Channel List for Country Codes: Example
Configuring Link Latency

- Finding Feature Information, on page 263
- Prerequisites for Configuring Link Latency, on page 263
- Restrictions for Configuring Link Latency, on page 263
- Information About Configuring Link Latency, on page 264
- How to Configure Link Latency, on page 265
- How to Configure TCP MSS, on page 268
- Performing a Link Test (CLI), on page 269
- Configuration Examples for Configuring Link Latency, on page 270

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Link Latency

- The switch displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the switch is up or can be cleared and allowed to restart.
- You can configure link latency for a specific access point using the switch GUI or CLI or for all access points joined to the switch using the CLI.

Restrictions for Configuring Link Latency

- Link latency calculates the Control and Provisioning of Wireless Access Points (CAPWAP) response time between the access point and the switch. It does not measure network latency or ping responses.
Information About Configuring Link Latency

You can configure link latency on the switch to measure the link between an access point and the switch. You can use this feature with all access points that are joined to the switch where the link can be a slow or unreliable WAN connection.

TCP MSS

If the client’s maximum segment size (MSS) in a Transmission Control Protocol (TCP) three-way handshake is greater than the maximum transmission unit can handle, the client might experience reduced throughput and the fragmentation of packets. To avoid this problem, you can specify the MSS for all access points that are joined to the switch or for a specific access point.

When you enable this feature, the access point selects the MSS for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

Link Tests

A link test is used to determine the quality of the radio link between two devices. Two types of link-test packets are transmitted during a link test: request and response. Any radio receiving a link-test request packet fills in the appropriate text boxes and echoes the packet back to the sender with the response type set.

The radio link quality in the client-to-access point direction can differ from that in the access point-to-client direction due to the asymmetrical distribution of the transmit power and receive sensitivity on both sides. Two types of link tests can be performed: a ping test and a CCX link test.

With the ping link test, the controller can test link quality only in the client-to-access point direction. The RF parameters of the ping reply packets received by the access point are polled by the controller to determine the client-to-access point link quality.

With the CCX link test, the switch can also test the link quality in the access point-to-client direction. The switch issues link-test requests to the client, and the client records the RF parameters (received signal strength indicator [RSSI], signal-to-noise ratio [SNR], and so on) of the received request packet in the response packet. Both the link-test requestor and responder roles are implemented on the access point and switch. Not only can the access point or switch initiate a link test to a CCX v4 or v5 client, but a CCX v4 or v5 client can initiate a link test to the access point or switch.

The switch shows the link-quality metrics for CCX link tests in both directions (out—the access point to the client; in—the client to the access point):

- Signal strength in the form of RSSI (minimum, maximum, and average)
- Signal quality in the form of SNR (minimum, maximum, and average)
- Total number of packets that are retried
- Maximum retry count for a single packet
- Number of lost packets
- Data rate of a successfully transmitted packet
The controller shows this metric regardless of direction:

- Link test request/reply round-trip time (minimum, maximum, and average)

The controller software supports CCX versions 1 through 5. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to limit the features for this client. If a client does not support CCXv4 or v5, the controller performs a ping link test on the client. If a client supports CCXv4 or v5, the controller performs a CCX link test on the client. If a client times out during a CCX link test, the controller switches to the ping link test automatically.

# How to Configure Link Latency

## Configuring Link Latency (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch# enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>ap link-latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Switch(config)# ap link-latency</td>
<td>Enables link latency for all access points that are currently associated with the switch.</td>
</tr>
</tbody>
</table>

**Note** To disable link latency for all the access points that are associated with the switch, use the `no ap link-latency` command.

**Note** These commands enable or disable link latency only for access points that are currently joined to the switch. You have to enable or disable link latency for the access points that join in the future.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> ap tcp-adjust-mss size (size)</td>
<td>Configures TCP MSS adjust size for all access points. The range is from 536 to 1363.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# ap tcp-adjust-mss size 537</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show ap name <em>Cisco_AP</em> config general</td>
<td>Displays the general configuration details of the access point. These configuration details contain the link latency results that correspond to the access point that you specify in the command.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# show ap name AP02 config general</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ap name <em>Cisco_AP</em> link-latency ([reset])</td>
<td>Clears the current, minimum, and maximum link latency statistics on the switch for a specific access point.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# ap name AP02 link-latency reset</code></td>
<td></td>
</tr>
</tbody>
</table>

- **Purpose:**

  To enable or disable link latency for specific access points that are associated with the switch, enter the following commands in Privileged EXEC mode:

  - `ap name *Cisco_AP* link-latency`—Enables link latency.
  - `ap name *Cisco_AP* no link-latency`—Disables link latency.

  **Note:** Configures TCP MSS adjust size for all access points. The range is from 536 to 1363.

  **Example:**

  `Switch(config)# ap tcp-adjust-mss size 537`

  **Display:**

  `Switch(config)# show ap name AP02 config general`

  **Clears:**

  `Switch(config)# ap name AP02 link-latency reset`

  - **Current Delay**—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the switch and back.
  - **Maximum Delay**—Since the time that link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the switch and back.
  - **Minimum Delay**—Since the time that link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the switch and back.
### Configuring Link Latency (GUI)

#### Procedure

**Step 1** Choose Configuration > Wireless > Access Points > All APs.

The **All APs** page appears with a list of access points.

**Step 2** Click the name of the access point.

The **AP > Edit** page appears.

**Step 3** Click the **Advanced** tab.

**Step 4** In the **Link Latency** area, select or unselect the **Enable Link Latency** check box.

**Note** You can select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the switch after every echo response is received. The default state is unselected.

**Step 5** Click **Apply**.

**Step 6** When a message box appears that indicates that AP Parameters are modified successfully, click **OK**.

**Step 7** When the **All APs** page is displayed, click the access point that you have modified earlier.

The **AP > Edit** page appears.

**Step 8** Click the **Advanced** tab.

In the **Link Latency** area, the following link latency and data latency results are displayed:

- **Current(mSec)**—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the switch and back.

- **Minimum(mSec)**—Since the time that link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the switch and back.

- **Maximum(mSec)**—Since the time that link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the switch and back.

**Step 9** Click **Reset Link Latency** to clear the current, minimum, and maximum link latency and data latency statistics on the switch for this access point.
How to Configure TCP MSS

Configuring TCP MSS (CLI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>ap tcp-adjust-mss size size_value</code></td>
<td>Enables the TCP MSS on the particular access point that you specify.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# ap tcp-adjust-mss size 537</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>reload</code></td>
<td>Reboots the switch in order for your change to take effect.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# reload</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>show ap tcp-adjust-mss</code></td>
<td>Displays the current TCP MSS setting for all the access points that are associated with the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# show ap tcp-adjust-mss</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To display the TCP MSS settings that correspond to a specific access point, enter the <code>show ap name Cisco_AP tcp-adjust-mss</code> command.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring TCP MSS (GUI)

**Procedure**

**Step 1** Choose Configuration > Wireless > Access Points > Global AP Configuration. The Global Configuration page is displayed.

**Step 2** In the TCP MSS area, select the Global TCP Adjust MSS check box and set the MSS for all access points that are associated with the switch. The valid range is from 536 to 1363 bytes.

**Step 3** Click Apply.

**Step 4** Click Save Configuration.

Performing a Link Test (CLI)

The procedure to perform this task using the switch GUI is not currently available.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> test wireless linktest mac_address</td>
<td>Runs a link test.</td>
</tr>
<tr>
<td>Example: Switch# test wireless linktest 00:0d:88:c5:8a:d1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> wireless linktest frame-size frame_size</td>
<td>Configures the link test frame size for each packet.</td>
</tr>
<tr>
<td>Example: Switch(config)# wireless linktest frame-size 41</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> wireless linktest number-of-frames number_of_frames</td>
<td>Configures the number of frames to send for the link test.</td>
</tr>
<tr>
<td>Example: Switch(config)# wireless linktest number-of-frames 50</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Examples for Configuring Link Latency

Running a Link Test: Example

This example shows how to run a link test:

Switch# test wireless linktest 6470.0227.ca55
Switch# show wireless linktest statistic

Link Test to 64700227CA55 with 500 frame-size.
Client MAC Address : 6470.0227.ca55
AP Mac Address : 44e4.d901.19c0
Link Test Packets Sent : 20
Link Test Packets Received : 20
Link Test Pkts Lost(Total/AP->Clnt/Clnt->AP) : 0/0/0
Link Test Pkts round trip time (min/max/avg) : 9ms/31ms/14ms
RSSI at AP (min/max/average) : -53dBm/-51dBm/-52dBm
RSSI at Client (min/max/average) : -48dBm/-40dBm/-44dBm

Displaying Link Latency Information: Example

This example shows how to display general configuration details of the access point. These configuration details contain the link latency results that correspond to the access point that you specify in the command.

Switch# show ap name AP01 config general

Cisco AP Name : AP01
Cisco AP Identifier : 55
Country Code : US - United States
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-A
AP Country Code : US - United States
AP Regulatory Domain : Unconfigured
Switch Port Number : Te1/0/1
MAC Address : 0000.2000.03f0
IP Address Configuration : Static IP assigned
IP Address : 9.9.9.16
IP Netmask : 255.255.0.0
Gateway IP Address : 9.9.9.2
Fallback IP Address Being Used : 9.9.9.16
Domain : Cisco
Name Server : 0.0.0.0
CAPWAP Path MTU : 1485
Telnet State : Enabled
SSH State : Disabled
Cisco AP Location : default-location
Cisco AP Group Name : default-group
Primary Cisco Controller Name : CAPWAP Controller
Primary Cisco Controller IP Address : 9.9.9.2
Secondary Cisco Controller Name : 

Step 5

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

Example:

Switch(config)# end
Secondary Cisco Controller IP Address : Not Configured
Tertiary Cisco Controller Name :
Tertiary Cisco Controller IP Address : Not Configured
Administrative State : Enabled
Operation State : Registered
AP Mode :
AP Submode :
Remote AP Debug : Disabled
Logging Trap Severity Level : informational
Software Version : 7.4.0.5
Boot Version : 7.4.0.5
Stats Reporting Period : 180
LED State : Enabled
PoE Pre-Standard Switch :
PoE Power Injector MAC Address :
Power Type/Mode : Power Injector/Normal Mode
Number of Slots : 2
AP Model :
AP Image : C3500-K9W8-M
IOS Version :
Reset Button :
AP Serial Number :
AP Certificate Type : Manufacture Installed
Management Frame Protection Validation :
AP User Mode :
AP User Name :
AP 802.1X User Mode :
AP 802.1X User Name :
Cisco AP System Logging Host : 255.255.255.255
AP Up Time : 16 days 3 hours 14 minutes 1 second
AP CAPWAP Up Time :
Join Date and Time : 01/02/2013 22:41:47
Join Taken Time : 16 days 2 hours 40 minutes 45 seconds
Join Priority :
Ethernet Port Duplex : Auto
Ethernet Port Speed :
AP Link Latency :
Current Delay :
Maximum Delay :
Minimum Delay :
Last Updated (based on AP up time) :
Rogue Detection :
AP TCP MSS Adjust :
AP TCP MSS Size :

Displaying TCP MSS Settings: Example

This example shows how to display the current TCP MSS setting for all the access points that are associated with the switch:

```
Switch# show ap tcp-adjust-mss

<table>
<thead>
<tr>
<th>AP Name</th>
<th>TCP State</th>
<th>MSS Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP01</td>
<td>Disabled</td>
<td>6146</td>
</tr>
<tr>
<td>AP02</td>
<td>Disabled</td>
<td>536</td>
</tr>
<tr>
<td>AP03</td>
<td>Disabled</td>
<td>6146</td>
</tr>
<tr>
<td>AP04</td>
<td>Disabled</td>
<td>6146</td>
</tr>
<tr>
<td>AP05</td>
<td>Disabled</td>
<td>6146</td>
</tr>
</tbody>
</table>
```

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
Displaying TCP MSS Settings: Example
Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Power over Ethernet

When an access point that has been converted to lightweight mode (such as an AP1262) access point is powered by a power injector that is connected to a Cisco pre-Intelligent Power Management (pre-IPM) switch, you must configure Power over Ethernet (PoE), which is also known as inline power.

How to Configure Power over Ethernet

Configuring Power over Ethernet (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>ap name <em>Cisco_AP</em> power injector installed</td>
<td>Enables the PoE power injector state. The access point remembers that a power injector is connected to this particular switch port. If you relocate the access point, you must reenter</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Switch# ap name AP02 power injector installed</td>
<td>this command after the presence of a new power injector is verified.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**  
Enter this command if your network contains any older Cisco 6-W switches that could be accidentally overloaded if connected directly to a 12-W access point. Make sure that the Cisco Discovery Protocol (CDP) is enabled before entering this command. Otherwise, this command will fail.

### Step 2

**ap name Cisco_AP power injector override**  
**Example:**  
Switch# ap name AP02 power injector override  

Removes the safety checks and allows the access point to be connected to any switch port. You can use this command if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The access point assumes that a power injector is always connected. If you relocate the access point, it continues to assume that a power injector is present.

### Step 3

**ap name Cisco_AP power injector switch-mac-address switch_mac_address**  
**Example:**  
Switch# ap name AP02 power injector switch-mac-address 10a.2d.5c.3d  

Sets the MAC address of the switch port that has a power injector.  
**Note**  
Enter this command if you know the MAC address of the connected switch port and do not want to automatically detect it using the installed option.

### Step 4

**show ap name Cisco_AP config general**  
**Example:**  
Switch# show ap name AP02 config general  

Displays common information that includes the PoE settings for a specific access point.  
**Note**  
The Power Type/Mode text box shows “degraded mode” if the access point is not operating at full power.

---

### Configuring Power over Ethernet (GUI)

**Procedure**

**Step 1**  
Choose Configuration > Wireless > Access Points > All APs.  
The All APs page appears with a list of access points that are associated with the switch.

**Step 2**  
Click the name of the access point.
The AP > Edit page appears.

**Step 3**  
Click the Advanced tab.

**Step 4**  
In the Power Over Ethernet Settings area, select the Pre-Standard 802.3af Switches check box.

Select this check box if the access point is being powered by a high-power 802.3af Cisco switch. This switch provides more than the traditional 6 Watts of power but does not support the intelligent power management (IPM) feature.

*Note*  
Unselect the Pre-standard 802.3af Switches check box if power is being provided by a power injector. This is the default value.

**Step 5**  
Select the Power Injector State check box.

Select this check box if the attached switch does not support IPM and a power injector is being used. If the attached switch supports IPM, you do not need to select this check box.

The Power Injector Selection drop-down list is displayed that contains parameters that enable you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed.

**Step 6**  
From the Power Injector Selection drop-down list, choose an option to specify the desired level of protection.

You can choose any one of the following three options:

- **Installed**—Examines and remembers the MAC address of the currently connected switch port and assumes that a power injector is connected. Choose this option if your network contains older Cisco 6-Watt switches and you want to avoid possible overloads by forcing a double-check of any relocated access points.

  If you want to configure the switch MAC address, enter the MAC address in the Injector Switch MAC Address text box. If you want the access point to find the switch MAC address, leave the Injector Switch MAC Address text box blank.

  *Note*  
  Each time that an access point is relocated, the MAC address of the new switch port fails to match the remembered MAC address, and the access point remains in low-power mode. You must then physically verify the existence of a power injector and reselect this option to cause the new MAC address to be remembered.

- **Override**—Allows the access point to operate in high-power mode without first verifying a matching MAC address. You can use this option if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The advantage of this option is that if you relocate the access point, it continues to operate in high-power mode without any further configuration. The disadvantage of this option is that if the access point is connected directly to a 6-W switch, an overload occurs.

**Step 7**  
Click Apply.

**Step 8**  
Click Save Configuration.

---

**What to do next**

Manually reset the access point in order for the change to take effect.
Configuration Examples for Configuring Power over Ethernet

Displaying Power over Ethernet Information: Example

This example shows how to display common information that includes the PoE settings for a specific access point:

Switch# show ap name AP01 config general

Cisco AP Identifier............... 1
Cisco AP Name..................... AP1

PoE Pre-Standard Switch........... Enabled
PoE Power Injector MAC Addr..... Disabled
Power Type/Mode................... PoE/Low Power (degraded mode)
PART VI

Mobility

• Information About Mobility, on page 279
• Mobility Network Elements, on page 285
• Mobility Control Protocols, on page 289
• Configuring Mobility, on page 297
CHAPTER 24

Information About Mobility

- Overview, on page 279
- Wired and Wireless Mobility, on page 280
- Features of Mobility, on page 280
- Sticky Anchoring for Low Latency Roaming, on page 282
- Bridge Domain ID and L2/L3 Roaming, on page 282
- Link Down Behavior, on page 282
- Platform Specific Scale Requirement for the Mobility Controller, on page 283

Overview

The switch delivers more services at access layer other than merely providing increased speeds and feeds. Wireless services is now integrated with the switch, which ensures that the access layer switch terminates the wireless users data plane, thereby delivering on the promise of Cisco's unified architecture. Unification implies that mobility services are provided to both wireless and wired stations.

The switch provides seamless roaming, which requires transparency of the network configuration and deployment options to the client.

From the end user's perspective, any mobility event must not change its IP address, its default router or DHCP server. This means that as stations roam, they must be able to

- Send an ARP to their default router, or
- Transmit a DHCP request to the server that had previously assigned their address.

From the infrastructure's perspective, as mobility events occur, the station's traffic must follow its current point of attachment, which can either be a mobility agent (MA) or mobility controller (MC). This must be true regardless of whether the station has moved to a network that is configured for a different subnet. The period from which the station is not receiving traffic following its mobility event must be as short as possible, even below 40 ms whenever possible, which includes any authentication procedures that are required.

From the infrastructure's perspective, the mobility management solution must have four main components, and all of these functions must be performed within the constraints of roaming:

- Initial Association—This function is used to identify the user's new point of attachment in the network.
- Context Transfer—This function is used to transfer state information associated with the station. This ensures that the station's static and real-time policies, including security and application ACLs, and services, remain the same across handoffs.
• **Handoff**—This function is used to signal that the station's point of attachment has changed, and control of the station should be relinquished by the previous access switch.

• **Data Plane**—This function is typically tied to the handoff process, and ensures that the station's traffic continues to be delivered and received from the station without any noticeable performance degradation.

---

**Note**

To form a mobility tunnel between Cisco Catalyst 4500E Supervisor Engine 8-E and the Cisco Unified Wireless Controller, you should match the wireless management interface's VLAN with the VLAN on the uplink interface.

---

**Caution**

If you have configured virtual routing and forwarding (VRF) on wireless management interface VLAN, the mobility feature may not work expected.

---

**Note**

You must enable PIM, IP ROUTING and IP MULTICAST Routing for wireless mobility multicast to work.

---

## Wired and Wireless Mobility

One of the key features of the Converged access solution (applicable to both the Cisco Catalyst 3850 Switch and Cisco WLC 5700 Series Controller) is its ability to provide a device with an IP address and maintain its session persistence, across mobility events from ethernet connections to wireless and vice-versa. This feature allows users to remain on an ethernet network when possible, and make use of the freedom of mobility associated with wireless when necessary.

This feature leverages support from both the client and the infrastructure and uses the two factor authentication-device and user. The device authentication credentials is cached in the mobility controller (MC). When a device transitions across link layers, the device credentials is validated, and if a match is found, the MC ensures that the same IP address is assigned to the new interface.

---

## Features of Mobility

• **Mobility Controller (MC)**—The controller provides mobility management services for inter-peer group roaming events. The MC provides a central point of contact for management and policy based control protocols, such as RADIUS. This eliminates the need for the infrastructure servers to maintain a user's location as it transitions throughout the network. The MC sends the configuration to all the mobility agents under its sub-domain of their mobility configuration, peer group membership and list of members. A sub-domain is synonymous to the MC that forms it. Each sub-domain consists of an MC and zero or more access switches that have AP's associated to them.

• **Mobility Agents (MA)**—A mobility agent is either an access switch that has a wireless module running on it or an MC with an internal MA running on it. A mobility agent is the wireless component that maintains client mobility state machine for a mobile client that is connected via an AP to the device that the MA is running on.
• Mobility Sub Domain— It is an autonomous portion of the mobility domain network. A mobility sub-domain comprises of a single mobility controller and its associated mobility agents (MAs).

  
  Note
  
  Even when more than one mobility controller is present, only one MC can be active at any given time.

A mobility sub-domain is the set of devices managed by the active mobility controller. A mobility sub-domain comprises of a set of mobility agents and associated access points.

• Mobility Group— A collection of mobility controllers (MCs) across which fast roaming is supported. The concept of mobility group is the same as a collection of buildings in a campus across which frequent roaming is expected.

• Mobility Domain— A collection of mobility sub-domains across which mobility is supported. The term mobility domain may be the same as a campus network.

• Mobility Oracle (MO)—The mobility oracle acts as the point of contact for mobility events that occur across mobility sub-domains. It also maintains a local database of each station in the entire mobility domain, their home and current sub-domain. A mobility domain includes one or more mobility oracle, though only one would be active at any given time.

• Mobility Tunnel Endpoint (MTE)— The mobility tunnel endpoint (MTE) provides data plane services for mobile devices through the use of tunneling. This minimizes the impact of roaming events on the network by keeping the user's point of presence on the network a constant.

• Point of Attachment— A station's point of attachment is where its data path is initially processed upon entry in the network. This could either be the access switch that is currently providing it service, or the wireless LAN controller.

• Point of Presence— A station's point of presence is the place in the network where the station is being advertised. For instance, if an access switch is advertising reachability to the station via a routing protocol, the interface on which the route is being advertised is considered the station's point of presence.

• Switch Peer Group (SPG)— A peer group is a statically created list of neighboring access switches between which fast mobility services is provided. A peer group limits the scope of interactions between switches during handoffs to only those that are geographically proximate.

• Station—A user's device that connects to and requests service from the network. The device may have a wired, wireless or both interfaces.

• Switch in the same SPG—A peer switch that is part of the peer group of the local switch.

• Switch outside the SPG—A peer access switch that is not part of the local switch's peer group.

• Foreign Mobility Controller— The mobility controller providing mobility management service for the station in a foreign mobility sub-domain. The foreign mobility controller acts as a liaison between access switches in the foreign sub-domain and the mobility controller in the home domain.

• Foreign Mobility Sub-Domain— The mobility sub-domain, controlled by a mobility controller, supporting a station which is anchored in another mobility sub-domain

• Foreign Switch— The access switch in the foreign mobility sub-domain currently providing service to the station.
- Anchor Mobility Controller— The mobility controller providing a single point of control and mobility management service for stations in their home mobility sub-domain.

- Anchor Mobility Sub-Domain— The mobility sub-domain, controlled by a mobility controller, for a station where its IP address was assigned.

- Anchor Switch— The switch in the home mobility sub-domain that last provided service to a station.

Sticky Anchoring for Low Latency Roaming

Sticky Anchoring ensures low roaming latency from the client's point of presence is maintained at the switch where the client initially joins the network. It is expensive to apply client policies at a switch for a roaming client. There can be considerable delay as it involves contacting the AAA server for downloadable ACLs which is not acceptable for restoring time sensitive client traffic.

To manage this delay, when the client roams between APs connected to different switches, irrespective of whether it is an intra sub-domain roam or inter sub-domain roam, the client traffic is always tunneled to the switch where the client first associates. The client is anchored at its first point of attachment for its lifetime in the network.

This behavior is enabled by default. You can also disable this behavior to allow the client anchoring only for inter-subnet roams. This configuration is per WLAN config and is available under the WLAN config mode. The customer can configure different SSIDs for time sensitive and non time sensitive applications.

Bridge Domain ID and L2/L3 Roaming

Bridge domain ID provides the mobility nodes with information to decide on specific roam type, either as L2 or L3 roam. It also allows the network administrators to reuse the VLAN IDs across network distribution. When the VLAN IDs do not have the associated subnet configurations, they may require additional parameter to use in conjunction with VLAN ID. The network administrator ensures that the given VLAN under the same bridge domain ID are associated with the unique subnet. The mobility nodes will first check for the bridge domain ID for the given node and the VLAN ID associated with the client to identify the roam type. The bridge domain ID and the VLAN ID must be same to treat a roam as L2 roam.

The bridge domain ID is configured for each SPG when creating a SPG and later on the MC. The bridge domain ID could be same for more than one SPG and all the MAs under the SPG will share the same bridge domain ID. This information is pushed to the MAs as part of the configuration download when MA comes up initially. If the bridge domain ID is modified when the system is up, it will be pushed to all the MAs in the modified SPG and will take immediate effect for the future roams.

Link Down Behavior

This section provides information about data synchronization between MA-MC and MC-MO when MC or MO faces downtime in absence of redundancy manager. When Keepalive is configured between MA-MC or MC-MO the clients database is synchronized between the MO and the MCs and the MC and its MAs respectively.
Platform Specific Scale Requirement for the Mobility Controller

The Mobility Controller (MC) role is supported on a number of different platforms like, the Cisco WLC 5700 Series, CUWN and Catalyst 3850 Switches. The scale requirements on these three platforms are summarized in the table below:

<table>
<thead>
<tr>
<th>Scalability</th>
<th>Catalyst 3850 as MC</th>
<th>Catalyst 3650 as MC</th>
<th>Cisco WLC 5700 as MC</th>
<th>CUWN 5508 as MC</th>
<th>WiSM2 as MC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max number of MC in Mobility Domain</td>
<td>8</td>
<td>8</td>
<td>72</td>
<td>72</td>
<td>72</td>
</tr>
<tr>
<td>Max number of MC in Mobility Group</td>
<td>8</td>
<td>8</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Max number of MAs in Sub-domain (per MC)</td>
<td>16</td>
<td>16</td>
<td>350</td>
<td>350</td>
<td>350</td>
</tr>
<tr>
<td>Max number of SPGs in Sub-domain (per MC)</td>
<td>8</td>
<td>8</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Max number of MAs in a SPG</td>
<td>16</td>
<td>16</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
</tbody>
</table>
Platform Specific Scale Requirement for the Mobility Controller
Mobility Network Elements

- Mobility Agent, on page 285
- Mobility Controller, on page 286
- Mobility Tunnel Endpoint, on page 287
- Mobility Oracle, on page 287
- Guest Controller, on page 287

Mobility Agent

The Mobility Agent (MA) interacts with the Mobility Controller (MC), which can be a Catalyst 3850 Switch, or a Cisco WLC 5760, or a Cisco Unified Wireless Networking Solution controller. The MA is responsible for:

- Handling the mobility events on the switch
- Configuring the datapath elements on the switch for mobility, and
- Communicating with the mobility controller

As MA, the switch performs the datapath functions by terminating the CAPWAP tunnels that encapsulate 802.11 traffic sourced by wireless stations.

This allows the switch to apply features to wired and wireless traffic in a uniform fashion. As far as switch is concerned, 802.11 is just another access medium.

The MA performs the following functions:

- Support the mobility protocol – The MA is responsible for responding in a timely manner, ensuring the switch is capable of achieving its roaming budget.
- Point of presence – If the wireless subnets are not available at the MC, the MA assumes the point of presence if the wireless client VLAN is not available at the new point of attachment and tunnel the client traffic accordingly.
- ARP Server – When the network is configured in a layer 2 mode, the MA is responsible for advertising reachability for the stations connected to it. If tunneling is employed, the ARP request is transmitted on behalf of the station through the tunnel, which the point of presence (anchor switch) would bridge onto its uplink interface.
- Proxy IGMP – The MA on the switch is responsible for subscribing to multicast groups on behalf of a station after a roaming event has occurred. This information is passed as part of the context to the new switch. This ensures the multicast flows follow the user as it roams.
• Routing – When the switch is connected to a layer 3 access network, the MA is responsible for injecting routes for the stations that are associated with it for which tunneling is not provided.
• 802.1X Authenticator – The authenticator function is included in the MA, and handles both wired and wireless stations.
• Secure PMK Sharing – When a station successfully authenticates to the network, the MA forwards the PMK to the MC. The MC is responsible for flooding the PMK to all the MAs under its sub-domain and to the peer MCs in the mobility group.

The MA also performs the following datapath functions:
• Mobility tunnel – If tunneling is used, the MA encapsulates and decapsulates packets from the mobility tunnel to the MC, and to other MA in the peer group, if the access switches are serving as points of presence. The MA supports the tunneling of client data traffic between the point of attachment and the point of attachment. The packet format used for other switches is CAPWAP with an 802.3 payload. The MA also supports reassembly and fragmentation for mobility tunnels.
• Encryption – The mobility control traffic between the mobility nodes is DTLS encrypted. The MA also encrypts the CAPWAP control and data (optional) at the point of attachment.
• CAPWAP – The switch supports the CAPWAP control and data planes. The switch forwarding logic is responsible for terminating the CAPWAP tunnels with 802.11 as well as 802.3 payloads. Since support for large frames (greater than 1500 bytes) is not universally available, the switch supports CAPWAP fragmentation and reassembly.

Note
Mobility tunnel path via an L3 interface on the 4500 or the L3 interface on the uplink port is not supported. It is not possible to have an L3 wireless management interface. Even if the tunnel comes up, packet forwarding is not possible as it is not supported. 4510 drops DHCP packets from wireless clients if SSID is anchored to a different Cisco WLC.

Mobility Controller

The main function of mobility controller is to coordinate the client roaming beyond a switch peer group. The other features of the mobility controller are:
• Station Database—The Mobility Controller maintains a database of all the clients that are connected within the local mobility sub-domain.
• Mobility Protocol—The MC supports the mobility protocol which ensures the target roaming point responds in a timely manner and achieves the 150ms roaming budget
• Interface to Mobility Oracle—The Mobility Controller acts as a gateway between the switch and the Mobility Oracle. When the Mobility Controller does not find a match in its local database, it suggests a match for a wireless client entry (in its database) and forwards the request to the Mobility Oracle, which manages the Mobility Domain.

Note
Mobility Oracle function can be enabled on an MC only if it is supported by the platform.
• ARP Server—When tunneling is employed for a station, its point of presence on the network is the Mobility Tunnel Endpoint (MTE). The Mobility Controller responds to any ARP requests received for the stations it is responsible for.
• Configures MTE—The Mobility Controller is the control point for the switch for all mobility management related requests. When a change in a station’s point of attachment occurs, the Mobility Controller is responsible for configuring the forwarding policy on the MTE.
• NTP Server—The Mobility Controller acts as an NTP server to the switch and supports all the nodes to have their clocks synchronized with it.

Note
The Cisco 5700 series WLC and other controller platforms that have the Mobility Controller function enabled by default should not be added to a switch peer group (SPG).

Mobility Tunnel Endpoint

MTE is the Data plane component of MC and MA and provides data plane services for mobile devices through the use of tunneling.

The functions of the MTE include:
• Tunnel Termination: The MTE terminates the data part of mobility tunnels from the Switch. Traffic to and from the roamed client is sent to the foreign switch via the mobility tunnel.
• Inter-MTETunnel Termination – The MTE-MTE tunnel is used to tunnel traffic between mobility sub-domains. These tunnels have the same format as the Switch-MTE tunnels.
• Mobility Controller Configuration Interface: This is the interface the MC uses to configure the MTE’s forwarding tables to reflect mobility events.

Mobility Oracle

The Mobility Oracle coordinates the client roams beyond the subdomain on a need basis and consists of the following features:
• Station Database—The Mobility Oracle maintains a database of all stations that are serviced within the mobility domain. This database is populated during the Mobility Oracle's interactions with all the Mobility Controllers, in all of the mobility sub-domains it supports.
• Interface to Mobility Controller—When the Mobility Oracle receives a request from a Mobility Controller, it performs a station lookup, and forwards, whenever needed, the request to the proper Mobility Controller.
• NTP Server—The Mobility Oracle acts as an NTP server to the Mobility Controllers and synchronizes all the switch clocks within the mobility domain.

Guest Controller

The guest access feature provides guest access to wireless clients. The guest tunnels use the same format as the mobility tunnels. Using the guest access feature, there is no need to configure guest VLANs on the access switch. Traffic from the wired and wireless clients terminates on Guest Controller. Since the guest VLAN is
not present on the access switch, the traffic is tunneled to the MTE over the existing mobility tunnel, and then via a guest tunnel to the Guest Controller.

The advantage of this approach is that all guest traffic passes through the MTE before it is tunneled to the Guest Controller. The Guest Controller only needs to support tunnels between itself and all the MTEs.

The disadvantage is that the traffic from the guest client is tunneled twice - once to the MTE and then again to the Guest Controller.

Clients cannot roam to Guest Controllers because roaming is not supported on Guest Controllers. This restriction is applicable only for the IOS-XE guest anchor, and not for AireOS.
Mobility Control Protocols

- About Mobility Control Protocols, on page 289
- Initial Association and Roaming, on page 289
- Initial Association, on page 290
- Intra Switch Handoff, on page 291
- Intra Switch Peer Group Handoff, on page 291
- Inter Switch Peer Group Handoff, on page 292
- Inter Sub Domain Handoff, on page 293
- Inter Mobility Group Handoff, on page 295
- Three Way Sub Domain Handoff, on page 295

About Mobility Control Protocols

The mobility control protocol is used regardless of whether tunneled or routed. The mobility control protocol is used for mobility events between the MO, MC and MA.

The mobility architecture uses both,
- Distributed approach, using the direct communication with the switches in their respective SPG, as well as
- Centralized approach, using the MC and MO.

The goal is to reduce the overhead on the centralized MC, while limiting the interactions between switches to help scale the overall system.

Initial Association and Roaming

The following scenarios are applicable to the mobility management protocol:
- Initial Association
- Intra Switch Roam
- Intra Switch Peer Group Roam
- Inter Switch Peer Group Roam
- Inter Sub-Domain Roam
- Inter Group Roam
Initial Association

The illustration below explains the initial association process followed by the switch:

Figure 21: Initial Association

1. When a station initially associates with a mobility agent, the MA performs a lookup to determine whether keying information for key caching is locally available in the MA. If no keying information is available, which is the case when the station first appears in the network, the switch prompts the device to authenticate itself to generate the Pairwise Master Key (PMK). The PMK is generated on the client and the RADIUS server side, and the RADIUS sever forwards the PMK to the authenticator, the MA.
2. The MA sends the PMK to the MC.
3. After receiving the PMK from the MA, the MC transmits the PMK to all the MAs in its sub-domain, and to all the other MCs in its mobility group.
4. The mobility group is a single key domain. This ensures that 802.11r compliant stations recognize the key domain, and attempts to utilize the fast transition procedures defined in 802.11r.

**Note**
The 802.11r protocol defines a key domain, which is a collection of access points that share keying information.

5. (Refer to step 2B in the illustration). Since the station is new to the mobility sub-domain, as indicated by the fact that the PMK is not in the MA local key cache, the MA transmits a mobile announce message to the MC.

6. The MC checks if the client exists in its database. As the client cannot be found, the MC in turn forwards it to the MO, if available.

7. (Refer to step 5 in the illustration). As the station is new to the network, the MO returns a negative response (NACK), which is forwarded by the MC to the switch. If the Mobility Oracle is not available then the MC is responsible for not responding to the Mobile Announce.

**Note**
In new mobility if there are many peers, the IOS controller will not react on a NACK message from the AirOS peer and sends two more probes. NACK is ignored if the client is not present it just drops it, is such a scenario AirEOS sends the NACK. So NACK from mobility controller is not processed.

8. The MA on the switch informs the MC about the station's new point of attachment via the Handoff Complete message.

9. The MA then informs the other MAs in its switch peer group (SPG) about the station's new point of attachment via the Handoff Notification message. It is necessary to transmit this notification to the MAs in its SPG to allow local handoff without interacting with the MC. The Handoff Notification message sent to MAs in SPG need not carry all the information in Handoff Complete message sent to the MC.

10. (Refer to step 7B in the illustration). The MC updates its database and forwards the Handoff Complete message to the Mobility Oracle. This ensures that the Mobility Oracle's database is updated to record the station's current home mobility sub-domain.

To eliminate race conditions that could occur with devices moving quickly across switch, regardless of whether they are within a mobility sub-domain or not, the messages between MA and MC/MO are time synchronized. This would allow the MC and MO to properly process requests, if they are received out of order.

The Handoff Notification sent to MAs in the SPG are not acknowledged.

**Intra Switch Handoff**

Mobility events within an MA are completely transparent to the SPG and the MC. When a station moves across APs on the same MA and attempts to perform a fast handoff, the PMK is present on the MA. The MA will complete the fast handoff without invoking any additional signal.

**Intra Switch Peer Group Handoff**

The switch peer group (SPG) is a group of MAs between which users may roam, and expect fast roaming services. Allowing the MA to handoff directly within a SPG reduces the overhead on the MC as it requires fewer messages to be exchanged.
After the initial association is complete the station moves to another MA belonging to its SPG. In an intra switch peer group roam, the initial association, the stations PMK was forwarded to all MAs in the mobility sub-domain.

*Figure 22: Intra Switch Peer Group Handoff*

The following process explains the intra switch peer group handoff:

1. In the initial association example, the Handoff Notification message is sent to all MAs in its SPG to know the station's current point of attachment.
2. The new MA sends a unicast Mobile Announce message to the previous MA to which the client is associated.
3. After the handoff completion, the new MA transmits a Handoff Complete message to the MC.
4. The new switch sends a Handoff Notification to all MA in its own SPG to inform them about the clients new point of presence.

**Inter Switch Peer Group Handoff**

The Intra SPG roams do not cover all possible scenarios and there can be cases where it is possible for mobility events to occur between two MAs that are not in the same SPG.

When a MA does not have any information about a station's current point of attachment, because of the Handoff Notification message getting lost in the network, or because of the the station roaming to an MA that is not in the new SPG, the MA consults the MC. The MC provides information about the clients point of presence within the mobility sub-domain. This eliminates the need to consult all other MCs within the mobility sub-domain.
The image above illustrates an example of a mobility event that occurs across MAs that are not in the same SPG, but within the same mobility sub-domain.

**Note**

1. The new MA will have the PMK for the station, which was forwarded to each MA in the mobility sub-domain upon client initial authentication.
2. Since the MA had not been previously notified of the station's presence on a neighboring MA inside a different SPG transmits the mobile announce to the sub-domain's MC.
3. (Refer to step 2 in the illustration) On receiving the mobile announce message, the MC performs a lookup in its database, and forwards the request to the MA that was previously providing service to the station. This information is known to the MC through a previously received Handoff Complete message sent in a reliable fashion from the old MA.
4. (Refer to step 3 in the illustration) The old MA, shown in green above, transmits a Handoff message directly to the new MA.
5. The old MA needs to notify other MAs within its SPG of the fact that the station has left the group using a Station Left message. This ensures that if the station were to come back to one of the MA, they would be aware of the fact that the station is no longer being serviced by the old MA.
6. Once the handoff is complete, the new MA transmits the Handoff Complete message in a reliable fashion to the MC.
7. The new MA then transmits the Handoff Notification to the other MAs within its SPG.

**Inter Sub Domain Handoff**

A sub-domain is an ensemble formed by a mobility controller and the mobility agents it directly manages. An inter sub-domain mobility event implies communication between two mobility controllers. These 2 mobility controllers can be configured with the same mobility group value and recognize each other. They will appear in each other's mobility list, or they can be configured with different mobility group values, and still recognize each other.
When the roaming event occurs across sub-domains between MCs in the same mobility group, the 802.11r key domain advertised by the new APs are the same. Additionally, the client PMK is also transmitted to all MCs upon the client's initial authentication. The new MC does not need to force the client to reauthenticate, and the new MC also knows which previous MC was managing the wireless client mobility.

**Figure 24: Inter Sub Domain Handoff**

The following steps are involved in the inter sub domain handoff, when mobility controllers belong to the same mobility group:

1. When a clients PMK was sent by the initial MA to all the MCs in the mobility group, the new MA already had already received the client PMK from its MC, and re-authentication is not required.
2. The new MA was not notified previously of the station's presence on a neighboring MA inside a different SPG it transmits the mobile announce to the sub-domain's MC.
3. On receiving the mobile announce message, the MC forwards the mobile announce to the MO, which performs a lookup in its database, and forwards the request to the MC that was previously providing service to the station.
4. The previous MC, in turn, forwards the request to the MA that was previously providing service to the station.
5. The old MA, shown in yellow color above, transmits a Handoff message directly to the new MA.
6. The old MA must notify the other MAs within its SPG of the fact that the station has left the SPG using a Station Left message. This ensures that if the station comes back to one of the MA, the MA is aware of the fact that the station is no longer serviced by the old MA.
7. Once the handoff is complete, the new MA transmits the Handoff Complete message in a reliable fashion to the new Mobility Controller.
8. The new MA then transmits the Handoff Notification to all other MAs.
9. The new MC then transmits the Handoff Complete to the old MC.
Inter Mobility Group Handoff

A mobility group is formed by MCs sharing the same mobility group name, and knowing each other. Since the roaming event occurs across mobility groups, the 802.11r key domain advertised by the new APs differ. This forces the client to re-authenticate. They are propagated only within a mobility group, and roaming across mobility groups requires the stations to re-authenticate when they cross mobility group boundaries. When the authentication is complete, the PMK that is generated is pushed to the MAs and MCs within the same mobility group. The stations cache the PMK from the previous sub-domain because each PMK is associated to a given sub-domain (802.11y key domain). This ensures that you do not have to re-authenticate when the PMK roams back to the previous sub-domain within the pmk cache timeout interval. The remaining procedure follows the inter-sub-domain handoff steps, except that these steps relate to inter mobility group roaming.

Three Way Sub Domain Handoff

The controller also supports mobility events that occur across foreign domains, known as a three-way sub-domain mobility event.

The illustration below explains the interaction between the Mobility Controllers in both foreign sub-domains through the Mobility Oracle.

The message exchange shown in the illustration is identical to that described in Inter Sub Domain Handoff except for the exception that the Handoff Complete notification is transmitted to the Mobility Controllers in the old foreign sub-domain as well as the home sub-domain.
Three Way Sub Domain Handoff
Configuring Mobility

- Configuring Mobility Controller, on page 297
- Configuring the Mobility Oracle, on page 310

Configuring Mobility Controller

Configuring Converged Access Controllers

Creating Peer Groups, Peer Group Member, and Bridge Domain ID (CLI)

Before you begin

- On the mobility agent, you can only configure the IP address of the mobility controller.
- On the mobility controller, you can define the peer group and the IP address of each peer group member.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| wireless mobility controller | Enables the mobility controller functionality on the device. This command is applicable only to the switch. The controller is by default a mobility controller. |
| Example: Switch(config)# wireless mobility controller |
| **Step 2**
| wireless mobility controller peer-group SPG1 | Creates a peer group named SPG1. |
| Example: Switch(config)# wireless mobility controller peer-group SPG1 |
### Creating Peer Groups, Peer Group Member, and Bridge Domain ID (CLI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 3 | `wireless mobility controller peer-group SPG1 member ip member-ip-addr public-ip public-ip-addr` | Adds a mobility agent to the peer group.  
**Example:**  
Switch(config)# wireless mobility controller peer-group  
SPG1 member ip 10.10.20.2 public-ip 10.10.20.2 |
|  | **Note**  
The **10.10.20.2** is the mobility agent's direct IP address. When NAT is used, use the optional public IP address to enter the mobility agent's NATed address. When NAT is not used, the public IP address is not used and the device displays the mobility agent's direct IP address. |
| Step 4 | `wireless mobility controller peer-group SPG1 member ip member-ip-addr public-ip public-ip-addr` | Adds another member to the peer group SPG1.  
**Example:**  
Switch(config)# wireless mobility controller peer-group  
SPG1 member ip 10.10.20.6 public-ip 10.10.20.6 |
| Step 5 | `wireless mobility controller peer-group SPG2` | Creates another peer group SPG2.  
**Example:**  
Switch(config)# wireless mobility controller peer-group SPG2 |
| Step 6 | `wireless mobility controller peer-group SPG2 member ip member-ip-addr public-ip public-ip-addr` | Adds a member to peer group SPG2.  
**Example:**  
Switch(config)# wireless mobility controller peer-group  
SPG2 member ip 10.10.10.20 public-ip 10.10.10.20 |
| Step 7 | `wireless mobility controller peer-group SPG1 bridge-domain-id id` | (Optional) Adds a bridge domain to SPG1 used for defining the subnet-VLAN mapping with other SPGs.  
**Example:**  
Switch(config)# wireless mobility controller peer-group  
SPG1 bridge-domain-id 54 |

### Example

This example shows how to create peer group and add members to it:

```
Switch(config)# wireless mobility controller  
Switch(config)# wireless mobility controller peer-group SPG1  
Switch(config)# wireless mobility controller peer-group SPG1  
Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip
```
Creating Peer Groups, Peer Group Member, and Bridge Domain ID (GUI)

Before you begin

- Ensure that the device is in mobility controller state.
- On the mobility agent, you can only configure the IP address of the mobility controller.
- On the mobility controller, you can define the peer group and the IP address of each peer group member.

Procedure

Step 1  Choose Controller > Mobility Management > Switch Peer Group.
        The Mobility Switch Peer Groups page is displayed.

Step 2  Click New.

Step 3  Enter the following details:
        a)  Switch Peer Group Name
        b)  Bridge Domain ID
        c)  Multicast IP Address

Step 4  Click Apply.

Step 5  Click Save Configuration.

Configuring Optional Parameters for Roaming Behavior

Use this configuration to disable the sticky anchor. This command can also be used, if required, between all MA's and MC's where roaming is expected for the target SSID.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 wlan open21</td>
<td>Configures a WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# wlan open20</td>
<td></td>
</tr>
<tr>
<td>Step 2 no mobility anchor sticky</td>
<td>Disables the default sticky mobility anchor.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Switch(config-wlan)# no mobility anchor sticky</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

Switch(config)# wlan open20
Switch(config-wlan)# no mobility anchor sticky

**Configuring Local Mobility Group (CLI)**

Configuration for wireless mobility groups and mobility group members where the mobility group is a group of MCs.

**Before you begin**

MCs can belong only to one mobility group, and can know MCs in several mobility groups.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>wireless mobility group name <strong>group-name</strong></td>
<td>Creates a mobility group named <strong>Mygroup</strong>.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# wireless mobility group name Mygroup</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>wireless mobility group member ip <strong>member-ip-addr</strong> public-ip <strong>public-ip-addr</strong></td>
<td>Adds a mobility controller to the <strong>Mygroup</strong> mobility group.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28</td>
<td><strong>Note</strong> When NAT is used, use the optional public IP address to enter the NATed IP address of the mobility controller.</td>
</tr>
<tr>
<td>3</td>
<td>wireless mobility group keepalive interval <strong>time-in-seconds</strong></td>
<td>Configures the interval between two keepalives sent to a mobility member.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# wireless mobility group keepalive interval 5</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>wireless mobility group keepalive count <strong>count</strong></td>
<td>Configures the keep alive retries before a member status is termed DOWN.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# wireless mobility group keepalive count 3</td>
<td></td>
</tr>
</tbody>
</table>
Example

Switch(config)# wireless mobility group name Mygroup
Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28
Switch(config)# wireless mobility group keepalive interval 5
Switch(config)# wireless mobility group keepalive count 3

Configuring Local Mobility Group (GUI)

Before you begin
Mobility controllers can belong to only one mobility group and can know mobility controllers in several mobility groups.

Procedure

Step 1 Choose Controller > Mobility Management > Mobility Global Config.
The Mobility Controller Configuration page is displayed.

Step 2 Enter the following details:
   a) Mobility Group Name
   b) Mobility Keepalive Interval
   c) Mobility Keepalive Count
   d) Multicast IP Address if you want to enable multicast mode to send mobile announce messages to the mobility members.

   Note If you do not enable multicast IP address, the device uses unicast mode to send mobile announce messages.

Step 3 Click Apply.
Step 4 Click Save Configuration.

Adding a Peer Mobility Group (CLI)

Before you begin
MCs belong to only one group, and can know MCs in several groups.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> wireless mobility group member ip member-ip-addr public-ip public-ip-addr group group-name</td>
<td>Adds the member as a peer MC in a different group than the Mygroup.</td>
</tr>
</tbody>
</table>
## Adding a Peer Mobility Group (GUI)

### Before you begin

Mobility controllers belong to only one group, and can know several mobility groups.

### Procedure

1. **Step 1**  
   Choose **Controller > Mobility Management > Mobility Peer**.  
   The **Mobility Peer** page is displayed.

2. **Step 2**  
   Click **New**.

3. **Step 3**  
   Enter the following details:  
   a) **Mobility Member IP**  
   b) **Mobility Member Public IP**  
   c) **Mobility Member Group Name**  
   d) **Multicast IP Address**

4. **Step 4**  
   Click **Apply**.

5. **Step 5**  
   Click **Save Configuration**.

## Configuring Optional Parameters for Roaming Behavior

Use this configuration to disable the sticky anchor. This command can also be used, if required, between all MA's and MC's where roaming is expected for the target SSID.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
  wlan open21  
  Example:  
  Switch(config)# wlan open20 | Configures a WLAN. |
| **Step 2**  
  no mobility anchor sticky  
  Example:  
  Switch(config-wlan)# no mobility anchor sticky | Disables the default sticky mobility anchor. |
Example

Switch(config)# wlan open20
Switch(config-wlan)# no mobility anchor sticky

Pointing the Mobility Controller to a Mobility Oracle (CLI)

Before you begin
You can configure a mobility oracle on a known mobility controller.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> wireless mobility group member ip member-ip-addr group group-name</td>
<td>Creates and adds a MC to a mobility group.</td>
</tr>
<tr>
<td>Example: Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless mobility oracle ip oracle-ip-addr</td>
<td>Configures the mobility controller as mobility oracle.</td>
</tr>
<tr>
<td>Example: Switch(config)# wireless mobility oracle ip 10.10.10.10</td>
<td></td>
</tr>
</tbody>
</table>

Example

Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3
Switch(config)# wireless mobility oracle ip 10.10.10.10

Pointing the Mobility Controller to a Mobility Oracle (GUI)

Before you begin
You can configure a mobility oracle on a known mobility controller.

Procedure

**Step 1** Choose Controller > Mobility Management > Mobility Global Config.
The Mobility Controller Configuration page is displayed.

**Step 2** Enter the Mobility Oracle IP Address.

**Note** To make the mobility controller itself a mobility oracle, select the Mobility Oracle Enabled check box.
Configuring Guest Controller

A guest controller is used when the client traffic is tunneled to a guest anchor controller in the demilitarized zone (DMZ). The guest client goes through a web authentication process. The web authentication process is optional, and the guest is allowed to pass traffic without authentication too.

Enable the WLAN on the mobility agent on which the guest client connects with the mobility anchor address of the guest controller.

On the guest controller WLAN, which can be Cisco 5500 Series WLC, Cisco WiSM2, or Cisco 5700 Series WLC, configure the IP address of the mobility anchor as its own IP address. This allows the traffic to be tunneled to the guest controller from the mobility agent.

With Cisco 5700 Series WLC as the guest anchor controller and Cisco 5500 Series WLC or Cisco WiSM2 as export foreign controller, the guest user role per user is not supported on the Cisco 5700 Series WLC.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> wlan wlan-id&lt;br&gt;<strong>Example:</strong> Switch(config)# wlan Mywlan1</td>
<td>Creates a WLAN for the client.</td>
</tr>
<tr>
<td><strong>Step 2</strong> mobility anchor guest-anchor-ip-addr&lt;br&gt;<strong>Example:</strong> Switch(config-wlan)# mobility anchor 10.10.10.2</td>
<td>Enables the guest anchors (GA) IP address on the MA.&lt;br&gt;Note To enable guest anchor on the mobility controller, you need not enter the IP address. Enter the mobility anchor command in the WLAN configuration mode to enable GA on the mobility controller.</td>
</tr>
<tr>
<td><strong>Step 3</strong> client vlan vlan-name&lt;br&gt;<strong>Example:</strong> Switch(config-wlan)# client vlan gc_ga_vlan1</td>
<td>Assigns a VLAN to the client's WLAN.</td>
</tr>
<tr>
<td><strong>Step 4</strong> security open&lt;br&gt;<strong>Example:</strong> Switch(config-wlan)# security open</td>
<td>Assigns a security type to the WLAN.</td>
</tr>
</tbody>
</table>
### Configuring Guest Anchor

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>wlan Mywlan1</td>
<td>Creates a wlan for the client.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# wlan Mywlan1</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>mobility anchor &lt;guest-anchors-own-ip-address&gt;</td>
<td>Enables the guest anchors IP address on the guest anchor (GA). The GA assigns its own address on itself.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-wlan)# mobility anchor 10.10.10.2</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>client vlan&lt;vlan-name&gt;</td>
<td>Assigns a vlan to the clients wlan.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-wlan)# client vlan gc_ga_vlan1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>security open</td>
<td>Assigns a security type to the wlan.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-wlan)# security open</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

Switch(config)# wlan Mywlan1  
Switch(config-wlan)# mobility anchor 10.10.10.2  
Switch(config-wlan)# client vlan gc_ga_vlan1  
Switch(config-wlan)# security open
Configuring Converged Access Controller on 5508 or WiSM 2

Enabling the New Mobility

**Before you begin**

You will require Cisco Unified Wireless Network 7.3 MR1, 8.0 or later to configure the new mobility architecture.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config mobility new-architecture enable</td>
<td>Enables and installs the new mobility architecture on the CUWN based controller.</td>
</tr>
</tbody>
</table>

**Example**

(Cisco Controller) > config mobility new-architecture enable
Enabling new-architecture would change mobility architecture from flat to hierarchical !!!
Configuration changes will be saved and System will be rebooted. !!!
Are you sure you want to continue? (y/n) y

Configuring Mobility Controller

This configuration shows how to change the MCs public address, or mobility group name.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Example:</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

Creating Peer Groups, Peer Group Member, and Bridge Domain ID (CLI)

**Before you begin**

- On the mobility agent, you can only configure the IP address of the mobility controller.
- On the mobility controller, you can define the peer group and the IP address of each peer group member.
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>wireless mobility controller</td>
<td>Enables the mobility controller functionality on the device. This command is applicable only to the switch. The controller is by default a mobility controller.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# wireless mobility controller</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless mobility controller peer-group <em>SPG1</em></td>
<td>Creates a peer group named SPG1.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# wireless mobility controller peer-group SPG1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>wireless mobility controller peer-group <em>SPG1</em> member ip member-ip-addr public-ip public-ip-addr</td>
<td>Adds a mobility agent to the peer group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip 10.10.20.2</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The <em>10.10.20.2</em> is the mobility agent's direct IP address. When NAT is used, use the optional public IP address to enter the mobility agent's NATed address. When NAT is not used, the public IP address is not used and the device displays the mobility agent's direct IP address.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>wireless mobility controller peer-group <em>SPG1</em> member ip member-ip-addr public-ip public-ip-addr</td>
<td>Adds another member to the peer group SPG1.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip 10.10.20.6</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>wireless mobility controller peer-group <em>SPG2</em></td>
<td>Creates another peer group SPG2.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# wireless mobility controller peer-group SPG2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>wireless mobility controller peer-group <em>SPG2</em> member ip member-ip-addr public-ip public-ip-addr</td>
<td>Adds a member to peer group SPG2.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip 10.10.10.20</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>wireless mobility controller peer-group <em>SPG1</em> bridge-domain-id <em>id</em></td>
<td>(Optional) Adds a bridge domain to SPG1 used for defining the subnet-VLAN mapping with other SPGs.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Local Mobility Group (CLI)

Configuration for wireless mobility groups and mobility group members where the mobility group is a group of MCs.

**Before you begin**

MCs can belong only to one mobility group, and can know MCs in several mobility groups.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Creates a mobility group named <strong>Mygroup</strong>.</td>
</tr>
<tr>
<td>wireless mobility group name <em>group-name</em></td>
<td>Example:</td>
</tr>
<tr>
<td>Switch(config)# wireless mobility group name Mygroup</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Adds a mobility controller to the <strong>Mygroup</strong> mobility group.</td>
</tr>
<tr>
<td>wireless mobility group member ip member-ip-addr public-ip public-ip-addr</td>
<td>Example:</td>
</tr>
<tr>
<td>Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the interval between two keepalives sent to a mobility member.</td>
</tr>
<tr>
<td>wireless mobility group keepalive interval time-in-seconds</td>
<td>Example:</td>
</tr>
<tr>
<td>Switch(config)# wireless mobility group keepalive interval 5</td>
<td></td>
</tr>
</tbody>
</table>
Adding a Peer Mobility Group (CLI)

Before you begin

MCs belong to only one group, and can know MCs in several groups.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>wireless mobility group member ip member-ip-addr public-ip public-ip-addr group group-name</code></td>
<td>Adds the member as a peer MC in a different group than the <strong>Mygroup</strong>.</td>
</tr>
</tbody>
</table>

Example:

Switch(config)# wireless mobility group name Mygroup
Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28
Switch(config)# wireless mobility group keepalive interval 5
Switch(config)# wireless mobility group keepalive count 3

Configuring Optional Parameters for Roaming Behavior

Use this configuration to disable the sticky anchor. This command can also be used, if required, between all MA's and MC's where roaming is expected for the target SSID.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>wlan open21</code></td>
<td>Configures a WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# wlan open20</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>no mobility anchor sticky</code></td>
<td>Disables the default sticky mobility anchor.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>
Pointing the Mobility Controller to a Mobility Oracle (CLI)

Before you begin

You can configure a mobility oracle on a known mobility controller.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Switch(config-wlan)# wireless mobility group member ip member-ip-addr group group-name</td>
<td>Creates and adds a MC to a mobility group.</td>
</tr>
<tr>
<td>Example: Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3</td>
<td></td>
</tr>
<tr>
<td>Step 2: Switch(config)# wireless mobility oracle ip oracle-ip-addr</td>
<td>Configures the mobility controller as mobility oracle.</td>
</tr>
<tr>
<td>Example: Switch(config)# wireless mobility oracle ip 10.10.10.10</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the Mobility Oracle

Configuring Mobility Oracle on Converged Access Controller

This configuration shows how to configure mobility oracle on a converged access controller only. The mobility controller can either have mobility oracle enabled or point to an external mobility oracle, but not both.
Enabling the Mobility Oracle on the Controller

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wireless mobility oracle</td>
<td>Enables the mobility oracle on the mobility</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>controller.</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# wireless mobility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>oracle</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

This example shows how to enable the mobility oracle on the mobility controller:

```
Switch(config)# wireless mobility oracle
```

Configuring Mobility Oracle on CUWN

**Enabling Mobility Oracle on CUWN**

This configuration shows how to enable the mobility oracle on the 5508 or WiSM2 controllers.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>config mobility oracle enable</td>
<td>Enables the oracle on CUWN 5500.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;cisco-controller&gt; config</td>
<td></td>
</tr>
<tr>
<td></td>
<td>wireless mobility oracle</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>config mobility oracle ip 10.10.10.5</td>
<td>Configures the MC with MO's IP address.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;cisco-controller&gt; config</td>
<td></td>
</tr>
<tr>
<td></td>
<td>wireless mobility oracle</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip 10.10.10.5</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

This example shows how to enable oracle on CUWN and make the CUWN also act as MO:

```
<cisco-controller> config wireless mobility oracle
<cisco-controller> config wireless mobility oracle ip 10.10.10.5
```
Enabling Mobility Oracle on CUWN
PART VII

Multicast

• Configuring IGMP, on page 315
• Configuring Wireless Multicast, on page 369
• Configuring the Service Discovery Gateway, on page 383
CHAPTER 28

Configuring IGMP

- Finding Feature Information, on page 315
- Prerequisites for IGMP and IGMP Snooping, on page 315
- Restrictions for IGMP and IGMP Snooping, on page 316
- Information About IGMP, on page 317
- How to Configure IGMP, on page 328
- Monitoring IGMP, on page 360
- Configuration Examples for IGMP, on page 363
- Additional References, on page 366
- Feature History and Information for IGMP, on page 367

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IGMP and IGMP Snooping

Prerequisites for IGMP

- Before performing the tasks in this module, you should be familiar with the concepts explained in the "IP Multicast Routing Technology Overview" module.

- The tasks in this module assume that IP multicast has been enabled and that the Protocol Independent Multicast (PIM) interfaces have been configured using the tasks described in the "Configuring Basic IP Multicast Routing" module.
Prerequisites for IGMP Snooping

Observe these guidelines when configuring the IGMP snooping querier:

- Configure the VLAN in global configuration mode.

- Configure an IP address on the VLAN interface. When enabled, the IGMP snooping querier uses the IP address as the query source address.

- If there is no IP address configured on the VLAN interface, the IGMP snooping querier tries to use the configured global IP address for the IGMP querier. If there is no global IP address specified, the IGMP querier tries to use the VLAN switch virtual interface (SVI) IP address (if one exists). If there is no SVI IP address, the switch uses the first available IP address configured on the switch. The first IP address available appears in the output of the `show ip interface` privileged EXEC command. The IGMP snooping querier does not generate an IGMP general query if it cannot find an available IP address on the switch.

- The IGMP snooping querier supports IGMP Versions 1 and 2.

- When administratively enabled, the IGMP snooping querier moves to the nonquerier state if it detects the presence of a multicast router in the network.

- When it is administratively enabled, the IGMP snooping querier moves to the operationally disabled state under these conditions:
  - IGMP snooping is disabled in the VLAN.
  - PIM is enabled on the SVI of the corresponding VLAN.

Restrictions for IGMP and IGMP Snooping

Restrictions for Configuring IGMP

The following are the restrictions for configuring IGMP:

- The switch supports IGMP Versions 1, 2, and 3.

  **Note**

  For IGMP Version 3, only IGMP Version 3 BISS (Basic IGMPv3 Snooping Support) is supported.

- IGMP Version 3 uses new membership report messages that might not be correctly recognized by older IGMP snooping switches.

- IGMPv3 can operate with both ISM and SSM. In ISM, both exclude and include mode reports are applicable. In SSM, only include mode reports are accepted by the last-hop router. Exclude mode reports are ignored.

- IGMP filtering and throttling is not supported under the WLAN.
Restrictions for IGMP Snooping

The following are the restrictions for IGMP snooping:

- The switch supports IGMPv3 snooping based only on the destination multicast IP address. It does not support snooping based on a source IP address or proxy report.

- IGMPv3 join and leave messages are not supported on switches running IGMP filtering or Multicast VLAN registration (MVR).

- IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

- The IGMP configurable leave time is only supported on hosts running IGMP Version 2. IGMP version 2 is the default version for the switch.

  The actual leave latency in the network is usually the configured leave time. However, the leave time might vary around the configured time, depending on real-time CPU load conditions, network delays and the amount of traffic sent through the interface.

- The IGMP throttling action restriction can be applied only to Layer 2 ports. You can use `ip igmp max-groups action replace` interface configuration command on a logical EtherChannel interface but cannot use it on ports that belong to an EtherChannel port group.

  When the maximum group limitation is set to the default (no maximum), entering the `ip igmp max-groups action {deny | replace}` command has no effect.

  If you configure the throttling action and set the maximum group limitation after an interface has added multicast entries to the forwarding table, the forwarding-table entries are either aged out or removed, depending on the throttling action.

Information About IGMP

Role of the Internet Group Management Protocol

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Enabling PIM on an interface also enables IGMP. IGMP provides a means to automatically control and limit the flow of multicast traffic throughout your network with the use of special multicast queriers and hosts.

- A querier is a network device, such as a router, that sends query messages to discover which network devices are members of a given multicast group.
• A host is a receiver, including routers, that sends report messages (in response to query messages) to inform the querier of a host membership. Hosts use IGMP messages to join and leave multicast groups.

Hosts identify group memberships by sending IGMP messages to their local multicast device. Under IGMP, devices listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

IGMP Multicast Addresses

IP multicast traffic uses group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255.

Multicast addresses in the range 224.0.0.0 to 224.0.0.255 are reserved for use by routing protocols and other network control traffic. The address 224.0.0.0 is guaranteed not to be assigned to any group.

IGMP packets are transmitted using IP multicast group addresses as follows:

• IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).
• IGMP group-specific queries are destined to the group IP address for which the device is querying.
• IGMP group membership reports are destined to the group IP address for which the device is reporting.
• IGMPv2 leave-group messages are destined to the address 224.0.0.2 (all devices on a subnet).
• IGMPv3 membership reports are destined to the address 224.0.0.22; all IGMPv3-capable multicast devices must listen to this address.

Related Topics
Configuring the Switch as a Member of a Group (CLI), on page 328
Example: Configuring the Switch as a Member of a Multicast Group, on page 363

IGMP Versions

The switch supports IGMP version 1, IGMP version 2, and IGMP version 3. These versions are interoperable on the switch. For example, if IGMP snooping is enabled and the querier's version is IGMPv2, and the switch receives an IGMPv3 report from a host, then the switch can forward the IGMPv3 report to the multicast router.

An IGMPv3 switch can receive messages from and forward messages to a device running the Source Specific Multicast (SSM) feature.

Related Topics
Changing the IGMP Version (CLI), on page 331
Restrictions for Configuring IGMP, on page 316
Restrictions for IGMP Snooping, on page 317

IGMP Version 1

IGMP version 1 (IGMPv1) primarily uses a query-response model that enables the multicast router and multilayer switch to find which multicast groups are active (have one or more hosts interested in a multicast group) on the local subnet. IGMPv1 has other processes that enable a host to join and leave a multicast group. For more information, see RFC 1112.
IGMP Version 2

IGMPv2 extends IGMP functionality by providing such features as the IGMP leave process to reduce leave latency, group-specific queries, and an explicit maximum query response time. IGMPv2 also adds the capability for routers to elect the IGMP querier without depending on the multicast protocol to perform this task. For more information, see RFC 2236.

Note

IGMP version 2 is the default version for the switch.

IGMP Version 3

The switch supports IGMP version 3.

An IGMPv3 switch supports Basic IGMPv3 Snooping Support (BISS), which includes support for the snooping features on IGMPv1 and IGMPv2 switches and for IGMPv3 membership report messages. BISS constrains the flooding of multicast traffic when your network includes IGMPv3 hosts. It constrains traffic to approximately the same set of ports as the IGMP snooping feature on IGMPv2 or IGMPv1 hosts.

An IGMPv3 switch can receive messages from and forward messages to a device running the Source Specific Multicast (SSM) feature.

IGMPv3 Host Signaling

IGMPv3 is the third version of the IETF standards track protocol in which hosts signal membership to last-hop devices of multicast groups. IGMPv3 introduces the ability for hosts to signal group membership that allows filtering capabilities with respect to sources. A host can signal either that it wants to receive traffic from all sources sending to a group except for some specific sources (a mode called EXCLUDE) or that it wants to receive traffic only from some specific sources sending to the group (a mode called INCLUDE).

IGMPv3 can operate with both ISM and SSM. In ISM, both EXCLUDE and INCLUDE mode reports are accepted by the last-hop router. In SSM, only INCLUDE mode reports are accepted by the last-hop router.

IGMP Versions Differences

There are three versions of IGMP, as defined by Request for Comments (RFC) documents of the Internet Engineering Task Force (IETF). IGMPv2 improves over IGMPv1 by adding the ability for a host to signal desire to leave a multicast group and IGMPv3 improves over IGMPv2 mainly by adding the ability to listen to multicast originating from a set of source IP addresses only.

Table 12: IGMP Versions

<table>
<thead>
<tr>
<th>IGMP Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMPv1</td>
<td>Provides the basic query-response mechanism that allows the multicast device to determine which multicast groups are active and other processes that enable hosts to join and leave a multicast group. RFC 1112 defines the IGMPv1 host extensions for IP multicasting.</td>
</tr>
</tbody>
</table>
IGMP Versions Differences

<table>
<thead>
<tr>
<th>IGMP Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMPv2</td>
<td>Extends IGMP, allowing such capabilities as the IGMP leave process, group-specific queries, and an explicit maximum response time field. IGMPv2 also adds the capability for devices to elect the IGMP querier without dependence on the multicast protocol to perform this task. RFC 2236 defines IGMPv2.</td>
</tr>
</tbody>
</table>

By default, enabling a PIM on an interface enables IGMPv2 on that device. IGMPv2 was designed to be as backward compatible with IGMPv1 as possible. To accomplish this backward compatibility, RFC 2236 defined special interoperability rules. If your network contains legacy IGMPv1 hosts, you should be familiar with these operability rules. For more information about IGMPv1 and IGMPv2 interoperability, see RFC 2236, Internet Group Management Protocol, Version 2.

Note

By default, enabling a PIM on an interface enables IGMPv2 on that device. IGMPv2 was designed to be as backward compatible with IGMPv1 as possible. To accomplish this backward compatibility, RFC 2236 defined special interoperability rules. If your network contains legacy IGMPv1 hosts, you should be familiar with these operability rules. For more information about IGMPv1 and IGMPv2 interoperability, see RFC 2236, Internet Group Management Protocol, Version 2.

Devices That Run IGMPv1

IGMPv1 devices send IGMP queries to the “all-hosts” multicast address of 224.0.0.1 to solicit multicast groups with active multicast receivers. The multicast receivers also can send IGMP reports to the device to notify it that they are interested in receiving a particular multicast stream. Hosts can send the report asynchronously or in response to the IGMP queries sent by the device. If more than one multicast receiver exists for the same multicast group, only one of these hosts sends an IGMP report message; the other hosts suppress their report messages.

In IGMPv1, there is no election of an IGMP querier. If more than one device on the segment exists, all the devices send periodic IGMP queries. IGMPv1 has no special mechanism by which the hosts can leave the group. If the hosts are no longer interested in receiving multicast packets for a particular group, they simply do not reply to the IGMP query packets sent from the device. The device continues sending query packets. If the device does not hear a response in three IGMP queries, the group times out and the device stops sending multicast packets on the segment for the group. If the host later wants to receive multicast packets after the timeout period, the host simply sends a new IGMP join to the device, and the device begins to forward the multicast packet again.

If there are multiple devices on a LAN, a designated router (DR) must be elected to avoid duplicating multicast traffic for connected hosts. PIM devices follow an election process to select a DR. The PIM device with the highest IP address becomes the DR.

The DR is responsible for the following tasks:

- Sending PIM register and PIM Join and Prune messages toward the rendezvous point (RP) to inform it about host group membership.
- Sending IGMP host-query messages.
- Sending host-query messages by default every 60 seconds in order to keep the IGMP overhead on hosts and networks very low.

Devices That Run IGMPv2

IGMPv2 improves the query messaging capabilities of IGMPv1.

The query and membership report messages in IGMPv2 are identical to the IGMPv1 messages with two exceptions:
• IGMPv2 query messages are broken into two categories: general queries (identical to IGMPv1 queries) and group-specific queries.

• IGMPv1 membership reports and IGMPv2 membership reports have different IGMP type codes.

IGMPv2 also enhances IGMP by providing support for the following capabilities:

• Querier election process--Provides the capability for IGMPv2 devices to elect the IGMP querier without having to rely on the multicast routing protocol to perform the process.

• Maximum Response Time field--A new field in query messages permits the IGMP querier to specify the maximum query-response time. This field permits the tuning of the query-response process to control response burstiness and to fine-tune leave latencies.

• Group-Specific Query messages--Permits the IGMP querier to perform the query operation on a specific group instead of all groups.

• Leave-Group messages--Provides hosts with a method of notifying devices on the network that they wish to leave the group.

Unlike IGMPv1, in which the DR and the IGMP querier are typically the same device, in IGMPv2 the two functions are decoupled. The DR and the IGMP querier are selected based on different criteria and may be different devices on the same subnet. The DR is the device with the highest IP address on the subnet, whereas the IGMP querier is the device with the lowest IP address.

Query messages are used to elect the IGMP querier as follows:

1. When IGMPv2 devices start, they each multicast a general query message to the all-systems group address of 224.0.0.1 with their interface address in the source IP address field of the message.

2. When an IGMPv2 device receives a general query message, the device compares the source IP address in the message with its own interface address. The device with the lowest IP address on the subnet is elected the IGMP querier.

3. All devices (excluding the querier) start the query timer, which is reset whenever a general query message is received from the IGMP querier. If the query timer expires, it is assumed that the IGMP querier has gone down, and the election process is performed again to elect a new IGMP querier.

By default, the timer is two times the query interval.

IGMP Join and Leave Process

IGMP Join Process

When a host wants to join a multicast group, the host sends one or more unsolicited membership reports for the multicast group it wants to join. The IGMP join process is the same for IGMPv1 and IGMPv2 hosts.

In IGMPv3, the join process for hosts proceeds as follows:

• When a host wants to join a group, it sends an IGMPv3 membership report to 224.0.0.22 with an empty EXCLUDE list.

• When a host wants to join a specific channel, it sends an IGMPv3 membership report to 224.0.0.22 with the address of the specific source included in the INCLUDE list.
• When a host wants to join a group excluding particular sources, it sends an IGMPv3 membership report to 224.0.0.22 excluding those sources in the EXCLUDE list.

---

**Note**
If some IGMPv3 hosts on a LAN wish to exclude a source and others wish to include the source, then the device will send traffic for the source on the LAN (that is, inclusion trumps exclusion in this situation).

---

**IGMP Leave Process**

The method that hosts use to leave a group varies depending on the version of IGMP in operation.

**IGMPv1 Leave Process**

There is no leave-group message in IGMPv1 to notify the devices on the subnet that a host no longer wants to receive the multicast traffic from a specific group. The host simply stops processing traffic for the multicast group and ceases responding to IGMP queries with IGMP membership reports for the group. As a result, the only way IGMPv1 devices know that there are no longer any active receivers for a particular multicast group on a subnet is when the devices stop receiving membership reports. To facilitate this process, IGMPv1 devices associate a countdown timer with an IGMP group on a subnet. When a membership report is received for the group on the subnet, the timer is reset. For IGMPv1 devices, this timeout interval is typically three times the query interval (3 minutes). This timeout interval means that the device may continue to forward multicast traffic onto the subnet for up to 3 minutes after all hosts have left the multicast group.

**IGMPv2 Leave Process**

IGMPv2 incorporates a leave-group message that provides the means for a host to indicate that it wishes to stop receiving multicast traffic for a specific group. When an IGMPv2 host leaves a multicast group, if it was the last host to respond to a query with a membership report for that group, it sends a leave-group message to the all-devices multicast group (224.0.0.2).

**IGMPv3 Leave Process**

IGMPv3 enhances the leave process by introducing the capability for a host to stop receiving traffic from a particular group, source, or channel in IGMP by including or excluding sources, groups, or channels in IGMPv3 membership reports.

---

**IGMP Snooping**

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

---

**Note**
For more information on IP multicast and IGMP, see RFC 1112 and RFC 2236.
The multicast router (which could be a switch with the IP services feature) set on the active switch sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. The switch creates one entry per VLAN in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The switch supports IP multicast group-based bridging, instead of MAC-addressed based groups. With multicast MAC address-based groups, if an IP address being configured translates (aliases) to a previously configured MAC address or to any reserved multicast MAC addresses (in the range 224.0.0.xxx), the command fails. Because the switch uses IP multicast groups, there are no address aliasing issues.

The IP multicast groups learned through IGMP snooping are dynamic. However, you can statically configure multicast groups by using the `ip igmp snooping vlan vlan-id static ip_address interface interface-id` global configuration command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings.

You can configure an IGMP snooping querier to support IGMP snooping in subnets without multicast interfaces because the multicast traffic does not need to be routed.

If a port spanning-tree, a port group, or a VLAN ID change occurs, the IGMP snooping-learned multicast groups from this port on the VLAN are deleted.

These sections describe IGMP snooping characteristics:

### Joining a Multicast Group

**Figure 25: Initial IGMP Join Message**

When a host connected to the switch wants to join an IP multicast group and it is an IGMP version 2 client, it sends an unsolicited IGMP join message, specifying the IP multicast group to join. Alternatively, when the switch receives a general query from the router, it forwards the query to all ports in the VLAN. IGMP version 1 or version 2 hosts wanting to join the multicast group respond by sending a join message to the switch. The switch CPU creates a multicast forwarding-table entry for the group if it is not already present. The CPU also adds the interface where the join message was received to the forwarding-table entry. The host associated with that interface receives multicast traffic for that multicast group.

Router A sends a general query to the switch, which forwards the query to ports 2 through 5, all of which are members of the same VLAN. Host 1 wants to join multicast group 224.1.2.3 and multicasts an IGMP
membership report (IGMP join message) to the group. The switch CPU uses the information in the IGMP report to set up a forwarding-table entry that includes the port numbers connected to Host 1 and to the router.

### Table 13: IGMP Snooping Forwarding Table

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Type of Packet</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.1.2.3</td>
<td>IGMP</td>
<td>1, 2</td>
</tr>
</tbody>
</table>

The switch hardware can distinguish IGMP information packets from other packets for the multicast group. The information in the table tells the switching engine to send frames addressed to the 224.1.2.3 multicast IP address that are not IGMP packets to the router and to the host that has joined the group.

**Figure 26: Second Host Joining a Multicast Group**

If another host (for example, Host 4) sends an unsolicited IGMP join message for the same group, the CPU receives that message and adds the port number of Host 4 to the forwarding table. Because the forwarding table directs IGMP messages only to the CPU, the message is not flooded to other ports on the switch. Any known multicast traffic is forwarded to the group and not to the CPU.

### Table 14: Updated IGMP Snooping Forwarding Table

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Type of Packet</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.1.2.3</td>
<td>IGMP</td>
<td>1, 2, 5</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring the Switch as a Member of a Group (CLI), on page 328
- Example: Configuring the Switch as a Member of a Multicast Group, on page 363

### Leaving a Multicast Group

The router sends periodic multicast general queries, and the switch forwards these queries through all ports in the VLAN. Interested hosts respond to the queries. If at least one host in the VLAN wants to receive multicast traffic, the router continues forwarding the multicast traffic to the VLAN. The switch forwards multicast group traffic only to those hosts listed in the forwarding table for that IP multicast group maintained by IGMP snooping.
When hosts want to leave a multicast group, they can silently leave, or they can send a leave message. When the switch receives a leave message from a host, it sends a group-specific query to learn if any other devices connected to that interface are interested in traffic for the specific multicast group. The switch then updates the forwarding table for that MAC group so that only those hosts interested in receiving multicast traffic for the group are listed in the forwarding table. If the router receives no reports from a VLAN, it removes the group for the VLAN from its IGMP cache.

**Immediate Leave**

The switch uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends a leave message without the switch sending group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate Leave ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

Immediate Leave is only supported on IGMP version 2 hosts. IGMP version 2 is the default version for the switch.

**Note**

You should use the Immediate Leave feature only on VLANs where a single host is connected to each port. If Immediate Leave is enabled on VLANs where more than one host is connected to a port, some hosts may be dropped inadvertently.

**Related Topics**

- Enabling IGMP Immediate Leave (CLI), on page 349

**IGMP Configurable-Leave Timer**

You can configure the time that the switch waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group. The IGMP leave response time can be configured from 100 to 32767 milliseconds.

**Related Topics**

- Configuring the IGMP Leave Timer (CLI), on page 350

**IGMP Report Suppression**

**Note**

IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP report suppression is enabled (the default), the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers.
If the multicast router query also includes requests for IGMPv3 reports, the switch forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression, all IGMP reports are forwarded to the multicast routers.

**Related Topics**
- Disabling IGMP Report Suppression (CLI), on page 359

**IGMP Filtering and Throttling**

In some environments, for example, metropolitan or multiple-dwelling unit (MDU) installations, you might want to control the set of multicast groups to which a user on a switch port can belong. You can control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan. You might also want to limit the number of multicast groups to which a user on a switch port can belong.

With the IGMP filtering feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing. You can also set the maximum number of IGMP groups that a Layer 2 interface can join.

IGMP filtering controls only group-specific query and membership reports, including join and leave reports. It does not control general IGMP queries. IGMP filtering has no relationship with the function that directs the forwarding of IP multicast traffic. The filtering feature operates in the same manner whether CGMP or MVR is used to forward the multicast traffic.

IGMP filtering applies only to the dynamic learning of IP multicast group addresses, not static configuration.

With the IGMP throttling feature, you can set the maximum number of IGMP groups that a Layer 2 interface can join. If the maximum number of IGMP groups is set, the IGMP snooping forwarding table contains the maximum number of entries, and the interface receives an IGMP join report, you can configure an interface to drop the IGMP report or to replace the randomly selected multicast entry with the received IGMP report.

---

**Note**

IGMPv3 join and leave messages are not supported on switches running IGMP filtering.

**Default IGMP Configuration**

This table displays the default IGMP configuration for the switch.

**Table 15: Default IGMP Configuration**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multilayer switch as a member of a multicast group</td>
<td>No group memberships are defined.</td>
</tr>
<tr>
<td>Access to multicast groups</td>
<td>All groups are allowed on an interface.</td>
</tr>
<tr>
<td>IGMP version</td>
<td>Version 2 on all interfaces.</td>
</tr>
<tr>
<td>IGMP host-query message interval</td>
<td>60 seconds on all interfaces.</td>
</tr>
</tbody>
</table>
Default IGMP Snooping Configuration

This table displays the default IGMP snooping configuration for the switch.

Table 16: Default IGMP Snooping Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP query timeout</td>
<td>60 seconds on all interfaces.</td>
</tr>
<tr>
<td>IGMP maximum query response time</td>
<td>10 seconds on all interfaces.</td>
</tr>
<tr>
<td>Multilayer switch as a statically connected member</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>

Default IGMP Filtering and Throttling Configuration

This table displays the default IGMP filtering and throttling configuration for the switch.

Table 17: Default IGMP Filtering Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP filters</td>
<td>None applied.</td>
</tr>
<tr>
<td>IGMP maximum number of IGMP groups</td>
<td>No maximum set.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When the maximum number of groups is in the forwarding table, the default IGMP throttling action is to deny the IGMP report.</td>
</tr>
<tr>
<td>IGMP profiles</td>
<td>None defined.</td>
</tr>
<tr>
<td>IGMP profile action</td>
<td>Deny the range addresses.</td>
</tr>
</tbody>
</table>

1 (1) TCN = Topology Change Notification
How to Configure IGMP

Configuring the Switch as a Member of a Group (CLI)

You can configure the switch as a member of a multicast group and discover multicast reachability in a network. If all the multicast-capable routers and multilayer switches that you administer are members of a multicast group, pinging that group causes all of these devices to respond. The devices respond to ICMP echo-request packets addressed to a group of which they are members. Another example is the multicast trace-route tools provided in the software.

⚠️ Caution

Performing this procedure might impact the CPU performance because the CPU will receive all data traffic for the group address.

This procedure is optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# config terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the interface on which you want to enable multicast routing,</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>and enters interface configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 1/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip igmp join-group group-address</td>
<td>Configures the switch to join a multicast group. By default, no group memberships are defined. For group-address, specify the multicast IP address in dotted decimal notation.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip igmp join-group 225.2.2.2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Controlling Access to IP Multicast Group (CLI)

The switch sends IGMP host-query messages to find which multicast groups have members on attached local networks. The switch then forwards to these group members all packets addressed to the multicast group. You can place a filter on each interface to restrict the multicast groups that hosts on the subnet serviced by the interface can join.

To limit the number of joins on the interface, configure the port for the filter which associates with the IGMP profile.

This procedure is optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Joining a Multicast Group, on page 323
- Example: Configuring the Switch as a Member of a Multicast Group, on page 363
- IGMP Multicast Addresses, on page 318
<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
<th>Example</th>
</tr>
</thead>
</table>
| Enters an IGMP filter profile number from 1 to 4294967295. | **Step 3** | ip igmp profile  
Example:  
Switch(config)# ip igmp profile 10  
Switch(config-igmp-profile)# ? |
| For additional information about configuring IGMP filter profiles, see Configuring IGMP Profiles (CLI), on page 337. | | |
| Enters an IGMP profile configuration action. The following IGMP profile configuration actions are supported:  
- deny—Matching IP addresses are denied.  
- exit—Exits from the IGMP profile configuration mode.  
- no—Negates a command or set its defaults.  
- permit—Matching addresses are permitted.  
- range—Adds a range to the set. | **Step 4** | permit  
Example:  
Switch(config-igmp-profile)# permit 229.9.9.0 |
| Returns to global configuration mode. | **Step 5** | exit  
Example:  
Switch(config-igmp-profile)# exit |
| Specifies the interface to be configured, and enters interface configuration mode. | **Step 6** | interface interface-id  
Example:  
Switch(config)# interface gigabitethernet 1/0/1 |
| Specifies the IGMP filter profile number. For additional information about applying IGMP filter profiles, see Applying IGMP Profiles (CLI), on page 339. | **Step 7** | ip igmp filter filter_number  
Example:  
Switch(config-if)# ip igmp filter 10 |
| Returns to privileged EXEC mode. | **Step 8** | end  
Example:  
Switch(config)# end |
| Verifies your entries. | **Step 9** | show ip igmp interface [interface-id]  
Example: |
## Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# show ip igmp interface</td>
<td></td>
</tr>
<tr>
<td>Step 10 copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example: Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Changing the IGMP Version(CLI)

By default, the switch uses IGMP Version 2, which provides features such as the IGMP query timeout and the maximum query response time.

All systems on the subnet must support the same version. The switch does not automatically detect Version 1 systems and switch to Version 1. You can mix Version 1 and Version 2 hosts on the subnet because Version 2 routers or switches always work correctly with IGMPv1 hosts.

Configure the switch for Version 1 if your hosts do not support Version 2.

This procedure is optional.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface interface-id</td>
<td>Specifies the interface to be configured, and enters the interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 1/0/1</td>
<td></td>
</tr>
</tbody>
</table>
### Modifying the IGMP Host-Query Message Interval (CLI)

The switch periodically sends IGMP host-query messages to discover which multicast groups are present on attached networks. These messages are sent to the all-hosts multicast group (224.0.0.1) with a time-to-live (TTL) of 1. The switch sends host-query messages to refresh its knowledge of memberships present on the network. If, after some number of queries, the software discovers that no local hosts are members of a multicast group, the software stops forwarding multicast packets to the local network from remote origins for that group and sends a prune message upstream toward the source.

The switch elects a PIM designated router (DR) for the LAN (subnet). The designated router is responsible for sending IGMP host-query messages to all hosts on the LAN. In sparse mode, the designated router also sends PIM register and PIM join messages toward the RP router. With IGMPv2, the DR is the router or multilayer switch with the highest IP address. With IGMPv1, the DR is elected according to the multicast routing protocol that runs on the LAN.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>`ip igmp version {1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# ip igmp version 2</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>show ip igmp interface [interface-id]</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# show ip igmp interface</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**
- IGMP Versions, on page 318
- Restrictions for Configuring IGMP, on page 316
- Restrictions for IGMP Snooping, on page 317

**Verifying your entries.**

**Returns to privileged EXEC mode.**

**Verifies your entries.**

**(Optional) Saves your entries in the configuration file.**

---

**Modifying the IGMP Host-Query Message Interval (CLI)**

The switch periodically sends IGMP host-query messages to discover which multicast groups are present on attached networks. These messages are sent to the all-hosts multicast group (224.0.0.1) with a time-to-live (TTL) of 1. The switch sends host-query messages to refresh its knowledge of memberships present on the network. If, after some number of queries, the software discovers that no local hosts are members of a multicast group, the software stops forwarding multicast packets to the local network from remote origins for that group and sends a prune message upstream toward the source.

The switch elects a PIM designated router (DR) for the LAN (subnet). The designated router is responsible for sending IGMP host-query messages to all hosts on the LAN. In sparse mode, the designated router also sends PIM register and PIM join messages toward the RP router. With IGMPv2, the DR is the router or multilayer switch with the highest IP address. With IGMPv1, the DR is elected according to the multicast routing protocol that runs on the LAN.
This procedure is optional.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable&lt;br&gt;<strong>Example:</strong> Switch&gt; enable</td>
<td>Enables privileged EXEC mode.&lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal&lt;br&gt;<strong>Example:</strong> Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface <em>interface-id</em>&lt;br&gt;<strong>Example:</strong> Switch(config)# interface gigabitethernet 1/0/1</td>
<td>Specifies the interface on which you want to enable multicast routing, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip igmp query-interval <em>seconds</em>&lt;br&gt;<strong>Example:</strong> Switch(config-if)# ip igmp query-interval 75</td>
<td>Configures the frequency at which the designated router sends IGMP host-query messages.&lt;br&gt;By default, the designated router sends IGMP host-query messages every 60 seconds to keep the IGMP overhead very low on hosts and networks.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end&lt;br&gt;<strong>Example:</strong> Switch(config)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show ip igmp interface [interface-id]&lt;br&gt;<strong>Example:</strong> Switch# show ip igmp interface</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config&lt;br&gt;<strong>Example:</strong> Switch# copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Changing the IGMP Query Timeout for IGMPv2 (CLI)

If you are using IGMPv2, you can specify the period of time before the switch takes over as the querier for the interface. By default, the switch waits twice the query interval period controlled by the `ip igmp query-interval` interface configuration command. After that time, if the switch has received no queries, it becomes the querier.

This procedure is optional.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the interface on which you want to enable multicast routing, and enters interface configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# interface gigabitethernet 1/0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies the IGMP query timeout.</td>
</tr>
<tr>
<td><code>ip igmp querier-timeout seconds</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>The default is 60 seconds (twice the query interval). The range is 60 to 300.</td>
</tr>
<tr>
<td><code>Switch(config-if)# ip igmp querier-timeout 120</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>show ip igmp interface [interface-id]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show ip igmp interface</code></td>
<td></td>
</tr>
</tbody>
</table>
Changing the Maximum Query Response Time for IGMPv2 (CLI)

If you are using IGMPv2, you can change the maximum query response time advertised in IGMP queries. The maximum query response time enables the switch to quickly detect that there are no more directly connected group members on a LAN. Decreasing the value enables the switch to prune groups faster. This procedure is optional.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 1/0/1</td>
<td>Specifies the interface on which you want to enable multicast routing, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip igmp query-max-response-time seconds</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip igmp query-max-response-time 15</td>
<td>Changes the maximum query response time advertised in IGMP queries.</td>
</tr>
<tr>
<td></td>
<td>The default is 10 seconds. The range is 1 to 25.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Verifies your entries.

Example:

Step 6  show ip igmp interface [interface-id]  (Optional) Saves your entries in the configuration file.

Example:

Step 7  copy running-config startup-config

Configuring the Switch as a Statically Connected Member (CLI)

At various times, either there is not a group member on a network segment or a host that cannot report its group membership by using IGMP. However, you may want multicast traffic to be sent to that network segment. The following commands are used to pull multicast traffic down to a network segment:

- **ip igmp join-group**—The switch accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the switch from fast switching.

- **ip igmp static-group**—The switch does not accept the packets itself, but only forwards them. This method enables fast switching. The outgoing interface appears in the IGMP cache, but the switch itself is not a member, as evidenced by lack of an L (local) flag in the multicast route entry.

This procedure is optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>  enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:  Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong>  configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:  Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
Configuring IGMP Profiles (CLI)

Follow these steps to create an IGMP profile:

This task is optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 3</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>interface <strong>interface-id</strong></td>
<td>Specifies the interface on which you want to enable multicast routing, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 1/0/1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 4</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp static-group <strong>group-address</strong></td>
<td>Configures the switch as a statically connected member of a group. By default, this feature is disabled.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip igmp static-group 239.100.100.101</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 5</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 6</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp interface <strong>[interface-id]</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show ip igmp interface gigabitethernet 1/0/1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 7</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>ip igmp profile profile number</td>
<td>Assigns a number to the profile you are</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>configuring, and enters IGMP profile</td>
</tr>
<tr>
<td>Switch(config)# ip igmp profile 3</td>
<td>configuration mode. The profile number</td>
</tr>
<tr>
<td></td>
<td>range is 1 to 4294967295. When you are in</td>
</tr>
<tr>
<td></td>
<td>IGMP profile configuration mode, you can</td>
</tr>
<tr>
<td></td>
<td>create the profile by using these commands:</td>
</tr>
<tr>
<td></td>
<td>• deny—Specifies that matching addresses</td>
</tr>
<tr>
<td></td>
<td>are denied; this is the default.</td>
</tr>
<tr>
<td></td>
<td>• exit—Exits from igmp-profile configuration</td>
</tr>
<tr>
<td></td>
<td>mode.</td>
</tr>
<tr>
<td></td>
<td>• no—Negates a command or returns to its</td>
</tr>
<tr>
<td></td>
<td>defaults.</td>
</tr>
<tr>
<td></td>
<td>• permit—Specifies that matching addresses</td>
</tr>
<tr>
<td></td>
<td>are permitted.</td>
</tr>
<tr>
<td></td>
<td>• range—Specifies a range of IP addresses</td>
</tr>
<tr>
<td></td>
<td>for the profile. You can enter a single IP</td>
</tr>
<tr>
<td></td>
<td>address or a range with a start and an end</td>
</tr>
<tr>
<td></td>
<td>address.</td>
</tr>
<tr>
<td></td>
<td>The default is for the switch to have no IGMP</td>
</tr>
<tr>
<td></td>
<td>profiles configured.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> To delete a profile, use the <strong>no</strong></td>
</tr>
<tr>
<td></td>
<td><strong>ip igmp profile profile number</strong> global</td>
</tr>
<tr>
<td></td>
<td>configuration command.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
Purpose
Command or Action

Note
To delete an IP multicast address or range of IP multicast addresses, use the no range ip multicast address IGMP profile configuration command.

Step 6
end
Example:
Switch(config)# end

Step 7
show ip igmp profile profile number
Example:
Switch# show ip igmp profile 3

Step 8
show running-config
Example:
Switch# show running-config

Step 9
copy running-config startup-config
Example:
Switch# copy running-config startup-config

Applying IGMP Profiles (CLI)

To control access as defined in an IGMP profile, you have to apply the profile to the appropriate interfaces. You can apply IGMP profiles only to Layer 2 access ports; you cannot apply IGMP profiles to routed ports or SVIs. You cannot apply profiles to ports that belong to an EtherChannel port group. You can apply a profile to multiple interfaces, but each interface can have only one profile applied to it.

Follow these steps to apply an IGMP profile to a switch port:

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
### Setting the Maximum Number of IGMP Groups (CLI)

Follow these steps to set the maximum number of IGMP groups that a Layer 2 interface can join:

#### Before you begin

This restriction can be applied to Layer 2 ports only; you cannot set a maximum number of IGMP groups on routed ports or SVIs. You also can use this command on a logical EtherChannel interface but cannot use it on ports that belong to an EtherChannel port group.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2** configure terminal  
Example:  
Switch# configure terminal | Enters global configuration mode. |
| **Step 3** interface interface-id  
Example:  
Switch(config)# interface gigabitethernet1/0/1 | Specifies the physical interface, and enters interface configuration mode. The interface must be a Layer 2 port that does not belong to an EtherChannel port group. |
| **Step 4** ip igmp filter profile number  
Example:  
Switch(config-if)# ip igmp filter 321 | Applies the specified IGMP profile to the interface. The range is 1 to 4294967295.  
**Note** To remove a profile from an interface, use the `no ip igmp filter profile number interface configuration command`. |
| **Step 5** end  
Example:  
Switch(config-if)# end | Returns to privileged EXEC mode. |
| **Step 6** show running-config  
Example:  
Switch# show running-config | Verifies your entries. |
| **Step 7** copy running-config startup-config  
Example:  
Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
  * Enter your password if prompted. |
| Example: | Switch> enable |
| **Step 2** | configure terminal | Enters global configuration mode. |
| Example: | Switch# configure terminal |
| **Step 3** | interface interface-id | Specifies the interface to be configured, and enters interface configuration mode. The interface can be a Layer 2 port that does not belong to an EtherChannel group or a EtherChannel interface. |
| Example: | Switch(config)# interface gigabitethernet1/0/2 |
| **Step 4** | ip igmp max-groups number | Sets the maximum number of IGMP groups that the interface can join. The range is 0 to 4294967294. The default is to have no maximum set.  
  **Note** The switch supports a maximum number of 4096 Layer 2 IGMP groups and 2048 Layer 3 IGMP groups. |
| Example: | Switch(config-if)# ip igmp max-groups 20 |
| **Step 5** | end | Returns to privileged EXEC mode. |
| Example: | Switch(config)# end |
| **Step 6** | show running-config interface interface-id | Verifies your entries. |
| Example: | Switch# interface gigabitethernet1/0/1 |
| **Step 7** | copy running-config startup-config | *(Optional)* Saves your entries in the configuration file. |
| Example: | Switch# copy running-config startup-config |
### Configuring the IGMP Throttling Action (CLI)

After you set the maximum number of IGMP groups that a Layer 2 interface can join, you can configure an interface to replace the existing group with the new group for which the IGMP report was received.

Follow these steps to configure the throttling action when the maximum number of entries is in the forwarding table:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
<td>Specifies the physical interface to be configured, and enters interface configuration mode. The interface can be a Layer 2 port that does not belong to an EtherChannel group or an EtherChannel interface. The interface cannot be a trunk port.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface gigabitethernet1/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>ip igmp max-groups action {deny</td>
<td>replace}</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# ip igmp max-groups action replace</td>
<td>• <strong>deny</strong>—Drops the report. If you configure this throttling action, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out and the maximum number of entries is in the forwarding table, the switch drops the next IGMP report received on the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>replace</strong>—Replaces the existing group with the new group for which the IGMP report was received. If you configure this throttling action, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the</td>
</tr>
</tbody>
</table>
How to Configure IGMP Snooping

Enabling IGMP Snooping

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

Example:

Switch(config)# end

Step 6

show running-config interface interface-id

Verify your entries.

Example:

Switch# show running-config interface gigabitethernet1/0/1

Step 7

copy running-config startup-config

(Optional) Saves your entries in the configuration file.

Example:

Switch# copy running-config startup-config
### Enabling or Disabling IGMP Snooping on a VLAN Interface (CLI)

Follow these steps to enable IGMP snooping on a VLAN interface:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

---

### Enabling or Disabling IGMP Snooping on a VLAN Interface (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> ip igmp snooping</td>
<td>Globally enables IGMP snooping after it has been disabled.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip igmp snooping</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> bridge-domain bridge-id</td>
<td>(Optional) Enters bridge domain configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# bridge-domain 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ip igmp snooping</td>
<td>(Optional) Enables IGMP snooping on the bridge domain interface being configured.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Required only if IGMP snooping was previously explicitly disabled on the specified bridge domain.</td>
</tr>
<tr>
<td>Device(config-bdomain)# ip igmp snooping</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-bdomain)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Setting the Snooping Method (CLI)

Multicast-capable router ports are added to the forwarding table for every Layer 2 multicast entry. The switch learns of the ports through one of these methods:

- Snooping on IGMP queries, Protocol-Independent Multicast (PIM) packets
- Statically connecting to a multicast router port using the `ip igmp snooping mrouter` global configuration command

Beginning in privileged EXEC mode, follow these steps to alter the method in which a VLAN interface accesses a multicast router:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
</tbody>
</table>

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip igmp snooping vlan vlan-id</code></td>
<td>Enables IGMP snooping on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td><code>no ip igmp snooping vlan vlan-id</code></td>
<td>To disable IGMP snooping on a VLAN interface, use the <code>no ip igmp snooping vlan vlan-id</code> global configuration command for the specified VLAN number.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
## Configuring a Multicast Router Port (CLI)

Perform these steps to add a multicast router port (enable a static connection to a multicast router) on the switch.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Configuring a Multicast Router Port (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip igmp snooping vlan vlan-id mrouter interface {GigabitEthernet</td>
<td>Enables IGMP snooping on a VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td>Port-Channel</td>
<td>TenGigabitEthernet}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip igmp snooping</td>
<td></td>
</tr>
<tr>
<td>vlan 1 mrouter interface</td>
<td></td>
</tr>
<tr>
<td>GigabitEthernet 1/0/3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show ip igmp snooping</td>
<td>Verifies the configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show ip igmp snooping</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config</td>
<td></td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Note

Static connections to multicast routers are supported only on switch ports.
### Configuring a Multicast Router Port (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch &gt; enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>ip igmp snooping vlan vlan-id mrouter interface interface-id</code></td>
<td>Specifies the multicast router VLAN ID and the interface to the multicast router.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# ip igmp snooping vlan 5 mrouter interface gigabitethernet1/0/1</code></td>
<td>- The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td></td>
<td>- The interface can be a physical interface or a port channel. The port-channel range is 1 to 128.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>To remove a multicast router port from the VLAN, use the <code>no ip igmp snooping vlan vlan-id mrouter interface interface-id global</code> configuration command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>show ip igmp snooping mrouter [vlan vlan-id]</code></td>
<td>Verifies that IGMP snooping is enabled on the VLAN interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show ip igmp snooping mroutervlan 5</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Host Statically to Join a Group (CLI)

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also statically configure a host on an interface.

Follow these steps to add a Layer 2 port as a member of a multicast group:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
*Example:*  
Switch> enable |
| Step 2 | configure terminal | Enters global configuration mode. |
| Step 3 | ip igmp snooping vlan vlan-id static ip_address interface interface-id | Statically configures a Layer 2 port as a member of a multicast group:  
*Example:*  
Switch(config)# ip igmp snooping vlan 105 static 230.0.0.1 interface gigabitethernet1/0/1  
*Note:* To remove the Layer 2 port from the multicast group, use the no ip igmp snooping vlan vlan-id static mac-address interface interface-id global configuration command. |
| Step 4 | end | Returns to privileged EXEC mode. |
| Step 5 | show ip igmp snooping groups | Verifies the member port and the IP address. |

*Note:* Return to privileged EXEC mode.
Enabling IGMP Immediate Leave (CLI)

When you enable IGMP Immediate Leave, the switch immediately removes a port when it detects an IGMP Version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN.

**Note**

Immediate Leave is supported only on IGMP Version 2 hosts. IGMP Version 2 is the default version for the switch.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
  * Enter your password if prompted. |
|      | Example: Switch> enable |
| Step 2 | configure terminal | Enters global configuration mode. |
|      | Example: Switch# configure terminal |
| Step 3 | ip igmp snooping vlan vlan-id immediate-leave | Enables IGMP Immediate Leave on the VLAN interface.  
  **Note** To disable IGMP Immediate Leave on a VLAN, use the no ip igmp snooping vlan vlan-id immediate-leave global configuration command. |
|      | Example: Switch(config)# ip igmp snooping vlan 21 immediate-leave |
| Step 4 | end | Returns to privileged EXEC mode. |
|      | Example: Switch(config)# end |

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Example:

Step 6

Switch# copy running-config startup-config
### Configuring the IGMP Leave Timer (CLI)

You can configure the leave time globally or on a per-VLAN basis. Follow these steps to enable the IGMP configurable-leave timer:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal                             | Enters global configuration mode.                                      |
| Example:                                                  |                                                                          |
| Switch# configure terminal                                |                                                                          |

| **Step 3** ip igmp snooping last-member-query-interval time | Configures the IGMP leave timer globally. The range is 100 to 32767 milliseconds. The default leave time is 1000 milliseconds. Note To globally reset the IGMP leave timer to the default setting, use the no ip igmp snooping last-member-query-interval global configuration command. |
| Example:                                                  |                                                                          |
| Switch(config)# ip igmp snooping last-member-query-interval 1000 |                                                                          |
### Configuring the IGMP Robustness-Variable (CLI)

Use the following procedure to configure the IGMP robustness variable on the switch.

The robustness variable is the integer used by IGMP snooping during calculations for IGMP messages. The robustness variable provides fine tuning to allow for expected packet loss.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

---

**Related Topics**

- IGMP Configurable-Leave Timer, on page 325
## Configuring the IGMP Robustness-Variable (CLI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>3</td>
<td>ip igmp snooping robustness-variable count</td>
<td>Configures the IGMP robustness variable. The range is 1 to 3 times. The recommended value for the robustness variable is 2. Use this command to change the value of the robustness variable for IGMP snooping from the default (2) to a specified value.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Switch(config)# ip igmp snooping robustness-variable 3</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>Configuring the robustness variable count on a VLAN overrides the globally configured value.</td>
</tr>
<tr>
<td>4</td>
<td>ip igmp snooping vlan vlan-id robustness-variable count</td>
<td>(Optional) Configures the IGMP robustness variable on the VLAN interface. The range is 1 to 3 times. The recommended value for the robustness variable is 2.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Switch(config)# ip igmp snooping vlan 10 robustness-variable 3</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>Configuring the robustness variable count on a VLAN overrides the globally configured value.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td>6</td>
<td>show ip igmp snooping</td>
<td>(Optional) Displays the configured IGMP robustness variable count.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Switch# show ip igmp snooping</td>
</tr>
<tr>
<td>7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>
Configuring the IGMP Last Member Query Count (CLI)

To configure the number of times the switch sends IGMP group-specific or group-source-specific (with IGMP version 3) query messages in response to receiving a group-specific or group-source-specific leave message, use this command.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
</tbody>
</table>

```
Switch> enable
```

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enters global configuration mode.</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

```
Switch# configure terminal
```

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the IGMP last member query count. The range is 1 to 7 messages. The default is 2 messages.</td>
<td>ip igmp snooping last-member-query-count count</td>
<td>Configures the IGMP last member query count. The range is 1 to 7 messages. The default is 2 messages.</td>
</tr>
</tbody>
</table>

```
Switch(config)# ip igmp snooping last-member-query-count 3
```

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Configures the IGMP last member query count on the VLAN interface. The range is 1 to 7 messages.</td>
<td>ip igmp snooping vlan vlan-id last-member-query-count count</td>
<td>(Optional) Configures the IGMP last member query count on the VLAN interface. The range is 1 to 7 messages.</td>
</tr>
</tbody>
</table>

```
Switch(config)# ip igmp snooping vlan 100 last-member-query-count 3
```

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns to privileged EXEC mode.</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

```
Switch(config)# end
```

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Displays the configured IGMP last member query count.</td>
<td>show ip igmp snooping</td>
<td>(Optional) Displays the configured IGMP last member query count.</td>
</tr>
</tbody>
</table>

```
Switch# show ip igmp snooping
```
### Configuring TCN-Related Commands

#### Controlling the Multicast Flooding Time After a TCN Event (CLI)

You can configure the number of general queries by which multicast data traffic is flooded after a topology change notification (TCN) event. If you set the TCN flood query count to 1 the flooding stops after receiving 1 general query. If you set the count to 7, the flooding continues until 7 general queries are received. Groups are relearned based on the general queries received during the TCN event.

Some examples of TCN events are when the client location is changed and the receiver is on same port that was blocked but is now forwarding, and when a port goes down without sending a leave message.

Follow these steps to configure the TCN flood query count:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
  * Enter your password if prompted. |
| Example: | Switch> enable | |
| Step 2 | configure terminal | Enters global configuration mode. |
| Example: | Switch# configure terminal | |
| Step 3 | ip igmp snooping tcn flood query count \( count \) | Specifies the number of IGMP general queries for which the multicast traffic is flooded.  
The range is 1 to 10. The default, the flooding query count is 2. |
| Example: | Switch(config)# ip igmp snooping tcn flood query count 3 | |
| Note | To return to the default flooding query count, use the no ip igmp snooping tcn flood query count global configuration command. |
| Step 4 | end | Returns to privileged EXEC mode. |
### Recovering from Flood Mode (CLI)

When a topology change occurs, the spanning-tree root sends a special IGMP leave message (also known as global leave) with the group multicast address 0.0.0.0. However, you can enable the switch to send the global leave message whether it is the spanning-tree root or not. When the router receives this special leave, it immediately sends general queries, which expedite the process of recovering from the flood mode during the TCN event. Leaves are always sent if the switch is the spanning-tree root regardless of this configuration.

Follow these steps to enable sending of leave messages:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip igmp snooping tcn query solicit</td>
<td>Sends an IGMP leave message (global leave) to speed the process of recovering from the flood mode caused during a TCN event. By default, query solicitation is disabled.</td>
</tr>
<tr>
<td>Example:</td>
<td>To return to the default query solicitation, use the no ip igmp snooping tcn query solicit global configuration command.</td>
</tr>
</tbody>
</table>
Disabling Multicast Flooding During a TCN Event (CLI)

When the switch receives a TCN, multicast traffic is flooded to all the ports until 2 general queries are received. If the switch has many ports with attached hosts that are subscribed to different multicast groups, this flooding might exceed the capacity of the link and cause packet loss. Follow these steps to control TCN flooding:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  * enable
  * Example:
    * Switch> enable | Enables privileged EXEC mode.
    * • Enter your password if prompted. |
| **Step 2**
  * configure terminal
  * Example:
    * Switch# configure terminal | Enters global configuration mode. |
| **Step 3**
  * interface interface-id
  * Example:
    * Switch(config)# interface gigabitethernet 1/0/1 | Specifies the interface to be configured, and enters interface configuration mode. |
## Configuring the IGMP Snooping Querier (CLI)

Follow these steps to enable the IGMP snooping querier feature in a VLAN:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;enable&lt;br&gt;Example:&lt;br&gt;<code>Switch&gt; enable</code></td>
<td>Enables privileged EXEC mode.&lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;configure terminal&lt;br&gt;Example:&lt;br&gt;<code>Switch# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>3</td>
<td><code>ip igmp snooping querier</code></td>
</tr>
</tbody>
</table>

**Example:**
```
Switch(config)# ip igmp snooping querier
```

| 4    | `ip igmp snooping querier address ip_address` | (Optional) Specifies an IP address for the IGMP snooping querier. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier. |

**Note** The IGMP snooping querier does not generate an IGMP general query if it cannot find an IP address on the switch. | 

**Example:**
```
Switch(config)# ip igmp snooping querier address 172.16.24.1
```

| 5    | `ip igmp snooping querier query-interval interval-count` | (Optional) Sets the interval between IGMP queries. The range is 1 to 18000 seconds. |

**Example:**
```
Switch(config)# ip igmp snooping querier query-interval 30
```

| 6    | `ip igmp snooping querier tcn query count | interval` | (Optional) Sets the time between Topology Change Notification (TCN) queries. The count range is 1 to 10. The interval range is 1 to 255 seconds. |

**Example:**
```
Switch(config)# ip igmp snooping querier tcn query interval 20
```

| 7    | `ip igmp snooping querier timer expiry timeout` | (Optional) Sets the length of time until the IGMP querier expires. The range is 60 to 300 seconds. |

**Example:**
```
Switch(config)# ip igmp snooping querier timer expiry 180
```

| 8    | `ip igmp snooping querier version version` | (Optional) Selects the IGMP version number that the querier feature uses. Select 1 or 2. |

**Example:**
```
Switch(config)# ip igmp snooping querier version 2
```

| 9    | `end` | Returns to privileged EXEC mode. |

**Example:**
```
Switch(config)# end
```
Disabling IGMP Report Suppression (CLI)

Follow these steps to disable IGMP report suppression:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>no ip igmp snooping report-suppression</td>
<td>Disables IGMP report suppression. When report suppression is disabled, all IGMP reports are forwarded to the multicast routers.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>IGMP report suppression is enabled by default.</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# no ip igmp snooping report-suppression</td>
<td>When IGMP report suppression is enabled, the switch forwards only one IGMP report per multicast router query.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> To re-enable IGMP report suppression, use the <strong>ip igmp snooping report-suppression</strong> global configuration command.</td>
</tr>
</tbody>
</table>
Monitor IGMP

You can display specific statistics, such as the contents of IP routing tables, caches, and databases.

**Note**
This release does not support per-route statistics.

You can display information to learn resource usage and solve network problems. You can also display information about node reachability and discover the routing path that packets of your device are taking through the network.

You can use any of the privileged EXEC commands in the following table to display various routing statistics.

**Table 18: Commands for Displaying System and Network Statistics**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping [group-name</td>
<td>group-address]</td>
</tr>
<tr>
<td>show ip igmp filter</td>
<td>Displays IGMP filter information.</td>
</tr>
<tr>
<td>show ip igmp groups [type-number</td>
<td>detail ]</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td><code>show ip igmp interface [type number]</code></td>
<td>Displays multicast-related information about an interface.</td>
</tr>
<tr>
<td>`show ip igmp membership [ name/group address</td>
<td>all</td>
</tr>
<tr>
<td><code>show ip igmp profile [ profile_number]</code></td>
<td>Displays IGMP profile information.</td>
</tr>
<tr>
<td><code>show ip igmp ssm-mapping [ hostname/IP address ]</code></td>
<td>Displays IGMP SSM mapping information.</td>
</tr>
<tr>
<td><code>show ip igmp static-group [class-map [ interface [ type ] ]</code></td>
<td>Displays static group information.</td>
</tr>
<tr>
<td><code>show ip igmp vrf</code></td>
<td>Displays the selected VPN routing/forwarding instance by name.</td>
</tr>
</tbody>
</table>

### Monitoring IGMP Snooping Information

You can display IGMP snooping information for dynamically learned and statically configured router ports and VLAN interfaces. You can also display MAC address multicast entries for a VLAN configured for IGMP snooping.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip igmp snooping detail</code></td>
<td>Displays the operational state information.</td>
</tr>
</tbody>
</table>
| `show ip igmp snooping groups [ count | [vlan vlan-id [A.B.C.D | count ] ]` | Displays multicast table information for the switch or about a specific parameter:  
  - `count`—Displays the total number of groups.  
  - `vlan`—Displays group information by VLAN ID. |
| `show ip igmp snooping igmpv2-tracking` | Displays the IGMP snooping tracking.  
**Note**  
This command displays group and IP address entries only for wireless multicast IGMP joins and not for wired IGMP joins. Wireless IP multicast must be enabled for this command to display. |
### Monitoring IGMP Filtering and Throttling Configuration

You can display IGMP profile characteristics, and you can display the IGMP profile and maximum group configuration for all interfaces on the switch or for a specified interface. You can also display the IGMP throttling configuration for all interfaces on the switch or for a specified interface.

#### Table 20: Commands for Displaying IGMP Filtering and Throttling Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ip igmp snooping mrouter [vlan vlan-id]</strong></td>
<td>Displays information on dynamically learned and manually configured multicast router interfaces.</td>
</tr>
<tr>
<td>**show ip igmp snooping querier [ detail</td>
<td>vlan vlan-id]**</td>
</tr>
<tr>
<td><strong>show ip igmp snooping [vlan vlan-id [ detail ]]</strong></td>
<td>Displays the snooping configuration information for all VLANs on the switch or for a specified VLAN. (Optional) Enter <code>vlan vlan-id</code> to display information for a single VLAN.</td>
</tr>
<tr>
<td><strong>show ip igmp snooping wireless mgid</strong></td>
<td>Displays wireless-related events.</td>
</tr>
<tr>
<td><strong>show ip igmp profile [profile number]</strong></td>
<td>Displays the specified IGMP profile or all the IGMP profiles defined on the switch.</td>
</tr>
<tr>
<td><strong>show running-config [interface interface-id]</strong></td>
<td>Displays the configuration of the specified interface or the configuration of all interfaces on the switch, including (if configured) the maximum number of IGMP groups to which an interface can belong and the IGMP profile applied to the interface.</td>
</tr>
</tbody>
</table>
Configuration Examples for IGMP

Example: Configuring the Switch as a Member of a Multicast Group

This example shows how to enable the switch to join multicast group 255.2.2.2:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp join-group 255.2.2.2
```

Related Topics
- Configuring the Switch as a Member of a Group (CLI), on page 328
- Joining a Multicast Group, on page 323
- IGMP Multicast Addresses, on page 318

Example: Controlling Access to Multicast Groups

To limit the number of joins on the interface, configure the port for filter which associates with the IGMP profile.

```
Switch# configure terminal
Switch(config)# ip igmp profile 10
Switch(config-igmp-profile)# ?
IGMP profile configuration commands:
deny matching addresses are denied
exit Exit from igmp profile configuration mode
no Negate a command or set its defaults
permit matching addresses are permitted
range add a range to the set
Switch(config-igmp-profile)# range 172.16.5.1
Switch(config-igmp-profile)# exit
Switch(config)# interface gigabitEthernet 2/0/10
Switch(config-if)# ip igmp filter 10
```

Examples: Configuring IGMP Snooping

This example shows how to enable a static connection to a multicast router:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet1/0/2
Switch(config)# end
```

This example shows how to statically configure a host on a port:

```
Switch# configure terminal
```
Example: Configuring IGMP Profiles

This example shows how to enable IGMP Immediate Leave on VLAN 130:

Switch# configure terminal
Switch(config)# ip igmp snooping vlan 130 immediate-leave
Switch(config)# end

This example shows how to set the IGMP snooping querier source address to 10.0.0.64:

Switch# configure terminal
Switch(config)# ip igmp snooping querier 10.0.0.64
Switch(config)# end

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end

This example shows how to set the IGMP snooping querier timeout to 60 seconds:

Switch# configure terminal
Switch(config)# ip igmp snooping querier timer expiry 60
Switch(config)# end

This example shows how to set the IGMP snooping querier feature to Version 2:

Switch# configure terminal
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end

Example: Configuring IGMP Profiles

This example shows how to create IGMP profile 4 allowing access to the single IP multicast address and how to verify the configuration. If the action was to deny (the default), it would not appear in the show ip igmp profile output display.

Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
  permit
    range 229.9.9.0 229.9.9.0
Example: Applying IGMP Profile

This example shows how to apply IGMP profile 4 to a port:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

Example: Setting the Maximum Number of IGMP Groups

This example shows how to limit to 25 the number of IGMP groups that a port can join:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
```

Example: Interface Configuration as a Routed Port

This example shows how to configure an interface on the switch as a routed port. This configuration is required on the interface for several IP multicast routing configuration procedures that require running the `no switchport` command.

```
Switch configure terminal
Switch(config)# interface GigabitEthernet1/0/9
Switch(config-if)# description interface to be use as routed port
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.20.20.1 255.255.255.0
Switch(config-if)# ip pim sparse-mode
Switch(config-if)# ip igmp join-group 224.1.2.3 source 15.15.15.2
Switch(config-if)# end
Switch# configure terminal
Switch# show run interface gigabitEthernet 1/0/9
```

Example: Interface Configuration as an SVI

This example shows how to configure an interface on the switch as an SVI. This configuration is required on the interface for several IP multicast routing configuration procedures that require running the `no switchport` command.

```
Switch(config)# interface vlan 150
Switch(config-if)# ip address 10.20.20.1 255.255.255.0
Switch(config-if)# ip pim sparse-mode
Switch(config-if)# ip igmp join-group 224.1.2.3 source 15.15.15.2
Switch(config-if)# end
```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 20 static 224.1.2.3
interface gigabitEthernet 1/0/9
Switch# show run interface vlan 150

Current configuration : 137 bytes
! interface Vlan150
  ip address 10.20.20.1 255.255.255.0
  ip pim sparse-mode
  ip igmp static-group 224.1.2.3 source 15.15.15.2
end

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>For complete syntax and usage information for the commands used in this chapter.</td>
<td>IP Multicast Routing Command Reference (Catalyst 3850 Switches) Cisco 5760 Multicast Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Cisco IOS IP SLAs commands</td>
<td>Cisco IOS IP Multicast Command Reference</td>
</tr>
</tbody>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1112</td>
<td>Host Extensions for IP Multicasting</td>
</tr>
<tr>
<td>RFC 2236</td>
<td>Internet Group Management Protocol, Version 2</td>
</tr>
<tr>
<td>RFC 3376</td>
<td>Internet Group Management Protocol, Version 3</td>
</tr>
</tbody>
</table>
### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

### Feature History and Information for IGMP

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring Wireless Multicast

- Finding Feature Information, on page 369
- Prerequisites for Configuring Wireless Multicast, on page 369
- Restrictions on Configuring Wireless Multicast, on page 370
- Information About Wireless Multicast, on page 370
- How to Configure Wireless Multicast, on page 374
- Monitoring Wireless Multicast, on page 381
- Where to Go Next for Wireless Multicast, on page 381

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Wireless Multicast

- IP multicast routing must be enabled. The default routes should be available in the device. After performing these tasks, the device can forward multicast packets and populate its multicast routing table. The network should be multicast enabled to configure multicast mode.

- To participate in IP multicasting, the multicast hosts, routers, and multilayer switches must have IGMP operating.

- When enabling multicast mode on the switch, a CAPWAP multicast group address should also be configured. Access points listen to the CAPWAP multicast group using IGMP.
Restrictions on Configuring Wireless Multicast

The following are the restrictions for configuring IP multicast routing:

- Access points in monitor mode, sniffer mode, or rogue-detector mode do not join the CAPWAP multicast group address.
- The CAPWAP multicast group configured on the switch should be different for different switches.
- Multicast routing should not be enabled for the management interface.

Restrictions for IPv6 Snooping

The IPv6 snooping feature is not supported on Etherchannel ports.

Restrictions for IPv6 RA Guard

- The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.
- This feature is supported only in hardware when the ternary content addressable memory (TCAM) is programmed.
- This feature can be configured on a switch port interface in the ingress direction.
- This feature supports host mode and router mode.
- This feature is supported only in the ingress direction; it is not supported in the egress direction.
- This feature is not supported on EtherChannel and EtherChannel port members.
- This feature is not supported on trunk ports with merge mode.
- This feature is supported on auxiliary VLANs and private VLANs (PVLANS). In the case of PVLANS, primary VLAN features are inherited and merged with port features.
- Packets dropped by the IPv6 RA Guard feature can be spanned.
- If the platform ipv6 acl icmp optimize neighbor-discovery command is configured, the IPv6 RA Guard feature cannot be configured and an error message will be displayed. This command adds default global Internet Control Message Protocol (ICMP) entries that will override the RA guard ICMP entries.

Information About Wireless Multicast

If the network supports packet multicasting, the multicast method that the switch uses can be configured. The switch performs multicasting in two modes:

- Unicast mode—The switch unicasts every multicast packet to every access point associated to the switch. This mode is inefficient, but is required on networks that do not support multicasting.
• Multicast mode—The switch sends multicast packets to a CAPWAP multicast group. This method reduces the overhead on the switch processor and shifts the work of packet replication to the network, which is much more efficient than the unicast method.

When the multicast mode is enabled and the switch receives a multicast packet from the wired LAN, the switch encapsulates the packet using CAPWAP and forwards the packet to the CAPWAP multicast group address. The switch always uses the management VLAN for sending multicast packets. Access points in the multicast group receive the packet and forward it to all the BSSIDs mapped to the VLAN on which clients receive multicast traffic.

The switch supports all the capabilities of IGMP v1, including Multicast Listener Discovery (MLD) v1 snooping, but the IGMP v2 and IGMP v3 capabilities are limited. This feature keeps track of and delivers IPv6 multicast flows to the clients that request them. To support IPv6 multicast, global multicast mode should be enabled.

Internet Group Management Protocol (IGMP) snooping is introduced to better direct multicast packets. When this feature is enabled, the switch snooping gathers IGMP reports from the clients, processes them, creates unique multicast group IDs (MGIDs) based on the Layer 3 multicast address and the VLAN number, and sends the IGMP reports to the IGMP querier. The switch then updates the access-point MGID table on the corresponding access point with the client MAC address. When the switch receives multicast traffic for a particular multicast group, it forwards it to all the access points, but only those access points that have active clients listening or subscribed to that multicast group send multicast traffic on that particular VLAN. IP packets are forwarded with an MGID that is unique for an ingress VLAN and the destination multicast group. Layer 2 multicast packets are forwarded with an MGID that is unique for the ingress VLAN.

MGID is a 14-bit value filled in the 16-bit reserved field of wireless information in the CAPWAP header. The remaining two bits should be set to zero.

**Related Topics**
- Configuring Wireless Multicast-MCMC Mode (CLI), on page 374
- Configuring Wireless Multicast-MCUC Mode (CLI), on page 375

**Multicast Optimization**

Multicast used to be based on the group of the multicast addresses and the VLAN as one entity, MGID. With the VLAN group, duplicate packets might increase. Using the VLAN group feature, every client listens to the multicast stream on a different VLAN. As a result, the switch creates different MGIDs for each multicast address and the VLAN. Therefore, the upstream router sends a copy for each VLAN, which results in as many copies as the number of VLANs in the group. Because the WLAN remains the same for all the clients, multiple copies of the multicast packet are sent over the wireless network. To suppress the duplication of a multicast stream on the wireless medium between the switch and the access points, the multicast optimization feature can be used.

Multicast optimization enables you to create a multicast VLAN that can be used for multicast traffic. One of the VLANs in the switch can be configured as a multicast VLAN where multicast groups are registered. The clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using the multicast VLAN and multicast IP addresses. If multiple clients on different VLANs of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The switch makes sure that all the multicast streams from the clients on this VLAN group always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN group. Only one multicast stream hits the VLAN group even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the network is just one stream.
IPv6 Global Policies

IPv6 global policies provide storage and access policy database services. IPv6 ND inspection and IPv6 RA guard are IPv6 global policies features. Every time an ND inspection or RA guard is configured globally, the policy attributes are stored in the software policy database. The policy is then applied to an interface, and the software policy database entry is updated to include this interface to which the policy is applied.

IPv6 RA Guard

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network device platform. RAs are used by devices to announce themselves on the link. The IPv6 RA Guard feature analyzes these RAs and filters out RAs that are sent by unauthorized devices. In host mode, all RA and router redirect messages are disallowed on the port. The RA guard feature compares configuration information on the Layer 2 (L2) device with the information found in the received RA frame. Once the L2 device has validated the content of the RA frame and router redirect frame against the configuration, it forwards the RA to its unicast or multicast destination. If the RA frame content is not validated, the RA is dropped.

In the wireless deployment RAs coming on wireless ports are dropped as routers cannot reside on these interfaces.

Information About IPv6 Snooping

IPv6 Neighbor Discovery Inspection

The IPv6 Neighbor Discovery Inspection, or IPv6 "snooping," feature bundles several Layer 2 IPv6 first-hop security features, including IPv6 Address Glean and IPv6 Device Tracking. IPv6 neighbor discovery (ND) inspection operates at Layer 2, or between Layer 2 and Layer 3, and provides IPv6 features with security and scalability. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables and analyzes ND messages in order to build a trusted binding table. IPv6 ND messages that do not have valid bindings are dropped. An ND message is considered trustworthy if its IPv6-to-MAC mapping is verifiable. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

When IPv6 ND inspection is configured on a target (which varies depending on platform target support and may include device ports, switch ports, Layer 2 interfaces, Layer 3 interfaces, and VLANs), capture instructions are downloaded to the hardware to redirect the ND protocol and Dynamic Host Configuration Protocol (DHCP) for IPv6 traffic up to the switch integrated security features (SISF) infrastructure in the routing device. For ND traffic, messages such as NS, NA, RA, RS, RA, and REDIRECT are directed to SISF. For DHCP, UDP messages sourced from port 546 or 547 are redirected.

IPv6 ND inspection registers its "capture rules" to the classifier, which aggregates all rules from all features on a given target and installs the corresponding ACL down into the platform-dependent modules. Upon receiving redirected traffic, the classifier calls all entry points from any registered feature (for the target on
which the traffic is being received), including the IPv6 ND inspection entry point. This entry point is the last to be called, so any decision (such as drop) made by another feature supersedes the IPv6 ND inspection decision.

IPv6 ND Inspection

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyses neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery messages that do not have valid bindings are dropped. A neighbor discovery message is considered trustworthy if its IPv6-to-MAC mapping is verifiable.

This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

IPv6 Device Tracking

IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

IPv6 First-Hop Security Binding Table

The IPv6 First-Hop Security Binding Table recovery mechanism feature enables the binding table to recover in the event of a device reboot. A database table of IPv6 neighbors connected to the device is created from information sources such as ND snooping. This database, or binding, table is used by various IPv6 guard features to validate the link-layer address (LLA), the IPv4 or IPv6 address, and prefix binding of the neighbors to prevent spoofing and redirect attacks.

This mechanism enables the binding table to recover in the event of a device reboot. The recovery mechanism will block any data traffic sourced from an unknown source; that is, a source not already specified in the binding table and previously learned through ND or DHCP gleaning. This feature recovers the missing binding table entries when the resolution for a destination address fails in the destination guard. When a failure occurs, a binding table entry is recovered by querying the DHCP server or the destination host, depending on the configuration.

Recovery Protocols and Prefix Lists

The IPv6 First-Hop Security Binding Table Recovery Mechanism feature introduces the capability to provide a prefix list that is matched before the recovery is attempted for both DHCP and NDP.

If an address does not match the prefix list associated with the protocol, then the recovery of the binding table entry will not be attempted with that protocol. The prefix list should correspond to the prefixes that are valid for address assignment in the Layer 2 domain using the protocol. The default is that there is no prefix list, in which case the recovery is attempted for all addresses. The command to associate a prefix list to a protocol is `protocol {dhcp | ndp} [prefix-list prefix-list-name]`.

IPv6 Device Tracking

IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

IPv6 Address Glean

IPv6 address glean is the foundation for many other IPv6 features that depend on an accurate binding table. It inspects ND and DHCP messages on a link to glean addresses, and then populates the binding table with these addresses. This feature also enforces address ownership and limits the number of addresses any given node is allowed to claim.
The following figure shows how IPv6 address glean works.

**Figure 27: IPv6 Address Glean**

---

**How to Configure Wireless Multicast**

**Configuring Wireless Multicast-MCMC Mode (CLI)**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password, if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password, if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> wireless multicast</td>
<td>Enables the multicast traffic for wireless clients and enables mDNS bridging.</td>
</tr>
<tr>
<td>Example:</td>
<td>By default, the feature is in disabled state. Use the no form of this command to disable the multicast traffic for wireless clients and disable mDNS bridging.</td>
</tr>
<tr>
<td>Switch(config)# wireless multicast</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# no wireless multicast</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits configuration mode. Alternatively, press Ctrl-Z to exit configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring IPv6 Snooping (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>Enter your password, if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 mld snooping</td>
<td>Enables MLD snooping.</td>
</tr>
<tr>
<td>Example: Switch(config)# ipv6 mld snooping</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring IPv6 Snooping Policy (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>Enter your password, if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 snooping policy policy-name</td>
<td>Configures an IPv6 snooping policy with a name.</td>
</tr>
<tr>
<td>Example: Switch(config)# ipv6 snooping policy mypolicy</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> security-level guard</td>
<td>Configures the security level to inspect and drop unauthorized messages, if any.</td>
</tr>
<tr>
<td>Example: Switch(config-ipv6-snooping)# security-level guard</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Layer 2 Port as Multicast Router Port (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td>Step 3 ipv6 mld snooping vlan vlan-id mrouter interface Port-channel port-channel-interface-number</td>
<td>Configures a Layer 2 port as a Multicast router port. The VLAN is the client VLAN.</td>
</tr>
</tbody>
</table>

### Configuring IPv6 RA Guard (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 nd raguard policy <em>policy-name</em></td>
<td>Configures a policy for RA guard.</td>
</tr>
<tr>
<td>Example: Switch(config)# ipv6 nd raguard policy myraguardpolicy</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> trusted-port</td>
<td>Sets up a trusted port.</td>
</tr>
<tr>
<td>Example: Switch(config-nd-raguard)# trusted-port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> device-role {host</td>
<td>monitor</td>
</tr>
<tr>
<td>Example: Switch(config-nd-raguard)# device-role router</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring Non-IP Wireless Multicast (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>Enter your password, if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> wireless multicast non-ip</td>
<td>Enables non-IP multicast in all VLANs. By default, the non-IP multicast in all VLANs is in disabled state. Wireless multicast must be enabled for the traffic to pass. Use the no form of this command to disable non-IP multicast in all the VLANs.</td>
</tr>
<tr>
<td>Example: Switch(config)# wireless multicast non-ip</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# no wireless multicast non-ip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> wireless multicast non-ip vlan <em>vlanid</em></td>
<td>Enables non-IP multicast per VLAN. By default, non-IP multicast per VLAN is in disabled state. Both wireless multicast and wireless multicast non-IP must be enabled for</td>
</tr>
<tr>
<td>Example: Switch(config)# wireless multicast non-ip vlan 5</td>
<td></td>
</tr>
</tbody>
</table>
**Configuring Wireless Broadcast (CLI)**

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode. Enters global command mode.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables broadcast packets for wireless clients. By default, the broadcast packets for wireless clients is in disabled state. Enabling <strong>wireless broadcast</strong> enables broadcast traffic for each VLAN. Use the <strong>no</strong> form of this command to disable broadcasting packets.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables broadcast packets for single VLAN. By default, the broadcast packets for single VLAN feature is in disabled state. Wireless broadcast must be enabled for broadcasting. Use the <strong>no</strong> form of this command to disable broadcast traffic for each VLAN.</td>
</tr>
<tr>
<td>wireless broadcast</td>
<td>Enables broadcast packets for wireless clients. By default, the broadcast packets for wireless clients is in disabled state. Enabling <strong>wireless broadcast</strong> enables broadcast traffic for each VLAN. Use the <strong>no</strong> form of this command to disable broadcasting packets.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# wireless broadcast</td>
</tr>
<tr>
<td>Switch(config)# no wireless broadcast</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables broadcast packets for single VLAN. By default, the broadcast packets for single VLAN feature is in disabled state. Wireless broadcast must be enabled for broadcasting. Use the <strong>no</strong> form of this command to disable broadcast traffic for each VLAN.</td>
</tr>
<tr>
<td>wireless broadcast vlan vlanid</td>
<td>Enables broadcast packets for wireless clients. By default, the broadcast packets for wireless clients is in disabled state. Enabling <strong>wireless broadcast</strong> enables broadcast traffic for each VLAN. Use the <strong>no</strong> form of this command to disable broadcasting packets.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# wireless broadcast vlan 3</td>
</tr>
<tr>
<td>Switch(config)# no wireless broadcast vlan 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Exits configuration mode. Alternatively, press <strong>Ctrl-Z</strong> to exit configuration mode.</td>
</tr>
<tr>
<td>end</td>
<td>Exits configuration mode. Alternatively, press <strong>Ctrl-Z</strong> to exit configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
</tr>
</tbody>
</table>
# Configuring IP Multicast VLAN for WLAN (CLI)

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>wlan wlan_name</code></td>
<td>Enters configuration mode to configure various parameters in the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# wlan test1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>shutdown</code></td>
<td>Disables WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-wlan)# shutdown</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>ip multicast vlan {vlan_name vlan_id}</code></td>
<td>Configures multicast VLAN for WLAN. Use the <code>no</code> form of this command to disable the multicast VLAN for WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-wlan)# ip multicast vlan 5</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-wlan)# no ip multicast vlan 5</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>no shutdown</code></td>
<td>Enables the disabled WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-wlan)# no shutdown</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>end</code></td>
<td>Exits configuration mode. Alternatively, press Ctrl-Z to exit configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

## Related Topics
- Multicast Optimization, on page 371
Monitoring Wireless Multicast

Table 21: Commands for Monitoring Wireless Multicast

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless multicast</td>
<td>Displays the multicast status and IP multicast mode, and each VLAN's broadcast and non-IP multicast status. Also displays the mDNS bridging state.</td>
</tr>
<tr>
<td>show wireless multicast group summary</td>
<td>Displays all (Group and VLAN) lists and the corresponding MGID values.</td>
</tr>
<tr>
<td>show wireless multicast [source source] group group vlan vlanid</td>
<td>Displays details of the specified (S,G,V) and shows all the clients associated with and their MC2UC status.</td>
</tr>
<tr>
<td>show ip igmp snooping wireless mcast-spi-count</td>
<td>Displays statistics of the number of multicast SPIs per MGID sent between IOS and the Wireless Controller Module. Displays statistics of the number of multicast SPIs per MGID sent internally between IOS and the Wireless Controller Module.</td>
</tr>
<tr>
<td>show ip igmp snooping wireless mgid</td>
<td>Displays the MGID mappings.</td>
</tr>
<tr>
<td>show ip igmp snooping igmpv2-tracking</td>
<td>Displays the client-to-SGV mappings and the SGV-to-client mappings.</td>
</tr>
<tr>
<td>show ip igmp snooping querier vlan vlanid</td>
<td>Displays the IGMP querier information for the specified VLAN.</td>
</tr>
<tr>
<td>show ip igmp snooping querier detail</td>
<td>Displays the detailed IGMP querier information of all the VLANs.</td>
</tr>
<tr>
<td>show ipv6 mld snooping querier vlan vlanid</td>
<td>Displays the MLD querier information for the specified VLAN.</td>
</tr>
<tr>
<td>show ipv6 mld snooping wireless mgid</td>
<td>Displays MGIDs for the IPv6 multicast group.</td>
</tr>
</tbody>
</table>

Where to Go Next for Wireless Multicast

You can configure the following:

- IGMP
- Service Discovery Gateway
Where to Go Next for Wireless Multicast
CHAPTER 30

Configuring the Service Discovery Gateway

- Finding Feature Information, on page 383
- Restrictions for Configuring the Service Discovery Gateway, on page 383
- Information about the Service Discovery Gateway and mDNS, on page 384
- How to Configure the Service Discovery Gateway, on page 387
- Monitoring Service Discovery Gateway, on page 394
- Configuration Examples, on page 395
- Monitoring Service Cache (GUI), on page 397
- Monitoring Static Service Cache (GUI), on page 398
- Where to Go Next for Configuring Services Discovery Gateway, on page 398
- Additional References, on page 399
- Feature History and Information for Services Discovery Gateway, on page 400

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring the Service Discovery Gateway

The following are restrictions for configuring the Service Discovery Gateway:

- The Service Discovery Gateway does not support topologies with multiple hops. All network segments must be connected directly to it. The Service Discovery Gateway can learn services from all connected segments to build its cache and respond to requests acting as a proxy.

- The use of third-party mDNS servers or applications are not supported with this feature.

- On a Cat4500sup8e MC (3.7 ) running mDNS, iphone and ipads running iOS7.0 might have problems in accessing print services through mDNS.
Information about the Service Discovery Gateway and mDNS

mDNS

mDNS was defined to achieve zero configuration, with zero configuration being defined as providing the following features:

• Addressing—Allocating IP addresses to hosts
• Naming—Using names to refer to hosts instead of IP addresses
• Service discovery—Finding services automatically on the network

With mDNS, network users no longer have to assign IP addresses, assign host names, or type in names to access services on the network. Users only need to ask to see what network services are available, and choose from a list.

With mDNS, addressing is accomplished through the use of DHCP/DHCPv6 or IPv4 and IPv6 Link Local scoped addresses. The benefit of zero-configuration occurs when no infrastructure services such as DHCP or DNS are present and self-assigned link-local addressing can be used. The client can then select a random IPv4 address in the link-local range (169.254.0.0/24) or use its IPv6 link-local address (FE80::/10) for communication.

With mDNS, naming (name-to-address translation on a local network using mDNS) queries are sent over the local network using link-local scoped IP multicast. Because these DNS queries are sent to a multicast address (IPv4 address 224.0.0.251 or IPv6 address FF02::FB), no single DNS server with global knowledge is required to answer the queries. When a service or device sees a query for any service it is aware of, it provides a DNS response with the information from its cache.

With mDNS, service discovery is accomplished by browsing. An mDNS query is sent out for a given service type and domain, and any device that is aware of matching services replies with service information. The result is a list of available services for the user to choose from.

The mDNS protocol (mDNS-RFC), together with DNS Service Discovery (DNS-SD-RFC) achieves the zero-configuration addressing, naming, and service discovery.

mDNS-SD

Multicast DNS Service Discovery (mDNS-SD) uses DNS protocol semantics and multicast over well-known multicast addresses to achieve zero configuration service discovery. DNS packets are sent to and received on port 5353 using a multicast address of 224.0.0.251 and its IPv6 equivalent FF02::FB.

Because mDNS uses a link-local multicast address, its scope is limited to a single physical or logical LAN. If the networking reach needs to be extended to a distributed campus or to a wide-area environment consisting of many different networking technologies, mDNS gateway is implemented. An mDNS gateway provides a transport for mDNS packets across Layer 3 boundaries by filtering, caching, and redistributing services from one Layer 3 domain to another.

mDNS-SD Considerations for Wireless Clients

• mDNS packets can be sent out of Layer 3 interfaces that might not have an IP address.
• Packets with mDNS multicast IP and multicast MAC are sent on a multicast CAPWAP tunnel, if multicast-multicast mode is enabled. A multicast CAPWAP tunnel is a special CAPWAP tunnel used
for reducing the number of copies of multicast packet that are required to be generated for each AP CAPWAP tunnel. Sending packets on the multicast CAPWAP tunnel requires the outer IP header to be destined to the multicast CAPWAP tunnel's address, which all APs are subscribed to.

- All mDNS packet handling is done at a foreign switch for roamed clients. A foreign switch is the new switch that a roamed wireless client is actually attached to, which is called the point of attachment.

**Service Discovery Gateway**

The Service Discovery Gateway feature enables multicast Domain Name System (mDNS) to operate across Layer 3 boundaries (different subnets). An mDNS gateway provides transport for service discovery across Layer 3 boundaries by filtering, caching, and redistributing services from one Layer 3 domain (subnet) to another. Prior to implementation of this feature, mDNS was limited in scope to within a subnet because of the use of link-local scoped multicast addresses. This feature enhances Bring Your Own Device (BYOD).

**Related Topics**

- Configuring the Service List (CLI), on page 387
- Example: Creating a Service-List, Applying a Filter and Configuring Parameters, on page 396
- Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
- Example: Specify Alternative Source Interface for Outgoing mDNS Packets, on page 395
- Example: Redistribute Service Announcements, on page 395
- Example: Disable Bridging of mDNS Packets to Wireless Clients, on page 395
- Example: Enabling mDNS Gateway and Redistributing Services, on page 396
- Example: Global mDNS Configuration, on page 396
- Example: Interface mDNS Configuration, on page 397

**mDNS Gateway and Subnets**

You need to enable an mDNS gateway for service discovery to operate across subnets. You can enable mDNS gateway for a device or for an interface.

---

**Note**

You need to configure service routing globally before configuring at the interface level.

After the device or interface is enabled, you can redistribute service discovery information across subnets. You can create service policies and apply filters on either incoming service discovery information (called IN-bound filtering) or outgoing service discovery information (called OUT-bound filtering).

---

**Note**

If redistribution is enabled globally, global configuration is given higher priority than interface configuration.

**Figure 28: Sample Networking Scenario**

For example, if the mDNS gateway functionality is enabled on the router in this figure, then service information can be sent from one subnet to another and vice-versa. For example, the printer and fax service information being advertised in the network with IP address 192.0.2.6 are redistributed to the network with IP address 198.51.100.4. The printer and fax service information in the network with IP address 192.0.2.6 is learned by
Filtering

After configuring the mDNS gateway and subnets, you can filter services that you want to redistribute. While creating a service list, the permit or deny command options are used:

- The permit command option allows you to permit or transport specific service list information.
- The deny option allows you to deny service list information that is available to be transported to other subnets.

You need to include a sequence number when using the permit or deny command option. The same service list name can be associated with multiple sequence numbers and each sequence number will be mapped to a rule.

---

**Note**

If no filters are configured, then the default action is to deny service list information to be transported through the device or interface.

Query is another option provided when creating service lists. You can create queries using a service list. If you want to browse for a service, then active queries can be used. This function is helpful to keep the records refreshed in the cache.

---

**Note**

Active queries can only be used globally and cannot be used at the interface level.

A service end-point (such as a printer or fax) sends unsolicited announcements when a service starts up. After that, it sends unsolicited announcements whenever a network change event occurs (such as an interface coming up or going down). The device always respond to queries.
After creating a service list and using the **permit** or **deny** command options, you can filter using match statements (commands) based on **service-instance**, **service-type**, or **message-type** (announcement or query).

**Related Topics**
- Configuring the Service List (CLI), on page 387
- Example: Creating a Service-List, Applying a Filter and Configuring Parameters, on page 396
- Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
- Example: Specify Alternative Source Interface for Outgoing mDNS Packets, on page 395
- Example: Redistribute Service Announcements, on page 395
- Example: Disable Bridging of mDNS Packets to Wireless Clients, on page 395
- Example: Enabling mDNS Gateway and Redistributing Services, on page 396
- Example: Global mDNS Configuration, on page 396
- Example: Interface mDNS Configuration, on page 397

## How to Configure the Service Discovery Gateway

### Configuring the Service List (CLI)

This procedure describes how to create a service list, apply a filter for the service list, and configure parameters for the service list name.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>service-list mdns-sd service-list-name {deny sequence-number</td>
<td>Enters mDNS service discovery service list mode. In this mode, you can:</td>
</tr>
<tr>
<td>permit sequence-number</td>
<td>query}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# service-list mdns-sd sl1 permit 3</td>
<td>• Create a service list and associate a query for the service list name if the query option is used.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>query</td>
<td>Note</td>
</tr>
</tbody>
</table>

The sequence number sets the priority of the rule. A rule with a lower sequence number is selected first and the service announcement or query is allowed or denied accordingly. You define the sequence number as per your network requirements.

**Step 4**

**match message-type** {announcement | any | query}

**Example:**

Switch(config-mdns-sd-sl)# match message-type announcement

(Optional) Sets the message type to match. You can match the following message types:

- announcement
- any
- query

These commands configure the parameters for the service list name that is created in step 2.

If the `match message-type` is an announcement, then the service list rule only allows service advertisements or announcements for the device. If the `match message-type` is a query, then only a query from the client for a certain service in the network is allowed.

Multiple service maps of the same name with different sequence numbers can be created and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, each one has a permit or deny result. Evaluation of service list consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and an action permit/deny associated with the statement match is performed. The default action after scanning through the entire list is to deny.

**Note** You cannot use the `match` command if you have used the `query` option in the previous step. The `match` command can be used only for the `permit` or `deny` option.

**Step 5**

**match service-instance** {LINE}

**Example:**

(Optional) Sets the service instance to match.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-mdns-sd-sl)# match service-instance servInst 1</td>
<td>This command configures the parameters for the service list name that is created in step 2.</td>
</tr>
</tbody>
</table>

**Note** You cannot use the `match` command if you have used the `query` option in the previous step. The `match` command can be used only for the `permit` or `deny` option.

**Step 6**
match service-type \{LINE \}
Example:
Switch(config-mdns-sd-sl)# match service-type _ipp._tcp

(Optional) Sets the value of the mDNS service type string to match.

This command configures the parameters for the service list name that is created in step 2.

**Note** You cannot use the `match` command if you have used the `query` option in the previous step. The `match` command can be used only for the `permit` or `deny` option.

**Step 7**
end
Example:
Switch(config-mdns-sd-sl)# end

Returns to privileged EXEC mode.

What to do next
Proceed to enable the mDNS gateway and redistribution of services.

Related Topics
- Service Discovery Gateway, on page 385
- Filtering, on page 386
- Example: Creating a Service-List, Applying a Filter and Configuring Parameters, on page 396

### Configuring the Service List (GUI)

**Procedure**

**Step 1**  Choose Configuration > Controller > mDNS > Static Service.

**Step 2**  Click Create Service.
The Service List > Create Service page is displayed.

**Step 3**  In the Service List Name text box, enter the service list name.

**Step 4**  From the Service rule drop-down list, choose from the following options:
- `permit`—permits the service list.
• deny—denies the service list.

Step 5
In the Sequence number text box, enter the priority of the rule. A rule with a lower sequence number is selected first and the service announcement or query is allowed or denied accordingly. You define the sequence number as per your network requirements.

Step 6
From the Message type drop-down list, choose the message type to match from the following options:

• announcement—The service list rule allows only service advertisements or announcements for the device.
• query—The service list rule allows only a query from the client for a service in the network.
• any—The service list rule allows any type of message.

Multiple service maps of the same name with different sequence numbers can be created and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, each one has a permit or deny result. Evaluation of service list consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and an action permit/deny associated with the statement match is performed. The default action after scanning through the entire list is to deny.

Step 7
In the Service instance text box, enter the service instance to match.

Step 8
In the Custom text box, enter the mDNS service type string to match.

The Learned Service box shows the services that are added after enabling the learned service type configured by navigating to Configuration > Controller > mDNS > Global. For example, _roap._tcp.local.

The Selected Service box shows the learned service that you have selected for an mDNS service.

Step 9
Click Apply.

Step 10
Click Save Configuration.

What to do next
Proceed to enable the mDNS gateway and redistribution of services.

Enabling mDNS Gateway and Redistributing Services (CLI)

After enabling mDNS gateway for a device, you can apply filters (apply IN-bound filtering or OUT-bound filtering) and active queries by using service-policy and service-policy-query commands, respectively. You can redistribute services and service announcements using the redistribute mdns-sd command, and set some part of the system memory for cache using the cache-memory-max command.

Note
By default, mDNS gateway is disabled on all interfaces.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>Enter your password, if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> service-routing mdns-sd</td>
<td>Enables mDNS gateway functionality for a device and enters multicast DNS configuration (config-mdns) mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch (config)# service-routing mdns-sd</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This command enables the mDNS function globally.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Enter the service-routing mdns-sd source-interface if-name command in either global-config or interface-config mode, to specify an alternate source interface for outgoing mDNS packets, so its IP address can be used when there is none configured on the outgoing interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service-policy service-policy-name {IN</td>
<td>OUT}</td>
<td>(Optional) For a service list, applies a filter on incoming service discovery information (IN-bound filtering) or outgoing service discovery information (OUT-bound filtering).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch (config-mdns)# service-policy serv-poll IN</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> redistribute mdns-sd</td>
<td>(Optional) Redistributes services or service announcements across subnets.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch (config-mdns)# redistribute mdns-sd</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If redistribution is enabled globally, global configuration is given higher priority than interface configuration.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> cache-memory-max cache-config-percentage</td>
<td>(Optional) Sets some part of the system memory (in percentage) for cache.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch (config-mdns)# cache-memory-max 20</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>By default, 10 percent of the system memory is set aside for cache. You can override the default value by using this command.</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 7</td>
<td>service-policy-query service-list-query-name service-list-query-periodicity</td>
<td>(Optional) Configures service list-query periodicity.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-mdns)# service-policy-query sl-query1 100</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>exit</td>
<td>(Optional) Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-mdns)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>wireless multicast</td>
<td>(Optional) Enables wireless Ethernet multicast support.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config)# wireless multicast</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>no wireless mdns-bridging</td>
<td>(Optional) Disables bridging of mDNS packets to wireless clients.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config)# no wireless mdns-bridging</td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- [Service Discovery Gateway](#), on page 385
- [Filtering](#), on page 386
- [Example: Specify Alternative Source Interface for Outgoing mDNS Packets](#), on page 395
- [Example: Redistribute Service Announcements](#), on page 395
- [Example: Disable Bridging of mDNS Packets to Wireless Clients](#), on page 395
- [Example: Enabling mDNS Gateway and Redistributing Services](#), on page 396
- [Example: Global mDNS Configuration](#), on page 396
- [Example: Interface mDNS Configuration](#), on page 397
Configuring Interface Service Rules (GUI)

Procedure

Step 1  Choose Configuration > Controller > mDNS > Interface.
Step 2  Click an interface name.
The Interface Service Rules page is displayed.
Step 3  From the Service Policy IN drop-down list, choose the service policy that should be applied for incoming mDNS messages.
Step 4  From the Service Policy OUT drop-down list, choose the service policy that should be applied for outgoing mDNS messages.
Step 5  Select or unselect the Redistribution check box to enable or disable redistribution of service announcements received on one interface over all the interfaces or over a specific interface.
Step 6  Check Enable to enable a self designated gateway for the interface.
Step 7  Enter values for proximity- maximum service option and service list active query in the text box. The value ranges from 1 to 100 for maximum service.
Step 8  To create a new Service Type, select Create New from the drop-down box.
Step 9  Click Apply.
Step 10 Click Save Configuration.

Configuring mDNS Global Rules (GUI)

Procedure

Step 1  Choose Configuration > Controller > mDNS > Global.
Step 2  Select the mDNS gateway check box.
Step 3  Follow these steps to configure downstream rules that include service lists and service rules that you can apply for all the downstream traffic on the switch.
   a)  Click the Down Stream Rules tab.
   b)  From the Service List Name drop-down list, choose Create New. In the Service List Name box, enter a name.
   c)  Click Add to add a service rule, and follow on-screen instructions to specify the service rules that include Action, Message Type, Service Instance, and Service Type.
       See the online help for detailed descriptions of the fields.
Step 4  Follow these steps to configure the upstream rules that include service lists and service rules that you can apply for all the upstream traffic on the switch.
   a)  Click the Up Stream Rules tab.
   b)  From the Service List Name drop-down list, choose Create New. In the New Service List Name box, enter a name.
c) Click Add to add a service rule, and follow on-screen instructions to specify the service rules that include Action, Message Type, Service Instance, and Service Type.

   See the online help for detailed descriptions of the fields.

**Step 5**

Follow these steps to configure the switch as designated gateway and apply proximity rules:

a) Click the Advanced tab.

b) Select or unselect the Self Designated Gateway check box.

c) Under Proximity, in the Max Services Option box, enter the maximum number of devices supported with a particular service type that are in proximity. The valid range is between 1 and 100.

d) From the Service List Active Query drop-down list, choose the services that are filtered for proximity.
   You can create a custom service list, by choosing Create New and then specifying the service list name.

e) Click New to add a service type, and from the Service Type drop-down list, choose the service type to be added, and click OK.
   See the online help for detailed descriptions of the fields.

**Step 6**

From the Learn Service drop-down list, choose from the following options:

- **Enable** — Allows the switch to learn all the announced services. It is used to learn services by enabling all announcement/queries by using Service Policy IN of type GUI-permit-all and in Service Policy OUT of type GUI-deny-all.
- **Disable** — Denies all the traffics IN and OUT. It is used to deny services by disabling all announcement/queries by using Service Policy IN of type GUI-deny-all and in Service Policy OUT of type GUI-deny-all.
- **Custom** — You can set your own IN and OUT policy. It allows you to define a custom service list.

**Step 7**

Click Apply.

**Step 8**

Click Save Configuration.

---

### Monitoring Service Discovery Gateway

#### Table 22: Monitoring Service Discovery Gateway

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mdns requests [detail</td>
<td>name record-name</td>
</tr>
<tr>
<td>show mdns cache [interface type number</td>
<td>name record-name [type record-type]] type record-type</td>
</tr>
<tr>
<td>show mdns statistics {all</td>
<td>service-list list-name</td>
</tr>
</tbody>
</table>
### Configuration Examples

#### Example: Specify Alternative Source Interface for Outgoing mDNS Packets

The following example displays how to specify an alternate source interface for outgoing mDNS packets, so its IP address can be used when there is none configured on the outgoing interface.

```
Switch(config)# service-routing mdns-sd
Switch(config-mdns)# source-interface if-name
```

**Related Topics**
- Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
- Service Discovery Gateway, on page 385
- Filtering, on page 386

#### Example: Redistribute Service Announcements

The following example displays how to redistribute service announcements received on one interface over all the interfaces or over a specific interface.

```
Switch(config)# service-routing mdns-sd
Switch(config-mdns)# Redistribute mdns-sd if-name
```

**Related Topics**
- Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
- Service Discovery Gateway, on page 385
- Filtering, on page 386

#### Example: Disable Bridging of mDNS Packets to Wireless Clients

The following example displays how to disable bridging of mDNS packets to wireless clients.

```
Switch(config)# wireless multicast
Switch(config)# no wireless mdns-bridging
```

**Related Topics**
- Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
- Service Discovery Gateway, on page 385
- Filtering, on page 386
Example: Creating a Service-List, Applying a Filter and Configuring Parameters

The following example shows the creation of a service-list `sl1`. The `permit` command option is being applied on sequence number 3 and all services with message-type announcement are filtered and available for transport across various subnets associated with the device.

```
Switch# configure terminal
Switch(config)# service-list mdns-sd sl1 permit 3
Switch(config-mdns-sd-sl1)# match message-type announcement
Switch(config-mdns-sd-sl1)# exit
```

Related Topics
- Configuring the Service List (CLI), on page 387
- Service Discovery Gateway, on page 385
- Filtering, on page 386

Example: Enabling mDNS Gateway and Redistributing Services

The following example shows how to enable an mDNS gateway for a device and enable redistribution of services across subnets. IN-bound filtering is applied on the service-list `serv-pol1`. Twenty percent of system memory is made available for cache and service-list-query periodicity is configured at 100 seconds.

```
Switch# configure terminal
Switch# service-routing mdns-sd
Switch(config-mdns)## service-policy serv-pol1 IN
Switch(config-mdns)## redistribute mdns-sd
Switch(config-mdns)## cache-memory-max 20
Switch(config-mdns)## service-policy-query sl-query1 100
Switch(config-mdns)## exit
```

Related Topics
- Enabling mDNS Gateway and Redistributing Services (CLI), on page 390
- Service Discovery Gateway, on page 385
- Filtering, on page 386

Example: Global mDNS Configuration

The following example displays how to globally configure mDNS.

```
Switch# configure terminal
Switch(config)# service-list mdns-sd mypermit-all permit 10
Switch(config-mdns-sd-sl1)# exit
Switch(config)# service-list mdns-sd querier query
Switch(config-mdns-sd-sl1)# service-type _dns._udp
Switch(config-mdns-sd-sl1)# end
Switch# configure terminal
Switch(config)# service-routing mdns-sd
Switch(config-mdns)# service-policy mypermit-all IN
Switch(config-mdns)# service-policy mypermit-all OUT
```
Example: Interface mDNS Configuration

The following example displays how to configure mDNS for an interface.

Switch(config)#interface Vlan136
Switch(config-if)#  description *** Mgmt VLAN ***
Switch(config-if)#  ip address 9.7.136.10 255.255.255.0
Switch(config-if)#  ip helper-address 9.1.0.100
Switch(config-if)#  service-routing mdns-sd
Switch(config-if-mdns-sd)#  service-policy mypermit-all IN
Switch(config-if-mdns-sd)#  service-policy mypermit-all OUT
Switch(config-if-mdns-sd)#  service-policy-query querier 60

Monitoring Service Cache (GUI)

Click Monitor > Controller > mDNS > Service Cache to view domain names and other details of the service providers.

Each service advertisement contains a record that maps the domain name of the service provider to the IP address. The details of the following parameters is displayed:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the hostname assigned to each service provider machine.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Displays the VLAN ID of the service provider.</td>
</tr>
<tr>
<td>MAC ID</td>
<td>Displays the MAC address of the service provider machine.</td>
</tr>
<tr>
<td>TTL</td>
<td>Displays the Time to Live (TTL) value in seconds that determines the validity of the service offered by the service provider. The service provider is removed from the Switch when the TTL expires.</td>
</tr>
<tr>
<td>Remaining</td>
<td>Displays the time left in seconds before the service provider is removed from the Switch.</td>
</tr>
</tbody>
</table>
Type | Displays the service type record. Values are as follow:
- PTR
- TXT
- SRV

RR Record Data | Displays IP addresses, service names of the announced services.

---

### Monitoring Static Service Cache (GUI)

Click Monitor > Controller > mDNS > Static Service Cache to view domain names and other details of the service providers.

Each service advertisement contains a record that maps the domain name of the service provider to the IP address. The details of the following parameters is displayed:

| Name | Displays the hostname assigned to each service provider machine.
| VLAN ID | Displays the VLAN ID of the service provider.
| MAC ID | Displays the MAC address of the service provider machine.
| TTL | Displays the Time to Live (TTL) value in seconds that determines the validity of the service offered by the service provider. The service provider is removed from the Switch when the TTL expires.
| Remaining | Displays the time left in seconds before the service provider is removed from the Switch.
| Type | Displays the service type record. Values are as follow:
- PTR
- TXT
- SRV
| RR Record Data | Displays IP addresses, service names of the announced services.

---

### Where to Go Next for Configuring Services Discovery Gateway

You can configure the following:

- IGMP
- Wireless Multicast
Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring DNS</td>
<td><em>IP Addressing: DNS Configuration Guide, Cisco IOS XE Release 3SE</em></td>
</tr>
<tr>
<td>DNS conceptual information</td>
<td>'Information About DNS' section in <em>IP Addressing: DNS Configuration Guide, Cisco IOS XE Release 3SE</em></td>
</tr>
<tr>
<td>Platform-independent configuration information</td>
<td><em>IP Addressing: DNS Configuration Guide, Cisco IOS XE Release 3SE</em></td>
</tr>
</tbody>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 6763</td>
<td>DNS-Based Service Discovery</td>
</tr>
<tr>
<td>Multicast DNS Internet-Draft</td>
<td>Multicast</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information for Services Discovery Gateway

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
PART VIII

Network Management

• Configuring Cisco IOS Configuration Engine, on page 403
• Configuring the Cisco Discovery Protocol, on page 423
• Configuring Simple Network Management Protocol, on page 433
• Configuring Service Level Agreements, on page 461
• Configuring Local Policies, on page 485
• Configuring SPAN and RSPAN, on page 501
• Configuring Wireshark, on page 541
CHAPTER 31

Configuring Cisco IOS Configuration Engine

• Prerequisites for Configuring the Configuration Engine, on page 403
• Restrictions for Configuring the Configuration Engine, on page 403
• Information About Configuring the Configuration Engine, on page 404
• How to Configure the Configuration Engine, on page 409
• Monitoring CNS Configurations, on page 420
• Additional References, on page 421
• Feature History and Information for the Configuration Engine, on page 422

Prerequisites for Configuring the Configuration Engine

• Obtain the name of the configuration engine instance to which you are connecting.

• Because the CNS uses both the event bus and the configuration server to provide configurations to devices, you must define both ConfigID and Device ID for each configured switch.

• All switches configured with the cns config partial global configuration command must access the event bus. The DeviceID, as originated on the switch, must match the DeviceID of the corresponding switch definition in the Cisco Configuration Engine. You must know the hostname of the event bus to which you are connecting.

Restrictions for Configuring the Configuration Engine

• Within the scope of a single instance of the configuration server, no two configured switches can share the same value for ConfigID.

• Within the scope of a single instance of the event bus, no two configured switches can share the same value for DeviceID.
Information About Configuring the Configuration Engine

Cisco Configuration Engine Software

The Cisco Configuration Engine is network management utility software that acts as a configuration service for automating the deployment and management of network devices and services. Each Cisco Configuration Engine manages a group of Cisco devices (switches and routers) and the services that they deliver, storing their configurations and delivering them as needed. The Cisco Configuration Engine automates initial configurations and configuration updates by generating device-specific configuration changes, sending them to the device, executing the configuration change, and logging the results.

The Cisco Configuration Engine supports standalone and server modes and has these Cisco Networking Services (CNS) components:

- Configuration service:
  - Web server
  - File manager
  - Namespace mapping server

- Event service (event gateway)

- Data service directory (data models and schema)

---

**Note**

Support for Cisco Configuration Engine will be deprecated in future releases. Use the configuration described in Cisco Plug and Play Feature Guide.

In standalone mode, the Cisco Configuration Engine supports an embedded directory service. In this mode, no external directory or other data store is required. In server mode, the Cisco Configuration Engine supports the use of a user-defined external directory.
Configuration Service

The Configuration Service is the core component of the Cisco Configuration Engine. It consists of a Configuration Server that works with Cisco IOS CNS agents on the switch. The Configuration Service delivers device and service configurations to the switch for initial configuration and mass reconfiguration by logical groups. Switches receive their initial configuration from the Configuration Service when they start up on the network for the first time.

The Configuration Service uses the CNS Event Service to send and receive configuration change events and to send success and failure notifications.

The Configuration Server is a web server that uses configuration templates and the device-specific configuration information stored in the embedded (standalone mode) or remote (server mode) directory.

Configuration templates are text files containing static configuration information in the form of CLI commands. In the templates, variables are specified by using Lightweight Directory Access Protocol (LDAP) URLs that reference the device-specific configuration information stored in a directory.

The Cisco IOS agent can perform a syntax check on received configuration files and publish events to show the success or failure of the syntax check. The configuration agent can either apply configurations immediately or delay the application until receipt of a synchronization event from the configuration server.

Event Service

The Cisco Configuration Engine uses the Event Service for receipt and generation of configuration events. The Event Service consists of an event agent and an event gateway. The event agent is on the switch and facilitates the communication between the switch and the event gateway on the Cisco Configuration Engine.

The Event Service is a highly capable publish-and-subscribe communication method. The Event Service uses subject-based addressing to send messages to their destinations. Subject-based addressing conventions define a simple, uniform namespace for messages and their destinations.
NameSpace Mapper

The Cisco Configuration Engine includes the NameSpace Mapper (NSM) that provides a lookup service for managing logical groups of devices based on application, device or group ID, and event.

Cisco IOS devices recognize only event subject-names that match those configured in Cisco IOS software; for example, cisco.cns.config.load. You can use the namespace mapping service to designate events by using any desired naming convention. When you have populated your data store with your subject names, NSM changes your event subject-name strings to those known by Cisco IOS.

For a subscriber, when given a unique device ID and event, the namespace mapping service returns a set of events to which to subscribe. Similarly, for a publisher, when given a unique group ID, device ID, and event, the mapping service returns a set of events on which to publish.

Cisco Networking Services IDs and Device Hostnames

The Cisco Configuration Engine assumes that a unique identifier is associated with each configured switch. This unique identifier can take on multiple synonyms, where each synonym is unique within a particular namespace. The event service uses namespace content for subject-based addressing of messages.

The Cisco Configuration Engine intersects two namespaces, one for the event bus and the other for the configuration server. Within the scope of the configuration server namespace, the term ConfigID is the unique identifier for a device. Within the scope of the event bus namespace, the term DeviceID is the CNS unique identifier for a device.

ConfigID

Each configured switch has a unique ConfigID, which serves as the key into the Cisco Configuration Engine directory for the corresponding set of switch CLI attributes. The ConfigID defined on the switch must match the ConfigID for the corresponding switch definition on the Cisco Configuration Engine.

The ConfigID is fixed at startup time and cannot be changed until the device restarts, even if the switch hostname is reconfigured.

DeviceID

Each configured switch participating on the event bus has a unique DeviceID, which is analogous to the switch source address so that the switch can be targeted as a specific destination on the bus.

The origin of the DeviceID is defined by the Cisco IOS hostname of the switch. However, the DeviceID variable and its usage reside within the event gateway adjacent to the switch.

The logical Cisco IOS termination point on the event bus is embedded in the event gateway, which in turn functions as a proxy on behalf of the switch. The event gateway represents the switch and its corresponding DeviceID to the event bus.

The switch declares its hostname to the event gateway immediately after the successful connection to the event gateway. The event gateway couples the DeviceID value to the Cisco IOS hostname each time this connection is established. The event gateway retains this DeviceID value for the duration of its connection to the switch.
Hostname and DeviceID

The DeviceID is fixed at the time of the connection to the event gateway and does not change even when the switch hostname is reconfigured.

When changing the switch hostname on the switch, the only way to refresh the DeviceID is to break the connection between the switch and the event gateway. For instructions on refreshing DeviceIDs, see "Related Topics."

When the connection is reestablished, the switch sends its modified hostname to the event gateway. The event gateway redefines the DeviceID to the new value.

---

**Caution**

When using the Cisco Configuration Engine user interface, you must first set the DeviceID field to the hostname value that the switch acquires *after*, not *before*, and you must reinitialize the configuration for your Cisco IOS CNS agent. Otherwise, subsequent partial configuration command operations may malfunction.

Hostname, DeviceID, and ConfigID

In standalone mode, when a hostname value is set for a switch, the configuration server uses the hostname as the DeviceID when an event is sent on hostname. If the hostname has not been set, the event is sent on the cn=<value> of the device.

In server mode, the hostname is not used. In this mode, the unique DeviceID attribute is always used for sending an event on the bus. If this attribute is not set, you cannot update the switch.

These and other associated attributes (tag value pairs) are set when you run **Setup** on the Cisco Configuration Engine.

Cisco IOS CNS Agents

The CNS event agent feature allows the switch to publish and subscribe to events on the event bus and works with the Cisco IOS CNS agent. These agents, embedded in the switch Cisco IOS software, allow the switch to be connected and automatically configured.

Initial Configuration

When the switch first comes up, it attempts to get an IP address by broadcasting a Dynamic Host Configuration Protocol (DHCP) request on the network. Assuming there is no DHCP server on the subnet, the distribution switch acts as a DHCP relay agent and forwards the request to the DHCP server. Upon receiving the request, the DHCP server assigns an IP address to the new switch and includes the Trivial File Transfer Protocol (TFTP) server Internet Protocol (IP) address, the path to the bootstrap configuration file, and the default gateway IP address in a unicast reply to the DHCP relay agent. The DHCP relay agent forwards the reply to the switch.

The switch automatically configures the assigned IP address on interface VLAN 1 (the default) and downloads the bootstrap configuration file from the TFTP server. Upon successful download of the bootstrap configuration file, the switch loads the file in its running configuration.

The Cisco IOS CNS agents initiate communication with the Configuration Engine by using the appropriate ConfigID and EventID. The Configuration Engine maps the Config ID to a template and downloads the full configuration file to the switch.
The following figure shows a sample network configuration for retrieving the initial bootstrap configuration file by using DHCP-based autoconfiguration.

**Figure 30: Initial Configuration**

---

**Incremental (Partial) Configuration**

After the network is running, new services can be added by using the Cisco IOS CNS agent. Incremental (partial) configurations can be sent to the switch. The actual configuration can be sent as an event payload by way of the event gateway (push operation) or as a signal event that triggers the switch to initiate a pull operation.

The switch can check the syntax of the configuration before applying it. If the syntax is correct, the switch applies the incremental configuration and publishes an event that signals success to the configuration server. If the switch does not apply the incremental configuration, it publishes an event showing an error status. When the switch has applied the incremental configuration, it can write it to nonvolatile random-access memory (NVRAM) or wait until signaled to do so.

**Synchronized Configuration**

When the switch receives a configuration, it can defer application of the configuration upon receipt of a write-signal event. The write-signal event tells the switch not to save the updated configuration into its NVRAM. The switch uses the updated configuration as its running configuration. This ensures that the switch configuration is synchronized with other network activities before saving the configuration in NVRAM for use at the next reboot.

**Automated CNS Configuration**

To enable automated CNS configuration of the switch, you must first complete the prerequisites listed in this topic. When you complete them, power on the switch. At the `setup` prompt, do nothing; the switch begins the initial configuration. When the full configuration file is loaded on your switch, you do not need to do anything else.

For more information on what happens during initial configuration, see "Related Topics."

**Table 23: Prerequisites for Enabling Automatic Configuration**

<table>
<thead>
<tr>
<th>Device</th>
<th>Required Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access switch</td>
<td>Factory default (no configuration file)</td>
</tr>
</tbody>
</table>
### Required Configuration

<table>
<thead>
<tr>
<th>Device</th>
<th>Required Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution switch</td>
<td>• IP helper address</td>
</tr>
</tbody>
</table>
|                         |   • Enable DHCP relay agent
|                         |   • IP routing (if used as default gateway)                                              |
| DHCP server             | • IP address assignment                                                                 |
|                         |   • TFTP server IP address                                                               |
|                         |   • Path to bootstrap configuration file on the TFTP server                               |
|                         |   • Default gateway IP address                                                           |
| TFTP server             | • A bootstrap configuration file that includes the CNS configuration commands that enable the switch to communicate with the Configuration Engine |
|                         |   • The switch configured to use either the switch MAC address or the serial number (instead of the default hostname) to generate the ConfigID and EventID |
|                         |   • The CNS event agent configured to push the configuration file to the switch          |
| CNS Configuration Engine| One or more templates for each type of device, with the ConfigID of the device mapped to the template. |

2 A DHCP Relay is needed only when the DHCP Server is on a different subnet from the client.

## How to Configure the Configuration Engine

### Enabling the CNS Event Agent

---

**Note**

You must enable the CNS event agent on the switch before you enable the CNS configuration agent.

Follow these steps to enable the CNS event agent on the switch.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Enabling the CNS Event Agent

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 3** cns event \{hostname | Enables the event agent, and enters the gateway  
ip-address\} [port-number] [[keepalive seconds | parameters.  
retry-count] [failover-time seconds |  
[reconnect-time time] [backup] |  
Example:                           |         |
| Switch(config)# cns event 10.180.1.27  
keepalive 120 10 |         |
| • For \{hostname | ip-address\}, enter either the hostname or the IP address of the event  
gateway. |
| • (Optional) For port number, enter the port number for the event gateway. The default  
port number is 11011. |
| • (Optional) For keepalive seconds, enter how often the switch sends keepalive messages. For retry-count, enter the  
number of unanswered keepalive messages that the switch sends before the connection is terminated. The default for each is 0. |
| • (Optional) For failover-time seconds, enter how long the switch waits for the primary gateway route after the route to  
the backup gateway is established. |
| • (Optional) For reconnect-time time, enter the maximum time interval that the switch  
waits before trying to reconnect to the event gateway. |
| • (Optional) Enter backup to show that this is the backup gateway. (If omitted, this is  
the primary gateway.) |
| **Step 4** end                     | Returns to privileged EXEC mode. |
| Example:                           |         |
| Switch(config)# end                |         |
| **Step 5** show running-config    | Verifies your entries. |
| Example:                           |         |

Note: Though visible in the command-line help string, the encrypt and the clock-timeout time keywords are not supported.
### Enabling the Cisco IOS CNS Agent

Follow these steps to enable the Cisco IOS CNS agent on the switch.

#### Before you begin

You must enable the CNS event agent on the switch before you enable this agent.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`cns config initial {hostname</td>
<td>ip-address} [port-number]`</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# cns config initial 10.180.1.27 10</code></td>
<td>• For `{hostname</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For <code>port-number</code>, enter the port number for the configuration server.</td>
</tr>
</tbody>
</table>

#### What to do next

To verify information about the event agent, use the `show cns event connections` command in privileged EXEC mode.

To disable the CNS event agent, use the `no cns event {ip-address | hostname}` global configuration command.
## Enabling an Initial Configuration for Cisco IOS CNS Agent

Follow these steps to enable the CNS configuration agent and initiate an initial configuration on the switch.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Step 4**

- **cns config partial** \{hostname | ip-address\} [port-number]

  **Example:**
  ```
  Switch(config)# cns config partial 10.180.1.27 10
  ```

  Enables the Cisco IOS CNS agent and initiates a partial configuration on the switch.

  - For \{hostname | ip-address\}, enter either the hostname or the IP address of the configuration server.
  - (Optional) For port number, enter the port number for the configuration server.

**Step 5**

- **end**

  **Example:**
  ```
  Switch(config)# end
  ```

  Returns to privileged EXEC mode.

**Step 6**

- **show running-config**

  **Example:**
  ```
  Switch# show running-config
  ```

  Verifies your entries.

**Step 7**

- **copy running-config startup-config**

  **Example:**
  ```
  Switch# copy running-config startup-config
  ```

  (Optional) Saves your entries in the configuration file.

**Step 8**

Start the Cisco IOS CNS agent on the switch.

---

**What to do next**

You can now use the Cisco Configuration Engine to remotely send incremental configurations to the switch.

---

**Enabling an Initial Configuration for Cisco IOS CNS Agent**

Follow these steps to enable the CNS configuration agent and initiate an initial configuration on the switch.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>cns template connect name</code></td>
<td>Enters CNS template connect configuration mode, and specifies the name of the CNS connect template.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>cns template connect template-dhcp</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>cli config-text</code></td>
<td>Enters a command line for the CNS connect template. Repeat this step for each command line in the template.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-tmpl-conn)# <code>cli ip address dhcp</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>Repeat Steps 3 to 4 to configure another CNS connect template.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>cns connect name [retries number] [retry-interval seconds] [sleep seconds] [timeout seconds]</code></td>
<td>Enters CNS connect configuration mode, specifies the name of the CNS connect profile, and defines the profile parameters. The switch uses the CNS connect profile to connect to the Configuration Engine.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>cns connect dhcp</code></td>
<td></td>
</tr>
</tbody>
</table>

- Enter the `name` of the CNS connect profile.
- (Optional) For `retries number`, enter the number of connection retries. The range is 1 to 30. The default is 3.
- (Optional) For `retry-interval seconds`, enter the interval between successive connection attempts to the Configuration Engine. The range is 1 to 40 seconds. The default is 10 seconds.
- (Optional) For `sleep seconds`, enter the amount of time before which the first
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>connection attempt occurs. The range is 0 to 250 seconds. The default is 0.</strong> • (Optional) For <strong>timeout seconds</strong>, enter the amount of time after which the connection attempts end. The range is 10 to 2000 seconds. The default is 120.</td>
<td></td>
</tr>
</tbody>
</table>

---

**Step 8** | discover [controller controller-type | dlci [subinterface subinterface-number] | interface [interface-type] | line line-type] |
---|---
| Specifies the interface parameters in the CNS connect profile. |
| • For **controller controller-type**, enter the controller type. |
| • For **dlci**, enter the active data-link connection identifiers (DLCIs). |
| (Optional) For **subinterface subinterface-number**, specify the point-to-point subinterface number that is used to search for active DLCIs. |
| • For **interface [interface-type]**, enter the type of interface. |
| • For **line line-type**, enter the line type. |

---

**Step 9** | template name [... name] |
---|---
| Specifies the list of CNS connect templates in the CNS connect profile to be applied to the switch configuration. You can specify more than one template. |

---

**Example:**

```bash
Switch(config-cns-conn) # discover interface gigabitethernet
```

---

**Step 9** | \[template name [... name] \] |
---|---
| Specifies the list of CNS connect templates in the CNS connect profile to be applied to the switch configuration. You can specify more than one template. |

---

**Example:**

```bash
Switch(config-cns-conn) # template template-dhcp
```

---

**Step 10** | Repeat Steps 8 to 9 to specify more interface parameters and CNS connect templates in the CNS connect profile. |
---|---

---

**Step 11** | exit |
---|---
| Returns to global configuration mode. |

---

**Example:**

```bash
Switch(config-cns-conn) # exit
```

---

**Step 12** | hostname name |
---|---
| Enters the hostname for the switch. |

---

**Example:**

```bash
Switch(config) # hostname device1
```

---

**Step 13** | ip route network-number |
---|---
| (Optional) Establishes a static route to the Configuration Engine whose IP address is **network-number**. |

---

**Example:**

```bash
RemoteSwitch(config) # ip route
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.28.129.22 255.255.255.255 11.11.11.1</td>
<td>(Optional) Sets the unique EventID or ConfigID used by the Configuration Engine. If you enter this command, do not enter the `cns id {hardware-serial</td>
</tr>
</tbody>
</table>

**Step 14**

`cns id interface num {dns-reverse | ipaddress | mac-address} [event] [image]`

**Example:**

RemoteSwitch(config)# cns id GigabitEthernet0/1 ipaddress

- For `interface num`, enter the type of interface. For example, ethernet, group-async, loopback, or virtual-template. This setting specifies from which interface the IP or MAC address should be retrieved to define the unique ID.

- For `{dns-reverse | ipaddress | mac-address}`, enter `dns-reverse` to retrieve the hostname and assign it as the unique ID, enter `ipaddress` to use the IP address, or enter `mac-address` to use the MAC address as the unique ID.

- (Optional) Enter `event` to set the ID to be the event-id value used to identify the switch.

- (Optional) Enter `image` to set the ID to be the image-id value used to identify the switch.

**Note** If both the `event` and `image` keywords are omitted, the image-id value is used to identify the switch.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`cns id {hardware-serial</td>
<td>hostname</td>
</tr>
</tbody>
</table>

**Step 15**

**Example:**

RemoteSwitch(config)# cns id hostname

- For `{hardware-serial | hostname | string string | udi}`, enter `hardware-serial` to set the switch serial number as the unique ID, enter `hostname` (the default) to select the switch hostname as the unique ID, enter an arbitrary text string for `string string` as the unique ID, or enter `udi` to set the unique device identifier (UDI) as the unique ID.
### Enabling an Initial Configuration for Cisco IOS CNS Agent

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 16</strong></td>
<td>`cns config initial {hostname</td>
<td>ip-address} [port-number] [event] [no-persist] [page page] [source ip-address] [syntax-check]`</td>
</tr>
<tr>
<td></td>
<td>Example: RemoteSwitch(config)# <code>cns config initial 10.1.1.1 no-persist</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Though visible in the command-line help string, the <code>encrypt</code>, <code>status url</code>, and <code>inventory</code> keywords are not supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Step 17</strong></td>
<td><code>end</code> Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Step 18</strong></td>
<td><code>show running-config</code> Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# <code>show running-config</code></td>
<td></td>
</tr>
</tbody>
</table>
Purpose

Command or Action | Purpose
--- | ---
Step 19 | copy running-config startup-config
   Example:
Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file.

What to do next

To verify information about the configuration agent, use the `show cns config connections` command in privileged EXEC mode.

To disable the CNS Cisco IOS agent, use the `no cns config initial { ip-address | hostname }` global configuration command.

**Refreshing DeviceIDs**

Follow these steps to refresh a DeviceID when changing the hostname on the switch.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable  
   Example:
Switch> enable | Enables privileged EXEC mode.  
   • Enter your password if prompted.  
   |  
| Step 2 | show cns config connections  
   Example:
Switch# show cns config connections | Displays whether the CNS event agent is connecting to the gateway, connected, or active, and the gateway used by the event agent, its IP address and port number. |
| Step 3 | Make sure that the CNS event agent is properly connected to the event gateway. | Examine the output of `show cns config connections` for the following:  
   • Connection is active.  
   • Connection is using the currently configured switch hostname. The DeviceID will be refreshed to correspond to the new hostname configuration using these instructions. |
| Step 4 | show cns event connections  
   Example:
Switch# show cns event connections | Displays the event connection information for your switch. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Record from the output of Step 4 the information for the currently connected connection listed below. You will be using the IP address and port number in subsequent steps of these instructions.</td>
<td></td>
</tr>
</tbody>
</table>
| 6     | configure terminal  
**Example:**  
Switch# configure terminal | Enters global configuration mode. |
| 7     | no cns event *ip-address* *port-number*  
**Example:**  
Switch(config)# no cns event 172.28.129.22 2012 | Specifies the IP address and port number that you recorded in Step 5 in this command.  
This command breaks the connection between the switch and the event gateway. It is necessary to first break, then reestablish, this connection to refresh the DeviceID. |
| 8     | cns event *ip-address* *port-number*  
**Example:**  
Switch(config)# cns event 172.28.129.22 2012 | Specifies the IP address and port number that you recorded in Step 5 in this command.  
This command reestablishes the connection between the switch and the event gateway. |
| 9     | end  
**Example:**  
Switch(config)# end | Returns to privileged EXEC mode. |
| 10    | Make sure that you have reestablished the connection between the switch and the event connection by examining the output from `show cns event connections`. | |
| 11    | show running-config  
**Example:**  
Switch# show running-config | Verifies your entries. |
| 12    | copy running-config startup-config  
**Example:**  
Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
## Enabling a Partial Configuration for Cisco IOS CNS Agent

Follow these steps to enable the Cisco IOS CNS agent and to initiate a partial configuration on the switch.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
Example: ```Switch> enable``` |
| **Step 2** | configure terminal | Enters global configuration mode.  
Example: ```Switch# configure terminal``` |
| **Step 3** | cns config partial \{ip-address | hostname\} \[port-number\] \[source ip-address\] | Enables the configuration agent, and initiates a partial configuration.  
Example: ```Switch(config)# cns config partial 172.28.129.22 2013``` |
| **Step 4** | end | Returns to privileged EXEC mode.  
Example: ```Switch(config)# end``` |
| **Step 5** | show running-config | Verifies your entries.  
Example: ```Switch# show running-config``` |
| **Step 6** | copy running-config startup-config | (Optional) Saves your entries in the configuration file.  
Example: |
**Monitoring CNS Configurations**

### Table 24: CNS show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show cns config connections</code></td>
<td>Displays the status of the CNS Cisco IOS CNS agent connections.</td>
</tr>
<tr>
<td><code>Switch# show cns config connections</code></td>
<td></td>
</tr>
<tr>
<td><code>show cns config outstanding</code></td>
<td>Displays information about incremental (partial) CNS configurations that have started but are not yet completed.</td>
</tr>
<tr>
<td><code>Switch# show cns config outstanding</code></td>
<td></td>
</tr>
<tr>
<td><code>show cns config stats</code></td>
<td>Displays statistics about the Cisco IOS CNS agent.</td>
</tr>
<tr>
<td><code>Switch# show cns config stats</code></td>
<td></td>
</tr>
<tr>
<td><code>show cns event connections</code></td>
<td>Displays the status of the CNS event agent connections.</td>
</tr>
<tr>
<td><code>Switch# show cns event connections</code></td>
<td></td>
</tr>
<tr>
<td><code>show cns event gateway</code></td>
<td>Displays the event gateway information for your switch.</td>
</tr>
<tr>
<td><code>Switch# show cns event gateway</code></td>
<td></td>
</tr>
<tr>
<td><code>show cns event stats</code></td>
<td>Displays statistics about the CNS event agent.</td>
</tr>
<tr>
<td><code>Switch# show cns event stats</code></td>
<td></td>
</tr>
<tr>
<td><code>show cns event subject</code></td>
<td>Displays a list of event agent subjects that are subscribed to by applications.</td>
</tr>
<tr>
<td><code>Switch# show cns event subject</code></td>
<td></td>
</tr>
</tbody>
</table>
## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
<th>Link</th>
</tr>
</thead>
</table>

### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>-</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
## Feature History and Information for the Configuration Engine

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 32

Configuring the Cisco Discovery Protocol

Cisco Discovery Protocol is a Layer 2, media-independent, and network-independent protocol that runs on Cisco devices and enables networking applications to learn about directly connected devices nearby. This protocol facilitates the management of Cisco devices by discovering these devices, determining how they are configured, and allowing systems using different network-layer protocols to learn about each other.

This module describes Cisco Discovery Protocol Version 2 and how it functions with SNMP.

• Information About CDP, on page 423
• How to Configure CDP, on page 424
• Monitoring and Maintaining Cisco Discovery Protocol, on page 431
• Additional References, on page 431
• Feature History and Information for Cisco Discovery Protocol, on page 432

Information About CDP

Cisco Discovery Protocol Overview

Cisco Discovery Protocol is a device discovery protocol that runs over Layer 2 (the data-link layer) on all Cisco-manufactured devices (routers, bridges, access servers, controllers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With Cisco Discovery Protocol, network management applications can learn the device type and the SNMP agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.

Cisco Discovery Protocol runs on all media that support Subnetwork Access Protocol (SNAP). Because Cisco Discovery Protocol runs over the data-link layer only, two systems that support different network-layer protocols can learn about each other.

Each Cisco Discovery Protocol-configured device sends periodic messages to a multicast address, advertising at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime information, which is the length of time a receiving device holds Cisco Discovery Protocol information before discarding it. Each device also listens to the messages sent by other devices to learn about neighboring devices.

On the switch, Cisco Discovery Protocol enables Network Assistant to display a graphical view of the network. The switch uses Cisco Discovery Protocol to find cluster candidates and maintain information about cluster members and other devices up to three cluster-enabled devices away from the command switch by default.
• Cisco Discovery Protocol identifies connected endpoints that communicate directly with the switch.
• To prevent duplicate reports of neighboring devices, only one wired switch reports the location information.
• The wired switch and the endpoints both send and receive location information.

CDP and Stacks

A switch stack appears as a single switch in the network. Therefore, CDP discovers the switch stack, not the individual stack members. The switch stack sends CDP messages to neighboring network devices when there are changes to the switch stack membership, such as stack members being added or removed.

Default Cisco Discovery Protocol Configuration

This table shows the default Cisco Discovery Protocol configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Discovery Protocol global state</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco Discovery Protocol interface state</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco Discovery Protocol timer (packet update frequency)</td>
<td>60 seconds</td>
</tr>
<tr>
<td>Cisco Discovery Protocol holdtime (before discarding)</td>
<td>180 seconds</td>
</tr>
<tr>
<td>Cisco Discovery Protocol Version-2 advertisements</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

How to Configure CDP

Configuring Cisco Discovery Protocol Characteristics

You can configure these Cisco Discovery Protocol characteristics:
• Frequency of Cisco Discovery Protocol updates
• Amount of time to hold the information before discarding it
• Whether or not to send Version 2 advertisements

Steps 3 through 5 are all optional and can be performed in any order.

Follow these steps to configure the Cisco Discovery Protocol characteristics.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  enable
  Example: Switch> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| **Step 2**
  configure terminal
  Example: Switch# configure terminal | Enters global configuration mode. |
| **Step 3**
  cdp timer seconds
  Example: Switch(config)# cdp timer 20 | (Optional) Sets the transmission frequency of Cisco Discovery Protocol updates in seconds. The range is 5 to 254; the default is 60 seconds. |
| **Step 4**
  cdp holdtime seconds
  Example: Switch(config)# cdp holdtime 60 | (Optional) Specifies the amount of time a receiving device should hold the information sent by your device before discarding it. The range is 10 to 255 seconds; the default is 180 seconds. |
| **Step 5**
  cdp advertise-v2
  Example: Switch(config)# cdp advertise-v2 | (Optional) Configures Cisco Discovery Protocol to send Version 2 advertisements. This is the default state. |
| **Step 6**
  end
  Example: Switch(config)# end | Returns to privileged EXEC mode. |
| **Step 7**
  show running-config
  Example: Switch# show running-config | Verifies your entries. |
| **Step 8**
  copy running-config startup-config
  Example: Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
Disabling Cisco Discovery Protocol

Cisco Discovery Protocol is enabled by default.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> no cdp run</td>
<td>Disables Cisco Discovery Protocol.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# no cdp run</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange Cisco Discovery Protocol messages. Disabling Cisco Discovery Protocol can interrupt cluster discovery and device connectivity.

Follow these steps to disable the Cisco Discovery Protocol device discovery capability.

What to do next
Use the no form of the Cisco Discovery Protocol commands to return to the default settings.
Enabling Cisco Discovery Protocol

Cisco Discovery Protocol is enabled by default.

Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange Cisco Discovery Protocol messages. Disabling Cisco Discovery Protocol can interrupt cluster discovery and device connectivity.

Note

Follow these steps to enable Cisco Discovery Protocol when it has been disabled.

Before you begin

Cisco Discovery Protocol must be disabled, or it cannot be enabled.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup-config</td>
<td></td>
</tr>
</tbody>
</table>

What to do next

You must reenable Cisco Discovery Protocol to use it.
### Disabling Cisco Discovery Protocol on an Interface

Cisco Discovery Protocol is enabled by default on all supported interfaces to send and to receive Cisco Discovery Protocol information.

#### Note
Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange Cisco Discovery Protocol messages. Disabling Cisco Discovery Protocol can interrupt cluster discovery and device connectivity.

#### Note
Cisco Discovery Protocol bypass is not supported and may cause a port go into err-disabled state.

Follow these steps to disable Cisco Discovery Protocol on a port.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>

What to do next

Use the `show run all` command to show that Cisco Discovery Protocol has been enabled. If you enter only `show run`, the enabling of Cisco Discovery Protocol may not be displayed.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td>Specifies the interface on which you are disabling Cisco Discovery Protocol, and enters interface configuration mode.</td>
</tr>
</tbody>
</table>

**Step 3**

```
interface interface-id
```

**Example:**
```
Switch(config)# interface gigabitethernet 1/0/1
```

**Step 4**

```
no cdp enable
```

**Example:**
```
Switch(config-if)# no cdp enable
```

**Step 5**

```
end
```

**Example:**
```
Switch(config)# end
```

**Step 6**

```
show running-config
```

**Example:**
```
Switch# show running-config
```

**Step 7**

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

**Example:**
```
Switch# copy running-config startup-config
```

### Enabling Cisco Discovery Protocol on an Interface

Cisco Discovery Protocol is enabled by default on all supported interfaces to send and receive Cisco Discovery Protocol information.

**Note**

Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange Cisco Discovery Protocol messages. Disabling Cisco Discovery Protocol can interrupt cluster discovery and device connectivity.

**Note**

Cisco Discovery Protocol bypass is not supported and may cause a port to go into err-disabled state.

Follow these steps to enable Cisco Discovery Protocol on a port on which it has been disabled.
Before you begin
Cisco Discovery Protocol must be disabled on the port that you are trying to Cisco Discovery Protocol enable on, or it cannot be enabled.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the interface on which you are enabling Cisco Discovery Protocol, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# interface gigabitethernet1/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> cdp enable</td>
<td>Enables Cisco Discovery Protocol on a disabled interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# cdp enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Monitoring and Maintaining Cisco Discovery Protocol

Table 25: Commands for Displaying Cisco Discovery Protocol Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear cdp counters</td>
<td>Resets the traffic counters to zero.</td>
</tr>
<tr>
<td>clear cdp table</td>
<td>Deletes the Cisco Discovery Protocol table of information about neighbors.</td>
</tr>
<tr>
<td>show cdp</td>
<td>Displays global information, such as frequency of transmissions and the holdtime for packets being sent.</td>
</tr>
<tr>
<td>show cdp entry entry-name [version] [protocol]</td>
<td>Displays information about a specific neighbor. You can enter an asterisk (*) to display all Cisco Discovery Protocol neighbors, or you can enter the name of the neighbor about which you want 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.</td>
</tr>
<tr>
<td>show cdp interface [interface-id]</td>
<td>Displays information about interfaces where Cisco Discovery Protocol is enabled. You can limit the display to the interface about which you want information.</td>
</tr>
<tr>
<td>show cdp neighbors [interface-id] [detail]</td>
<td>Displays information about neighbors, including device type, interface type and number, holdtime settings, capabilities, platform, and port ID. You can limit the display to neighbors of a specific interface or expand the display to provide more detailed information.</td>
</tr>
<tr>
<td>show cdp traffic</td>
<td>Displays Cisco Discovery Protocol counters, including the number of packets sent and received and checksum errors.</td>
</tr>
</tbody>
</table>

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Management Commands</td>
<td>Network Management Command Reference, Cisco IOS XE Release 3E</td>
</tr>
</tbody>
</table>
Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>-</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information for Cisco Discovery Protocol

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring Simple Network Management Protocol

- Finding Feature Information, on page 433
- Prerequisites for SNMP, on page 433
- Restrictions for SNMP, on page 435
- Information About SNMP, on page 436
- How to Configure SNMP, on page 439
- Monitoring SNMP Status, on page 456
- SNMP Examples, on page 457
- Additional References, on page 458
- Feature History and Information for Simple Network Management Protocol, on page 459

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for SNMP

Supported SNMP Versions

This software release supports the following SNMP versions:

- SNMPv1—The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.
- SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the community-string-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic. It has these features:
- SNMPv2C—The community-string-based Administrative Framework for SNMPv2, an Experimental Internet Protocol defined in RFC 1901.
- SNMPv3—Version 3 of the SNMP is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network and includes these security features:
  - Message integrity—Ensures that a packet was not tampered with in transit.
  - Authentication—Determines that the message is from a valid source.
  - Encryption—Mixes the contents of a package to prevent it from being read by an unauthorized source.

To select encryption, enter the `priv` keyword.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent’s MIB is defined by an IP address access control list and password.

SNMPv2C includes a bulk retrieval function and more detailed error message reporting to management stations. The bulk retrieval function retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes in SNMPv2C report the error type.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up for a user and the group within which the user resides. A security level is the permitted level of security within a security model. A combination of the security level and the security model determine which security method is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2C, and SNMPv3.

The following table identifies characteristics and compares different combinations of security models and levels:

<table>
<thead>
<tr>
<th>Model</th>
<th>Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv1</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>SNMPv2C</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>noAuthNoPriv</td>
<td>Username</td>
<td>No</td>
<td>Uses a username match for authentication.</td>
</tr>
</tbody>
</table>
### Result

<table>
<thead>
<tr>
<th>Model</th>
<th>Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv3</td>
<td>authNoPriv</td>
<td>Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)</td>
<td>No</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>authPriv</td>
<td>MD5 or SHA</td>
<td>Data Encryption Standard (DES) or Advanced Encryption Standard (AES)</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 3DES 168-bit encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• AES 128-bit, 192-bit, or 256-bit encryption</td>
</tr>
</tbody>
</table>

You must configure the SNMP agent to use the SNMP version supported by the management station. Because an agent can communicate with multiple managers, you can configure the software to support communications using SNMPv1, SNMPv2C, or SNMPv3.

## Restrictions for SNMP

### Version Restrictions

- SNMPv1 does not support informs.
Information About SNMP

SNMP Overview

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a management information base (MIB). The SNMP manager can be part of a network management system (NMS) such as Cisco Prime Infrastructure. The agent and MIB reside on the switch. To configure SNMP on the switch, 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 Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in the following table:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get-request</td>
<td>Retrieves a value from a specific variable.</td>
</tr>
<tr>
<td>get-next-request</td>
<td>Retrieves a value from a variable within a table.</td>
</tr>
<tr>
<td>get-bulk-request</td>
<td>Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data.</td>
</tr>
<tr>
<td>get-response</td>
<td>Replies to a get-request, get-next-request, and set-request sent by an NMS.</td>
</tr>
<tr>
<td>set-request</td>
<td>Stores a value in a specific variable.</td>
</tr>
<tr>
<td>trap</td>
<td>An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.</td>
</tr>
</tbody>
</table>

3 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.

4 The get-bulk command only works with SNMPv2 or later.

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.

Related Topics
Disabling the SNMP Agent, on page 439
Monitoring SNMP Status, on page 456

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the switch, the community string definitions on the NMS must match at least one of the three community string definitions on the switch.

A community string can have one of the following attributes:

• Read-only (RO)—Gives all objects in the MIB except the community strings read access to authorized management stations, but does not allow write access.

• Read-write (RW)—Gives all objects in the MIB read and write access to authorized management stations, but does not allow access to the community strings.

• When a cluster is created, the command switch manages the exchange of messages among member switches and the SNMP application. The Network Assistant software appends the member switch number (@esN, where N is the switch number) to the first configured RW and RO community strings on the command switch and propagates them to the member switches.

Related Topics
Configuring Community Strings, on page 441

SNMP MIB Variables Access

An example of an NMS is the Cisco Prime Infrastructure network management software. Cisco Prime Infrastructure 2.0 software uses the switch 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 internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown in the figure, the SNMP agent gathers data from the MIB. The agent can send traps, or notification of certain events, to the SNMP manager, which receives and processes the traps. Traps alert 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 31: SNMP Network
SNMP Notifications

SNMP allows the switch to send notifications to SNMP managers when particular events occur. SNMP notifications can be sent as traps or inform requests. In command syntax, unless there is an option in the command to select either traps or informs, the keyword traps refers to either traps or informs, or both. Use the `snmp-server host` command to specify whether to send SNMP notifications as traps or informs.

---

**Note**

SNMPv1 does not support informs.

Traps are unreliable because the receiver does not send an acknowledgment when it receives a trap, and the sender cannot determine if the trap was received. When an SNMP manager receives an inform request, it acknowledges the message with an SNMP response protocol data unit (PDU). If the sender does not receive a response, the inform request can be sent again. Because they can be resent, informs are more likely than traps to reach their intended destination.

The characteristics that make informs more reliable than traps also consume more resources in the switch and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request is held in memory until a response is received or the request times out. Traps are sent only once, but an inform might be resent or retried several times. The retries increase traffic and contribute to a higher overhead on the network. Therefore, traps and informs require a trade-off between reliability and resources. If it is important that the SNMP manager receive every notification, use inform requests. If traffic on the network or memory in the switch is a concern and notification is not required, use traps.

**Related Topics**

- Configuring SNMP Notifications, on page 446
- Monitoring SNMP Status, on page 456

SNMP ifIndex MIB Object Values

The SNMP agent's IF-MIB module comes up shortly after reboot. As various physical interface drivers are initialized they register with the IF-MIB module, essentially saying "Give me an ifIndex number". The IF-MIB module assigns the next available ifIndex number on a first-come-first-served basis. That is, minor differences in driver initialization order from one reboot to another can result in the same physical interface getting a different ifIndex number than it had before the reboot (unless ifIndex persistency is enabled of course).

Default SNMP Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP agent</td>
<td>Disabled².</td>
</tr>
<tr>
<td>SNMP trap receiver</td>
<td>None configured.</td>
</tr>
<tr>
<td>SNMP traps</td>
<td>None enabled except the trap for TCP connections (tty).</td>
</tr>
<tr>
<td>SNMP version</td>
<td>If no version keyword is present, the default is Version 1.</td>
</tr>
<tr>
<td>SNMPv3 authentication</td>
<td>If no keyword is entered, the default is the noauth (noAuthNoPriv) security level.</td>
</tr>
<tr>
<td>SNMP notification type</td>
<td>If no type is specified, all notifications are sent.</td>
</tr>
</tbody>
</table>
This is the default when the switch starts and the startup configuration does not have any `snmp-server` global configuration commands.

## SNMP Configuration Guidelines

If the switch starts and the switch startup configuration has at least one `snmp-server` global configuration command, the SNMP agent is enabled.

An SNMP group is a table that maps SNMP users to SNMP views. An SNMP user is a member of an SNMP group. An SNMP host is the recipient of an SNMP trap operation. An SNMP engine ID is a name for the local or remote SNMP engine.

When configuring SNMP, follow these guidelines:

- When configuring an SNMP group, do not specify a notify view. The `snmp-server host` global configuration command auto-generates a notify view for the user and then adds it to the group associated with that user. Modifying the group's notify view affects all users associated with that group.

- To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides.

- Before you configure remote users for a particular agent, configure the SNMP engine ID, using the `snmp-server engineID` global configuration command with the `remote` option. The remote agent's SNMP engine ID and user password are used to compute the authentication and privacy digests. If you do not configure the remote engine ID first, the configuration command fails.

- When configuring SNMP informs, you need to configure the SNMP engine ID for the remote agent in the SNMP database before you can send proxy requests or informs to it.

- If a local user is not associated with a remote host, the switch does not send informs for the `auth` (authNoPriv) and the `priv` (authPriv) authentication levels.

- Changing the value of the SNMP engine ID has significant results. A user's password (entered on the command line) is converted to an MD5 or SHA security digest based on the password and the local engine ID. The command-line password is then destroyed, as required by RFC 2274. Because of this deletion, if the value of the engine ID changes, the security digests of SNMPv3 users become invalid, and you need to reconfigure SNMP users by using the `snmp-server user` `username` global configuration command. Similar restrictions require the reconfiguration of community strings when the engine ID changes.

### Related Topics

- Configuring SNMP Groups and Users, on page 443
- Monitoring SNMP Status, on page 456

## How to Configure SNMP

### Disabling the SNMP Agent

The `no snmp-server` global configuration command disables all running versions (Version 1, Version 2C, and Version 3) of the SNMP agent on the device. You reenable all versions of the SNMP agent by the first
The SNMP Agent must be enabled before it can be disabled. The SNMP agent is enabled by the first `snmp-server` global configuration command entered on the device.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> no snmp-server</td>
<td>Disables the SNMP agent operation.</td>
</tr>
<tr>
<td>Example: Switch(config)# no snmp-server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example: Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example: Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Configuring 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 switch. 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, which 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

Follow these steps to configure a community string on the switch.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> snmp-server community string [view view-name] [ro</td>
<td>rw] [access-list-number]</td>
</tr>
<tr>
<td><strong>Note</strong> The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# snmp-server community comaccess ro 4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For <em>string</em>, 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.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <em>view</em>, specify the view record accessible to the community.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Specify either read-only (<em>ro</em>) if you want authorized management stations to retrieve MIB objects, or specify</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) For access-list-number, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**

access-list 4 deny any

**Example:**

Switch(config)# access-list 4 deny any

(Optional) If you specified an IP standard access list number in Step 3, then create the list, repeating the command as many times as necessary.

• For access-list-number, enter the access list number specified in Step 3.

• 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.

Recall that the access list is always terminated by an implicit deny statement for everything.

**Step 5**

end

**Example:**

Switch(config)# end

Returns to privileged EXEC mode.

**Step 6**

show running-config

**Example:**

Switch# show running-config

Verifies your entries.

**Step 7**

copy running-config startup-config

**Example:**

(Optional) Saves your entries in the configuration file.
<table>
<thead>
<tr>
<th><strong>Purpose</strong></th>
<th><strong>Command or Action</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

To disable access for an SNMP community, set the community string for that community to the null string (do not enter a value for the community string).

To remove a specific community string, use the `no snmp-server community-string` global configuration command.

You can specify an identification name (engine ID) for the local or remote SNMP server engine on the switch. You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.

**Related Topics**

SNMP Community Strings, on page 437

---

**Configuring SNMP Groups and Users**

You can specify an identification name (engine ID) for the local or remote SNMP server engine on the switch. You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.

Follow these steps to configure SNMP groups and users on the switch.

**Procedure**

<table>
<thead>
<tr>
<th><strong>Step</strong></th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>snmp-server engineID (local engineid-string</td>
<td>Configures a name for either the local or remote copy of SNMP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The engineid-string is a 24-character ID string with the name of the copy of SNMP. You need not specify the entire 24-character engine ID if it has trailing zeros. Specify only the portion of the</td>
</tr>
<tr>
<td></td>
<td>[remote ip-address [udp-port port-number] engineid-string]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# snmp-server engineID local 1234</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>engine ID up to the point where only zeros remain in the value. The Step Example configures an engine ID of 123400000000000000000000.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If you select <code>remote</code>, specify the <code>ip-address</code> of the device that contains the remote copy of SNMP and the optional User Datagram Protocol (UDP) port on the remote device. The default is 162.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures a new SNMP group on the remote device.</td>
<td></td>
</tr>
<tr>
<td>`snmp-server group group-name {v1</td>
<td>v2c</td>
<td>v3 {auth</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• <code>v1</code> is the least secure of the possible security models.</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# snmp-server group public v2c access lmnop</code></td>
<td>• <code>v2c</code> is the second least secure model. It allows transmission of informs and integers twice the normal width.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>v3</code>, the most secure, requires you to select one of the following authentication levels:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>auth</code>—Enables the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA) packet authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>noauth</code>—Enables the noAuthNoPriv security level. This is the default if no keyword is specified.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>priv</code>—Enables Data Encryption Standard (DES) packet encryption (also called privacy).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Optional) Enter <code>read readview</code> with a string (not to exceed 64 characters) that is the name of the view in which you can only view the contents of the agent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Optional) Enter <code>write writeview</code> with a string (not to exceed 64 characters) that is the name of the view in which you enter data and configure the contents of the agent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Optional) Enter <code>notify notifyview</code> with a string (not to exceed 64 characters) that is the name of the view in which you specify a notify, inform, or trap.</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring SNMP Groups and Users

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Enter <code>access access-list</code> with a string (not to exceed 64 characters) that is the name of the access list.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

```bash
snmp-server user username group-name
remote host [ udp-port port ] { v1 [access access-list] | v2c [access access-list] | v3 [encrypted] [access access-list] [auth {md5 | sha} auth-password] } [priv {des | 3des | aes {128 | 192 | 256}} priv-password]
```

**Example:**

```bash
Switch(config)# snmp-server user Pat public v2c
```

- Adds a new user for an SNMP group.
- **username** is the name of the user on the host that connects to the agent.
- **group-name** is the name of the group to which the user is associated.
- Enter `remote` to specify a remote SNMP entity to which the user belongs and the hostname or IP address of that entity with the optional UDP port number. The default is 162.
- Enter the SNMP version number (`v1`, `v2c`, or `v3`). If you enter `v3`, you have these additional options:
  - **encrypted** specifies that the password appears in encrypted format. This keyword is available only when the `v3` keyword is specified.
  - **auth** is an authentication level setting session that can be either the HMAC-MD5-96 (`md5`) or the HMAC-SHA-96 (`sha`) authentication level and requires a password string `auth-password` (not to exceed 64 characters).

If you enter `v3` you can also configure a private (`priv`) encryption algorithm and password string `priv-password` using the following keywords (not to exceed 64 characters):

- **priv** specifies the User-based Security Model (USM).
- **des** specifies the use of the 56-bit DES algorithm.
- **3des** specifies the use of the 168-bit DES algorithm.
- **aes** specifies the use of the DES algorithm. You must select either 128-bit, 192-bit, or 256-bit encryption.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Enter <strong>access access-list</strong> with a string (not to exceed 64 characters) that is the name of the access list.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# <strong>end</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example: Switch# <strong>show running-config</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example: Switch# <strong>copy running-config startup-config</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**
- SNMP Configuration Guidelines, on page 439
- Monitoring SNMP Status, on page 456

## Configuring SNMP Notifications

A trap manager is a management station that receives and processes traps. Traps are system alerts that the switch generates when certain events occur. By default, no trap manager is defined, and no traps are sent. Switches running this Cisco IOS release can have an unlimited number of trap managers.

### Note

Many commands use the word **traps** in the command syntax. Unless there is an option in the command to select either traps or informs, the keyword **traps** refers to traps, informs, or both. Use the **snmp-server host** global configuration command to specify whether to send SNMP notifications as traps or informs.

You can use the **snmp-server host** global configuration command for a specific host to receive the notification types listed in the following table. You can enable any or all of these traps and configure a trap manager to receive them.

### Table 28: Device Notification Types

<table>
<thead>
<tr>
<th>Notification Type Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge</td>
<td>Generates STP bridge MIB traps.</td>
</tr>
<tr>
<td>cluster</td>
<td>Generates a trap when the cluster configuration changes.</td>
</tr>
<tr>
<td>Notification Type Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>config</td>
<td>Generates a trap for SNMP configuration changes.</td>
</tr>
<tr>
<td>copy-config</td>
<td>Generates a trap for SNMP copy configuration changes.</td>
</tr>
<tr>
<td>cpu threshold</td>
<td>Allow CPU-related traps.</td>
</tr>
<tr>
<td>entity</td>
<td>Generates a trap for SNMP entity changes.</td>
</tr>
<tr>
<td>envmon</td>
<td>Generates environmental monitor traps. You can enable any or all of these environmental traps: fan, shutdown, status, supply, temperature.</td>
</tr>
<tr>
<td>flash</td>
<td>Generates SNMP FLASH notifications. In a switch stack, you can optionally enable notification for flash insertion or removal, which would cause a trap to be issued whenever a switch in the stack is removed or inserted (physical removal, power cycle, or reload).</td>
</tr>
<tr>
<td>fru-ctrl</td>
<td>Generates entity field-replaceable unit (FRU) control traps. In the switch stack, this trap refers to the insertion or removal of a switch in the stack.</td>
</tr>
<tr>
<td>hsrp</td>
<td>Generates a trap for Hot Standby Router Protocol (HSRP) changes.</td>
</tr>
<tr>
<td>ipmulticast</td>
<td>Generates a trap for IP multicast routing changes.</td>
</tr>
<tr>
<td>mac-notification</td>
<td>Generates a trap for MAC address notifications.</td>
</tr>
<tr>
<td>ospf</td>
<td>Generates a trap for Open Shortest Path First (OSPF) changes. You can enable any or all of these traps: Cisco specific, errors, link-state advertisement, rate limit, retransmit, and state changes.</td>
</tr>
<tr>
<td>pim</td>
<td>Generates a trap for Protocol-Independent Multicast (PIM) changes. You can enable any or all of these traps: invalid PIM messages, neighbor changes, and rendezvous point (RP)-mapping changes.</td>
</tr>
</tbody>
</table>
| port-security             | Generates SNMP port security traps. You can also set a maximum trap rate per second. The range is from 0 to 1000; the default is 0, which means that there is no rate limit. **Note** When you configure a trap by using the notification type `port-security`, configure the port security trap first, and then configure the port security trap rate:  
  1. `snmp-server enable traps port-security`  
  2. `snmp-server enable traps port-security trap-rate rate` |
| syslog                    | Generates SNMP syslog traps. |
### Configuration SNMP Notifications

<table>
<thead>
<tr>
<th>Notification Type</th>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tty</td>
<td>Generates a trap for TCP connections. This trap is enabled by default.</td>
</tr>
<tr>
<td></td>
<td>vlan-mem</td>
<td>Generates a trap for SNMP VLAN membership changes.</td>
</tr>
<tr>
<td></td>
<td>vlancreate</td>
<td>Generates SNMP VLAN created traps.</td>
</tr>
<tr>
<td></td>
<td>vlandelete</td>
<td>Generates SNMP VLAN deleted traps.</td>
</tr>
<tr>
<td></td>
<td>vtp</td>
<td>Generates a trap for VLAN Trunking Protocol (VTP) changes.</td>
</tr>
</tbody>
</table>

Follow these steps to configure the switch to send traps or informs to a host.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>snmp-server engineID remote ip-address engineid-string</td>
<td>Specifies the engine ID for the remote host.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# snmp-server engineID remote 192.180.1.27 0000063000100a1c0b4011b</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>snmp-server user username group-name {remote host [udp-port port] {v1 [access access-list]</td>
<td>v2c [access access-list]</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You cannot configure a remote user for an address without first configuring the engine ID for the remote host. Otherwise, you receive an error message, and the command is not executed.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# snmp-server user Pat public v2c</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>snmp-server group group-name {v1</td>
<td>v2c</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# snmp-server group public v2c access lmnop</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring SNMP Notifications

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>`snmp-server host host-addr [informs</td>
<td>trapping] [version {1</td>
</tr>
<tr>
<td>7</td>
<td><code>snmp-server enable traps notification-types</code></td>
<td>Enables the switch to send traps or informs and specifies the type of notifications to be sent. For a list of notification types, see the table above, or enter <code>snmp-server enable traps ?</code> To enable multiple types of traps, you must enter a separate <code>snmp-server enable traps</code> command for each trap type.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>snmp-server trap-source interface-id</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# snmp-server trap-source gigabitethernet 1/0/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Optional) Specifies the source interface, which provides the IP address for the trap message. This command also sets the source IP address for informs.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>snmp-server queue-length length</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# snmp-server queue-length 20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Optional) Establishes the message queue length for each trap host. The range is 1 to 5000; the default is 10.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>snmp-server trap-timeout seconds</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# snmp-server trap-timeout 60</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Optional) Defines how often to resend trap messages. The range is 1 to 1000; the default is 30 seconds.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>end</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>show running-config</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verifies your entries.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>copy running-config startup-config</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Optional) Saves your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>
### What to do next

The **snmp-server host** command specifies which hosts receive the notifications. The **snmp-server enable traps** command globally enables the method for the specified notification (for traps and informs). To enable a host to receive an inform, you must configure an **snmp-server host informs** command for the host and globally enable informs by using the **snmp-server enable traps** command.

To remove the specified host from receiving traps, use the **no snmp-server host host** global configuration command. The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** global configuration command. To disable a specific trap type, use the **no snmp-server enable traps notification-types** global configuration command.

#### Related Topics
- SNMP Notifications, on page 438
- Monitoring SNMP Status, on page 456

### Setting the Agent Contact and Location Information

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.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>snmp-server contact <strong>text</strong></td>
<td>Sets the system contact string.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# snmp-server contact Dial System Operator at beeper 21555</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>snmp-server location <strong>text</strong></td>
<td>Sets the system location string.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# snmp-server location Building 3/Room 222</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Limiting TFTP Servers Used Through SNMP

Follow these steps to limit the TFTP servers used for saving and loading configuration files through SNMP to the servers specified in an access list.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>snmp-server tftp-server-list access-list-number</td>
<td>Limits the TFTP servers used for configuration file copies through SNMP to the servers in the access list. For access-list-number, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# snmp-server tftp-server-list 44</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>access-list access-list-number {deny</td>
<td>permit} source [source-wildcard]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
**Purpose**

Command or Action | Purpose
------------------|--------------------------------------------------
Switch(config)# access-list 44 permit 10.1.1.2 | 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 TFTP servers that can access the switch. (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. The access list is always terminated by an implicit deny statement for everything.

**Step 5**

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Step 6**

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show running-config</td>
<td></td>
</tr>
</tbody>
</table>

**Step 7**

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

---

**Configuring Trap Flags for SNMP**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Trap Flags for SNMP

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2** | `trapflags ap \{ interfaceup | register \}` | Enables sending AP-related traps. Use the `no` form of the command to disable the trap flags.  
- `interfaceup`– Enables trap when a Cisco AP interface (A or B) comes up.  
- `register`– Enables trap when a Cisco AP registers with a Cisco switch. |
| **Example:** | `Switch(config)# trapflags ap interfaceup` | |
| **Step 3** | `trapflags client \{ dot11 | excluded \}` | Enables sending client-related dot11 traps. Use the `no` form of the command to disable the trap flags.  
- `dot11`– Enables Dot11 traps for clients.  
- `excluded`– Enables excluded traps for clients. |
| **Example:** | `Switch(config)# trapflags client excluded` | |
| **Step 4** | `trapflags dot11-security \{ ids-sig-attack | wep-decrypt-error \}` | Enables sending 802.11 security-related traps. Use the `no` form of the command to disable the trap flags.  
- `ids-sig-attack`– Enables IDS signature attack traps.  
- `wep-decrypt-error`– Enables traps for WEP decrypt error for clients. |
| **Example:** | `Switch(config)# trapflags dot11-security ids-sig-attack wep-decrypt-error` | |
| **Step 5** | `trapflags mesh` | Enables trap for the mesh. Use the `no` form of the command to disable the trap flags. |
| **Example:** | `Switch(config)# trapflags mesh` | |
| **Step 6** | `trapflags rogueap` | Enables trap for rogue AP detection. Use the `no` form of the command to disable the trap flags. |
| **Example:** | `Switch(config)# trapflags rogueap` | |
| **Step 7** | `trapflags rrm-params \{ channels | tx-power \}` | Enables sending RRM-parameter update-related traps. Use the `no` form of the command to disable the trap flags.  
- `channels`– Enables trap when RF Manager automatically changes a channel number for the Cisco AP interface.  
- `tx-power`– Enables the trap when RF Manager automatically changes Tx-Power level for the Cisco AP interface. |
| **Example:** | `Switch(config)# trapflags rrm-params channels tx-power` | |
Enabling SNMP Wireless Trap Notification

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>config terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# config terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>snmp-server enable traps wireless [AP</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# snmp-server enable traps wireless AP</td>
</tr>
</tbody>
</table>

Enables SNMP wireless trap notification.

  * AP– Enables access point traps.
  * RRM– Enables RRM traps.
  * bsn80211SecurityTrap– Enables the security-related trap.
  * bsnAPParamUpdate– Enables the trap for AP parameters that get updated.
  * bsnAPProfile– Enables BSN AP profile traps.
Monitoring 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. You also can use the other privileged EXEC commands listed in the table to display SNMP information.

**Table 29: Commands for Displaying SNMP Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show snmp</code></td>
<td>Displays SNMP statistics.</td>
</tr>
<tr>
<td><code>show snmp engineID</code></td>
<td>Displays information on the local SNMP engine and all remote engines that have been configured on the device.</td>
</tr>
<tr>
<td><code>show snmp group</code></td>
<td>Displays information on each SNMP group on the network.</td>
</tr>
<tr>
<td><code>show snmp pending</code></td>
<td>Displays information on pending SNMP requests.</td>
</tr>
<tr>
<td><code>show snmp sessions</code></td>
<td>Displays information on the current SNMP sessions.</td>
</tr>
</tbody>
</table>
Purpose

Command

show snmp user

Displays information on each SNMP user name in the SNMP users table.

Note

You must use this command to display SNMPv3 configuration information for auth | noauth | priv mode. This information is not displayed in the show running-config output.

Related Topics

- Disabling the SNMP Agent, on page 439
- SNMP Agent Functions, on page 436
- Configuring SNMP Groups and Users, on page 443
- SNMP Configuration Guidelines, on page 439
- Configuring SNMP Notifications, on page 446
- SNMP Notifications, on page 438

SNMP Examples

This example shows how to enable all versions of SNMP. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string public. This configuration does not cause the switch to send any traps.

Switch(config)# snmp-server community public

This example shows how to permit any SNMP manager to access all objects with read-only permission using the community string public. The switch also sends VTP traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string public is sent with the traps.

Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(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 using the community string public.

Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(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 switch 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.

Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
This example shows how to enable the switch to send all traps to the host `myhost.cisco.com` using the community string `public`:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

This example shows how to associate a user with a remote host and to send auth (authNoPriv) authentication-level informs when the user enters global configuration mode:

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Commands</td>
<td><em>Network Management Command Reference, Cisco IOS XE Release 3E</em></td>
</tr>
</tbody>
</table>

#### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

#### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>-</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information for Simple Network Management Protocol

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Feature History and Information for Simple Network Management Protocol
CHAPTER 34

Configuring Service Level Agreements

This chapter describes how to use Cisco IOS IP Service Level Agreements (SLAs) on the switch.

Unless otherwise noted, the term switch refers to a standalone switch or a switch stack.

- Finding Feature Information, on page 461
- Restrictions on SLAs, on page 461
- Information About SLAs, on page 462
- How to Configure IP SLAs Operations, on page 467
- Monitoring IP SLA Operations, on page 480
- Monitoring IP SLA Operation Examples, on page 481
- Additional References, on page 481
- Feature History and Information for Service Level Agreements, on page 483

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions on SLAs

This section lists the restrictions on SLAs.

The following are restrictions on IP SLAs network performance measurement:

- The switch does not support VoIP service levels using the gatekeeper registration delay operations measurements.

- Only a Cisco IOS device can be a source for a destination IP SLAs responder.

- You cannot configure the IP SLAs responder on non-Cisco devices and Cisco IOS IP SLAs can send operational packets only to services native to those devices.
Information About SLAs

Cisco IOS IP Service Level Agreements (SLAs)

Cisco IOS IP SLAs send data across the network to measure performance between multiple network locations or across multiple network paths. They simulate network data and IP services and collect network performance information in real time. Cisco IOS IP SLAs generate and analyze traffic either between Cisco IOS devices or from a Cisco IOS device to a remote IP device such as a network application server. Measurements provided by the various Cisco IOS IP SLA operations can be used for troubleshooting, for problem analysis, and for designing network topologies.

Depending on the specific Cisco IOS IP SLA operations, various network performance statistics are monitored within the Cisco device and stored in both command-line interface (CLI) and Simple Network Management Protocol (SNMP) MIBs. IP SLA packets have configurable IP and application layer options such as source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), Virtual Private Network (VPN) routing/forwarding instance (VRF), and URL web address.

Because Cisco IP SLAs are Layer 2 transport independent, you can configure end-to-end operations over disparate networks to best reflect the metrics that an end user is likely to experience. IP SLAs support the use of Cisco Mediatrace and Cisco Performance Monitor to collect and analyze the following performance metrics:

- Delay (both round-trip and one-way)
- Jitter (directional)
- Packet loss (directional)
- Packet sequencing (packet ordering)
- Path (per hop)
- Connectivity (directional)
- Server or website download time

Additionally, the switch also supports Cisco Medianet to enable intelligent services in the network infrastructure for a wide variety of video applications. Cisco Medianet supports the auto-provisioning of endpoints offering video conferencing services and of IP Surveillance cameras through Auto Smartports.

Cisco Mediatrace and Cisco Performance Monitor can be used on switches running the IP Base image or the IP Services image.

Because Cisco IOS IP SLAs is SNMP-accessible, it can also be used by performance-monitoring applications like Cisco Prime Internetwork Performance Monitor (IPM) and other third-party Cisco partner performance management products.

Using IP SLAs can provide the following benefits:
• Service-level agreement monitoring, measurement, and verification.

• Network performance monitoring
  • Measurement of jitter, latency, or packet loss in the network.
  • Continuous, reliable, and predictable measurements.

• IP service network health assessment to verify that the existing QoS is sufficient for new IP services.

• Edge-to-edge network availability monitoring for proactive verification and connectivity testing of network resources (for example, shows the network availability of an NFS server used to store business critical data from a remote site).

• Network operation troubleshooting by providing consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.

• Multiprotocol Label Switching (MPLS) performance monitoring and network verification (if the switch supports MPLS).

**Network Performance Measurement with Cisco IOS IP SLAs**

You can use IP SLAs to monitor the performance between any area in the network—core, distribution, and edge—without deploying a physical probe. It uses generated traffic to measure network performance between two networking devices.

*Figure 32: Cisco IOS IP SLAs Operation*

The following figure shows how IP SLAs begin when the source device sends a generated packet to the destination device. After the destination device receives the packet, depending on the type of IP SLAs operation, it responds with time-stamp information for the source to make the calculation on performance metrics. An IP SLAs operation performs a network measurement from the source device to a destination in the network using a specific protocol such as UDP.

**Related Topics**

- Implementing IP SLA Network Performance Measurement, on page 469
- Restrictions on SLAs, on page 461
IP SLA Responder and IP SLA Control Protocol

The IP SLA responder is a component embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLA request packets. The responder provides accurate measurements without the need for dedicated probes. The responder uses the Cisco IOS IP SLA Control Protocol to provide a mechanism through which it can be notified on which port it should listen and respond.

Note

The IP SLA responder can be a Cisco IOS Layer 2, responder-configurable switch. The responder does not need to support full IP SLA functionality.

The following figure shows where the Cisco IOS IP SLA responder fits in the IP network. The responder listens on a specific port for control protocol messages sent by an IP SLA operation. Upon receipt of the control message, it enables the specified UDP or TCP port for the specified duration. During this time, the responder accepts the requests and responds to them. It disables the port after it responds to the IP SLA packet, or when the specified time expires. MD5 authentication for control messages is available for added security.

**Figure 33: Cisco IOS IP SLAs Operation**

You do not need to enable the responder on the destination device for all IP SLA operations. For example, a responder is not required for services that are already provided by the destination router (such as Telnet or HTTP).

**Related Topics**

*Restrictions on SLAs*, on page 461

Response Time Computation for IP SLAs

Switches, controllers, and routers can take tens of milliseconds to process incoming packets due to other high priority processes. This delay affects the response times because the test-packet reply might be in a queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays. IP SLAs minimize these processing delays on the source device as well as on the target device (if the responder is being used) to determine true round-trip times. IP SLA test packets use time stamping to minimize the processing delays.

When the IP SLA responder is enabled, it allows the target device to take time stamps when the packet arrives on the interface at interrupt level and again just as it is leaving, eliminating the processing time. This time stamping is made with a granularity of sub-milliseconds (ms).
The following figure demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target router, with the responder functionality enabled, time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source router where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy.

\[
RTT \text{ (Round-trip time)} = T4 \text{ (Time stamp 4)} - T1 \text{ (Time stamp 1)} - \Delta
\]

An additional benefit of the two time stamps at the target device is the ability to track one-way delay, jitter, and directional packet loss. Because much network behavior is asynchronous, it is critical to have these statistics. However, to capture one-way delay measurements, you must configure both the source router and target router with Network Time Protocol (NTP) so that the source and target are synchronized to the same clock source. One-way jitter measurements do not require clock synchronization.

**IP SLAs Operation Scheduling**

When you configure an IP SLAs operation, you must schedule the operation to begin capturing statistics and collecting error information. You can schedule an operation to start immediately or to start at a certain month, day, and hour. You can use the `pending` option to set the operation to start at a later time. The pending option is an internal state of the operation that is visible through SNMP. The pending state is also used when an operation is a reaction (threshold) operation waiting to be triggered. You can schedule a single IP SLAs operation or a group of operations at one time.

You can schedule several IP SLAs operations by using a single command through the Cisco IOS CLI or the CISCO RTTMON-MIB. Scheduling the operations to run at evenly distributed times allows you to control the amount of IP SLAs monitoring traffic. This distribution of IP SLA operations helps minimize the CPU utilization and thus improves network scalability.

For more details about the IP SLA multi-operations scheduling functionality, see the “IP SLAs—Multiple Operation Scheduling” chapter of the *Cisco IOS IP SLAs Configuration Guide*.

**IP SLA Operation Threshold Monitoring**

To support successful service level agreement monitoring, you must have mechanisms that notify you immediately of any possible violation. IP SLAs can send SNMP traps that are triggered by events such as the following:

- Connection loss
- Timeout
- Round-trip time threshold
- Average jitter threshold
- One-way packet loss
• One-way jitter
• One-way mean opinion score (MOS)
• One-way latency

An IP SLA threshold violation can also trigger another IP SLA operation for further analysis. For example, the frequency could be increased or an Internet Control Message Protocol (ICMP) path echo or ICMP path jitter operation could be initiated for troubleshooting.

**ICMP Echo**

The ICMP echo operation measures the end-to-end response time between a Cisco device and any other device that uses IP. The response time is computed by measuring the time it takes to send an ICMP echo request message to a destination and receive an ICMP echo reply. Many customers use IP SLA ICMP-based operations, in-house ping testing, or ping-based dedicated probes to measure this response time. The IP SLA ICMP echo operation conforms to the same specifications as ICMP ping testing, and both methods result in the same response times.

**Related Topics**

Analyzing IP Service Levels by Using the ICMP Echo Operation, on page 477

**UDP Jitter**

Jitter is a simple term that describes interpacket delay variance. When multiple packets are sent consecutively at an interval of 10 ms from source to destination, the destination should receive them 10 ms apart (if the network is behaving correctly). However, if there are delays in the network (such as queuing, arriving through alternate routes, and so on), the time interval between packet arrivals might be more or less than 10 ms. A positive jitter value indicates that the packets arrived more than 10 ms apart. A negative jitter value indicates that the packets arrived less than 10 ms apart. If the packets arrive 12 ms apart, the positive jitter is 2 ms; if the packets arrive 8 ms apart, the negative jitter is 2 ms. For delay-sensitive networks, positive jitter values are undesirable, and a jitter value of 0 is ideal.

In addition to monitoring jitter, the IP SLA UDP jitter operation can be used as a multipurpose data gathering operation. The packets generated by IP SLAs carry sequence information and time stamps from the source and operational target that include packet sending and receiving data. Based on this data, UDP jitter operations measure the following:

• Per-direction jitter (source to destination and destination to source)
• Per-direction packet-loss
• Per-direction delay (one-way delay)
• Round-trip delay (average round-trip time)

Because the paths for the sending and receiving of data can be different (asymmetric), you can use the per-direction data to more readily identify where congestion or other problems are occurring in the network.

The UDP jitter operation generates synthetic (simulated) UDP traffic and sends a number of UDP packets, each of a specified size, sent a specified number of milliseconds apart, from a source router to a target router, at a given frequency. By default, ten packet-frames, each with a payload size of 10 bytes are generated every 10 ms, and the operation is repeated every 60 seconds. You can configure each of these parameters to best simulate the IP service you want to provide.
To provide accurate one-way delay (latency) measurements, time synchronization (as provided by NTP) is required between the source and the target device. Time synchronization is not required for the one-way jitter and packet loss measurements. If the time is not synchronized between the source and target devices, one-way jitter and packet loss data is returned, but values of 0 are returned for the one-way delay measurements provided by the UDP jitter operation.

**Related Topics**
- Analyzing IP Service Levels by Using the UDP Jitter Operation, on page 473

# How to Configure IP SLAs Operations

This section does not include configuration information for all available operations as the configuration information details are included in the *Cisco IOS IP SLAs Configuration Guide*. It does include several operations as examples, including configuring the responder, configuring a UDP jitter operation, which requires a responder, and configuring an ICMP echo operation, which does not require a responder. For details about configuring other operations, see the *Cisco IOS IP SLAs Configuration Guide*.

## Default Configuration

No IP SLAs operations are configured.

## Configuration Guidelines

For information on the IP SLA commands, see the *Cisco IOS IP SLAs Command Reference, Release 12.4T* command reference.

For detailed descriptions and configuration procedures, see the *Cisco IOS IP SLAs Configuration Guide, Release 12.4TL*.

Not all of the IP SLA commands or operations described in the referenced guide are supported on the switch. The switch supports IP service level analysis by using UDP jitter, UDP echo, HTTP, TCP connect, ICMP echo, ICMP path echo, ICMP path jitter, FTP, DNS, and DHCP, as well as multiple operation scheduling and proactive threshold monitoring. It does not support VoIP service levels using the gatekeeper registration delay operations measurements.

Before configuring any IP SLAs application, you can use the `show ip sla application` privileged EXEC command to verify that the operation type is supported on your software image. This is an example of the output from the command:

```
Switch# show ip sla application

   IP Service Level Agreements
   Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

   Supported Operation Types:
   icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
dns, udpJitter, dhcp, ftp, udpApp, wspApp

   Supported Features:
   IPSLAs Event Publisher

   IP SLAs low memory water mark: 33299323
   Estimated system max number of entries: 24389
```
Estimated number of configurable operations: 24389
Number of Entries configured : 0
Number of active Entries : 0
Number of pending Entries : 0
Number of inactive Entries : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012

Configuring the IP SLA Responder

The IP SLA responder is available only on Cisco IOS software-based devices, including some Layer 2 switches that do not support full IP SLA functionality.

Follow these steps to configure the IP SLA responder on the target device (the operational target):

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
**Example:**  
Switch> enable |  
* Enter your password if prompted. |
| Step 2 | configure terminal | Enters global configuration mode.  
**Example:**  
Switch# configure terminal | |
| Step 3 | ip sla responder {tcp-connect | udp-echo}  
ipaddress ip-address port port-number | Configures the switch as an IP SLA responder.  
The keywords have these meanings:  
* tcp-connect—Enables the responder for TCP connect operations.  
* udp-echo—Enables the responder for User Datagram Protocol (UDP) echo or jitter operations.  
* ipaddress ip-address—Enter the destination IP address.  
* port port-number—Enter the destination port number.  
**Note**  
The IP address and port number must match those configured on the source device for the IP SLA operation.  
**Example:**  
Switch(config)# ip sla responder udp-echo  
172.29.139.134 5000 |
## Implementing IP SLA Network Performance Measurement

Follow these steps to implement IP SLA network performance measurement on your switch:

**Before you begin**

Use the `show ip sla application` privileged EXEC command to verify that the desired operation type is supported on your software image.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip sla operation-number</td>
<td>Creates an IP SLA operation, and enters IP SLA configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# ip sla operation-number</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

`Switch(config)# ip sla 10`

**Purpose**

Configures the IP SLA operation as the operation type of your choice (a UDP jitter operation is used in the example), and enters its configuration mode (UDP jitter configuration mode is used in the example).

- **destination-ip-address | destination-hostname**—Specifies the destination IP address or hostname.
- **destination-port**—Specifies the destination port number in the range from 1 to 65535.
- **source-ip {ip-address | hostname}**—Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLA chooses the IP address nearest to the destination.
- **source-port port-number**—Specifies the source port number in the range from 1 to 65535. When a port number is not specified, IP SLA chooses an available port.
- **control {enable | disable}**—Enables or disables sending of IP SLA control messages to the IP SLA responder. By default, IP SLA control messages are sent to the destination device to establish a connection with the IP SLA responder.
- **num-packets number-of-packets**—Enters the number of packets to be generated. The range is 1 to 6000; the default is 10.
- **interval inter-packet-interval**—Enters the interval between sending packets in milliseconds. The range is 1 to 6000; the default value is 20 ms.

### Step 4

**udp-jitter {destination-ip-address | destination-hostname} destination-port [source-ip {ip-address | hostname}] [source-port port-number] [control {enable | disable}] [num-packets number-of-packets] [interval inter-packet-interval]**

**Example:**

`Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000`

### Step 5

**frequency seconds**

**Example:**

(Optional) Configures options for the SLA operation. This example sets the rate at which a specified IP SLA operation repeats. The
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config-ip-sla-jitter)# frequency 45</code></td>
<td><code>range is from 1 to 604800 seconds; the default is 60 seconds.</code></td>
</tr>
</tbody>
</table>

### Step 6

**threshold milliseconds**

**Example:**

`Switch(config-ip-sla-jitter)# threshold 200`

(Optional) Configures threshold conditions. This example sets the threshold of the specified IP SLA operation to 200. The range is from 0 to 60000 milliseconds.

### Step 7

**exit**

**Example:**

`Switch(config-ip-sla-jitter)# exit`

Exits the SLA operation configuration mode (UDP jitter configuration mode in this example), and returns to global configuration mode.

### Step 8

**ip sla schedule operation-number**

<table>
<thead>
<tr>
<th>life</th>
<th>start-time</th>
<th>ageout seconds</th>
<th>recurring</th>
</tr>
</thead>
</table>
| `{forever | seconds}` | `{hh:mm [ss]} | [month day | day month] | pending | now | after `hh:mm:ss` | [ageout seconds] | [recurring]

**Example:**

`Switch(config)# ip sla schedule 10 start-time now life forever`

Configures the scheduling parameters for an individual IP SLA operation.

- **operation-number**—Enter the RTR entry number.

- (Optional) **life**—Sets the operation to run indefinitely (forever) or for a specific number of seconds. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour).

- (Optional) **start-time**—Enters the time for the operation to begin collecting information:

  To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month.

  Enter **pending** to select no information collection until a start time is selected.

  Enter **now** to start the operation immediately.

  Enter **after hh:mm:ss** to show that the operation should start after the entered time has elapsed.

- (Optional) **ageout seconds**—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2073600 seconds, the default is 0 seconds (never ages out).</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <strong>recurring</strong>—Set the operation to automatically run every day.</td>
</tr>
</tbody>
</table>

**Step 9**

**Example:**

```
Switch(config)# end
```

Returns to privileged EXEC mode.

**Step 10**

**Example:**

```
Switch# show running-config
```

Verifies your entries.

**Step 11**

**Example:**

```
Switch# copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

---

**UDP Jitter Configuration**

This example shows how to configure a UDP jitter IP SLA operation:

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
```

IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
  Operation frequency (seconds): 30
Analyzing IP Service Levels by Using the UDP Jitter Operation

Follow these steps to configure a UDP jitter operation on the source device:

Before you begin
You must enable the IP SLA responder on the target device (the operational target) to configure a UDP jitter operation on the source device.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
| enable            | Enables privileged EXEC mode.  
| **Example:**      | • Enter your password if prompted.  
| Switch> enable    |         |
| **Step 2**        |         |
| configure terminal| Enters global configuration mode. |
| **Example:**      |         |
| Switch# configure terminal | | |
| **Step 3**        |         |
| ip sla operation-number | Creates an IP SLA operation, and enters IP SLA configuration mode. |
| **Example:**      |         |
| Switch(config)# ip sla 10 | | |
| **Step 4**        |         |
| udp-jitter {destination-ip-address | Configures the IP SLA operation as a UDP jitter operation, and enters UDP jitter configuration mode.  
<p>| destination-hostname} destination-port |         |
| {source-ip {ip-address |         |
| hostname}} |         |
| {source-port port-number} |         |
| [control {enable} |         |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Table content" /></td>
<td><img src="image" alt="Table content" /></td>
</tr>
</tbody>
</table>

**Step 5**

**frequency seconds**

**Example:**

```
Switch(config-ip-sla-jitter)# frequency 45
```

(Optional) Sets the rate at which a specified IP SLA operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.

**Step 6**

**exit**

**Example:**

```
Switch(config-ip-sla-jitter)# exit
```

Exits UDP jitter configuration mode, and returns to global configuration mode.
### Command or Action

| Step 7 | Command: `ip sla schedule operation-number [life {forever | seconds}] [start-time {hh:mm [:ss] [month day | day month] | pending | now | after hh:mm:ss} [ageout seconds] [recurring]}]` | Purpose: Configures the scheduling parameters for an individual IP SLA operation.  
- **operation-number**—Enter the RTR entry number.  
- (Optional) **life**—Sets the operation to run indefinitely (forever) or for a specific number of seconds. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour).  
- (Optional) **start-time**—Enters the time for the operation to begin collecting information:  
  To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month.  
  Enter **pending** to select no information collection until a start time is selected.  
  Enter **now** to start the operation immediately.  
  Enter **after hh:mm:ss** to show that the operation should start after the entered time has elapsed.  
- (Optional) **ageout seconds**—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds, the default is 0 seconds (never ages out).  
- (Optional) **recurring**—Set the operation to automatically run every day.  

#### Example:

Switch(config)# ip sla schedule 10 start-time now life forever

| Step 8 | Command: `end` | Purpose: Returns to privileged EXEC mode.  

#### Example:

Switch(config)# end

| Step 9 | Command: `show running-config` | Purpose: Verifies your entries.  

#### Example:

Switch# show running-config
### Configuring a UDP Jitter IP SLA Operation

This example shows how to configure a UDP jitter IP SLA operation:

```plaintext
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10

IP SLAs, Infrastructure Engine-II.
Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

### Related Topics

- [UDP Jitter](#), on page 466
## Analyzing IP Service Levels by Using the ICMP Echo Operation

Follow these steps to configure an ICMP echo operation on the source device:

### Before you begin

This operation does not require the IP SLA responder to be enabled.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
  Example:  
  `Switch> enable` |
| Step 2 | `configure terminal` | Enters global configuration mode.  
  Example:  
  `Switch# configure terminal` |
| Step 3 | `ip sla operation-number` | Creates an IP SLA operation and enters IP SLA configuration mode.  
  Example:  
  `Switch(config)# ip sla 10` |
| Step 4 | `icmp-echo {destination-ip-address |  
  destination-hostname} [source-ip {ip-address  
  | hostname} | source-interface interface-id]` | Configures the IP SLA operation as an ICMP Echo operation and enters ICMP echo configuration mode.  
  Example:  
  `Switch(config-ip-sla)# icmp-echo 172.29.139.134` |

- **destination-ip-address | destination-hostname**—Specifies the destination IP address or hostname.
- **(Optional) source-ip {ip-address | hostname}**—Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLA chooses the IP address nearest to the destination.
- **(Optional) source-interface interface-id**—Specifies the source interface for the operation.
### Analyzing IP Service Levels by Using the ICMP Echo Operation

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Sets the rate at which a specified IP SLA operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.</td>
</tr>
<tr>
<td><code>frequency seconds</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;<code>Switch(config-ip-sla-echo)# frequency 30</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Exits UDP echo configuration mode, and returns to global configuration mode.</td>
</tr>
<tr>
<td><code>exit</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;<code>Switch(config-ip-sla-echo)# exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Configures the scheduling parameters for an individual IP SLA operation.</td>
</tr>
<tr>
<td>`ip sla schedule operation-number [life {forever</td>
<td>seconds}] [start-time {hh:mm [:ss]</td>
</tr>
<tr>
<td>• <strong>operation-number</strong>—Enter the RTR entry number.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>life</strong>—Sets the operation to run indefinitely (forever) or for a specific number of seconds. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour)</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>start-time</strong>—Enter the time for the operation to begin collecting information:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month.</td>
</tr>
<tr>
<td></td>
<td>Enter <strong>pending</strong> to select no information collection until a start time is selected.</td>
</tr>
<tr>
<td></td>
<td>Enter <strong>now</strong> to start the operation immediately.</td>
</tr>
<tr>
<td></td>
<td>Enter <strong>after hh:mm:ss</strong> to indicate that the operation should start after the entered time has elapsed.</td>
</tr>
<tr>
<td>• (Optional) <strong>ageout seconds</strong>—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds; the default is 0 seconds (never ages out).</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>recurring</strong>—Sets the operation to automatically run every day.</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>Command or Action</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show running-config</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring an ICMP Echo IP SLA Operation**

This example shows how to configure an ICMP echo IP SLA operation:

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 172.29.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 22
```

IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
  Operation frequency (seconds): 60
  Next Scheduled Start Time: Pending trigger
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): 3600
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 1
Statistic distribution interval (milliseconds): 20
History Statistics:
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Enhanced History:

Related Topics
IP SLA Operation Threshold Monitoring, on page 465

Monitoring IP SLA Operations

The following table describes the commands used to display IP SLA operation configurations and results:

**Table 30: Monitoring IP SLA Operations**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip sla application</code></td>
<td>Displays global information about Cisco IOS IP SLAs.</td>
</tr>
<tr>
<td><code>show ip sla authentication</code></td>
<td>Displays IP SLA authentication information.</td>
</tr>
<tr>
<td><code>show ip sla configuration [entry-number]</code></td>
<td>Displays configuration values including all defaults for all IP SLA operations or a specific operation.</td>
</tr>
<tr>
<td>`show ip sla enhanced-history {collection-statistics</td>
<td>distribution statistics} [entry-number]`</td>
</tr>
<tr>
<td><code>show ip sla ethernet-monitor configuration [entry-number]</code></td>
<td>Displays IP SLA automatic Ethernet configuration.</td>
</tr>
<tr>
<td><code>show ip sla group schedule [schedule-entry-number]</code></td>
<td>Displays IP SLA group scheduling configuration and details.</td>
</tr>
<tr>
<td>`show ip sla history [entry-number</td>
<td>full</td>
</tr>
<tr>
<td>`show ip sla mpls-lsp-monitor {collection-statistics</td>
<td>configuration</td>
</tr>
<tr>
<td><code>show ip sla reaction-configuration [entry-number]</code></td>
<td>Displays the configured proactive threshold monitoring settings for all IP SLA operations or a specific operation.</td>
</tr>
<tr>
<td><code>show ip sla reaction-trigger [entry-number]</code></td>
<td>Displays the reaction trigger information for all IP SLA operations or a specific operation.</td>
</tr>
<tr>
<td><code>show ip sla responder</code></td>
<td>Displays information about the IP SLA responder.</td>
</tr>
<tr>
<td>`show ip sla statistics [entry-number</td>
<td>aggregated</td>
</tr>
</tbody>
</table>
Monitoring IP SLA Operation Examples

The following example shows all IP SLAs by application:

```
Switch# show ip sla application

IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
  icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
  IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389

Estimated number of configurable operations: 24389
Number of Entries configured : 0
Number of active Entries : 0
Number of pending Entries : 0
Number of inactive Entries : 0
Time of last change in whole IP SLAs: 13:04:37.668 UTC Wed Dec 19 2012

The following example shows all IP SLA distribution statistics:

Switch# show ip sla enhanced-history distribution-statistics

Point by point Enhanced History
Entry - Entry Number
Int - Aggregation Interval
BucI - Bucket Index
StartT - Aggregation Start Time
Pth - Path index
Hop - Hop in path index
Comps - Operations completed
OvrTh - Operations completed over thresholds
SumCmp - Sum of RTT (milliseconds)
SumCmp2L - Sum of RTT squared low 32 bits (milliseconds)
SumCmp2H - Sum of RTT squared high 32 bits (milliseconds)
TMax - RTT maximum (milliseconds)
TMin - RTT minimum (milliseconds)

Entry Int BucI StartT Pth Hop Comps OvrTh SumCmp SumCmp2L SumCmp2H T Max TMin

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>
### Related Topic

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Description</th>
</tr>
</thead>
</table>

### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>-</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
Feature History and Information for Service Level Agreements

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 35

Configuring Local Policies

• Finding Feature Information, on page 485
• Restrictions for Configuring Local Policies, on page 485
• Information About Configuring Local Policies, on page 486
• How to Configure Local Policies, on page 487
• Monitoring Local Policies, on page 496
• Examples: Local Policies Configuration, on page 497
• Additional References for Configuring Local Policies, on page 499
• Feature History for Performing Local Policies Configuration, on page 499

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring Local Policies

• The policy map attributes supported on the switch are QoS, VLAN, session timeout, and ACL.

• Apple iphone 6s will get classified as "workstation" after HTTP profiling.

Related Topics

Creating a Parameter Map (CLI), on page 489
Creating a Class Map (CLI), on page 491
Creating a Policy Map (CLI), on page 491
Applying a Local Policy for a Device on a WLAN (CLI), on page 492
Creating an Interface Template (CLI), on page 489
Information About Configuring Local Policies, on page 486
Creating a Service Template (GUI), on page 494
Information About Configuring Local Policies

Local policies can profile devices based on HTTP and DHCP to identify the end devices on the network. Users can configure device-based policies and enforce the policies per user or per device policy on the network. Local policies allow profiling of mobile devices and basic onboarding of the profiled devices to a specific VLAN. They also assign ACL and QoS or configure session timeouts. You can configure local policies as two separate components:

- Defining policy attributes as service templates specific to clients joining the network and applying policy match criteria.
- Applying match criteria to the policy.

The following policy match attributes are used for configuring local policies:

- **Device**—Defines the type of device. Windows-based computer, Smart phone, Apple devices such as iPad and iPhone.
- **Username**—Defines the username of the user.
- **User role**—Defines the user type or the user group the user belongs to, such as a student or employee.
- **MAC**—Defines the mac-address of the endpoint.
- **MAC OUI**—Defines the mac-address OUI.

Once the switch has a match corresponding to these parameters per end point, the policy can be added. Policy enforcement allows basic device on-boarding of mobile devices based on the following session attributes:

- VLAN
- QoS
- ACL
- Session timeout

You can configure these policies and enforce endpoints with specified policies. The wireless clients are profiled based on MAC OUI, DHCP, and HTTP user agent (valid Internet is required for successful HTTP profiling) MAC OUI and DHCP. The switch uses these attributes and predefined classification profiles to identify devices.

**Replacing Default Profile Text File**

If a new device is not classified, contact the Cisco support team with the device MAC address. The Cisco support team will provide a new `dc_default_profile.txt` file with the MAC address included in the file. You need to replace the `dc_default_profile.txt` file with the earlier file. Follow these steps to change the `dc_default_profile.txt` file:

1. Stop device classifier by entering this command:

   ```
   switch(config)# no device classifier
   ```
How to Configure Local Policies

Configuring Local Policies (CLI)

To configure local policies, complete these procedures:

1. Create a service template.
2. Create an interface template.
3. Create a parameter map.
4. Create a policy map.
5. Apply a local policy on a WLAN.
## Creating a Service Template (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>service-template service-template-name</code></td>
<td>Enters service template configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# service-template</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cisco-phone-template</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-service-template)#</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>access-group acl_list</code></td>
<td>Specifies the access list to be applied.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-service-template)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>access-group foo-acl</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>vlan vlan_id</code></td>
<td>Specifies VLAN ID. You can specify a value from 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-service-template)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan 100</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>absolute-timer seconds</code></td>
<td>Specifies session timeout value for service template. You can specify a value from 1 to 65535.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-service-template)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>absolute-timer 20</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>`service-policy qos {input</td>
<td>output}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-service-template)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>service-policy qos input foo-qos</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
# Creating an Interface Template (CLI)

## Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>template interface-template-name</code></td>
<td>Enters interface template configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# template cisco-phone-template</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-template)#</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>switchport mode access</code></td>
<td>Sets the interface as a nontrunking nontagged single-VLAN Ethernet interface. An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN1.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-template)# switchport mode access</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>switchport voice vlan vlan_id</code></td>
<td>Specifies to forward all voice traffic through the specified VLAN. You can specify a value from 1 to 4094.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-template)# switchport voice vlan 20</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

## Related Topics
- Information About Configuring Local Policies, on page 486
- Restrictions for Configuring Local Policies, on page 485
- Monitoring Local Policies, on page 496
- Examples: Local Policies Configuration, on page 497

---

# Creating a Parameter Map (CLI)

Parameter map is preferred to use than class map.

## Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
</tr>
</tbody>
</table>

### Purpose

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the parameter map type and name.</td>
</tr>
</tbody>
</table>

### Step 2

<table>
<thead>
<tr>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>parameter-map type subscriber attribute-to-service parameter-map-name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para</td>
</tr>
</tbody>
</table>

### Step 3

<table>
<thead>
<tr>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>map-index map ( device-type</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-parameter-map-filter)# 10 map device-type eq &quot;WindowsXP-Workstation&quot;</td>
</tr>
</tbody>
</table>

### Step 4

<table>
<thead>
<tr>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>service-template service-template-name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-parameter-map-filter-submode)# service-template cisco-phone-template Switch(config-parameter-map-filter-submode)#</td>
</tr>
</tbody>
</table>

### Step 5

<table>
<thead>
<tr>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-template interface-template-name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-parameter-map-filter-submode)# interface-template cisco-phone-template Switch(config-parameter-map-filter-submode)#</td>
</tr>
</tbody>
</table>

### Step 6

<table>
<thead>
<tr>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# end</td>
</tr>
</tbody>
</table>

### Related Topics

- [Information About Configuring Local Policies](#), on page 486
- [Restrictions for Configuring Local Policies](#), on page 485
- [Monitoring Local Policies](#), on page 496
- [Examples: Local Policies Configuration](#), on page 497
### Creating a Class Map (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
| **Step 2** | `class-map type control subscriber`  
`class-map-name { match-all | match-any | match-first }` | Specifies the class map type and name. |
|    | Example: `Switch(config)# class-map type control subscriber CLASS_AC_1 match-all` | |
| **Step 3** | `match { device-type | mac-address | oui | username | userrole } filter-type-name` | Specifies class map attribute filter criteria. |
|    | Example: `Switch(config-class-map)# match device-type Cisco-IP-Phone-7961` | |
| **Step 4** | `end` | Returns to privileged EXEC mode. Alternatively, you can also press `Ctrl-Z` to exit global configuration mode. |
|    | Example: `Switch(config)# end` | |

**Related Topics**
- Information About Configuring Local Policies, on page 486
- Restrictions for Configuring Local Policies, on page 485
- Monitoring Local Policies, on page 496
- Examples: Local Policies Configuration, on page 497

### Creating a Policy Map (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
| **Step 2** | `policy-map type control subscriber`  
`policy-map-name` | Specifies the policy map type. |
|    | Example: | |
### Applying a Local Policy for a Device on a WLAN (CLI)

#### Before you begin

If the service policy contains any device type-based rules in the parameter map, ensure that the device classifier is already enabled.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# policy-map type control subscriber Aironet-Policy</code></td>
<td></td>
</tr>
</tbody>
</table>

#### Step 3

**event identity-update { match-all | match-first }**

**Example:**

```
Switch(config-policy-map)# event identity-update match-all
```

- Specifies match criteria to the policy map.

#### Step 4

```
class_number class { class_map_name | always } { do-all | do-until-failure | do-until-success }
```

**Example:**

```
Switch(config-class-control-policymap)# 1 class local_policy1_class do-until-success
```

- Configures the local profiling policy class map number and specifies how to perform the action.

- The class map configuration mode includes the following command options:
  - **always** — Executes without doing any matching but return success.
  - **do-all** — Executes all the actions.
  - **do-until-failure** — Execute all the actions until any match failure is encountered. This is the default value.
  - **do-until-success** — Execute all the actions until any match success happens.

#### Step 5

```
action-index map attribute-to-service table parameter-map-name
```

**Example:**

```
Switch(config-policy-map)# 10 map attribute-to-service table Aironet-Policy-para
```

- Specifies parameter map table to be used.

#### Step 6

```
end
```

**Example:**

```
Switch(config)# end
```

- Returns to privileged EXEC mode.
- Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

---

**Related Topics**

- Information About Configuring Local Policies, on page 486
- Restrictions for Configuring Local Policies, on page 485
- Monitoring Local Policies, on page 496
- Examples: Local Policies Configuration, on page 497

---

---
You should use the **device classification** command to classify the device for it to be displayed correctly on the show command output.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wlan wlan-name</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config)# wlan wlan1</code></td>
<td>Enters WLAN configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>service-policy type control subscriber policymapname</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config-wlan)# service-policy type control subscriber Aironet-Policy</code></td>
<td>Applies local policy to WLAN.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>profiling local http (optional)</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config-wlan)# profiling local http</code></td>
<td>Enables only profiling of devices based on HTTP protocol (optional).</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>profiling radius http (optional)</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config-wlan)# profiling radius http</code></td>
<td>Enables profiling of devices on ISE (optional).</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>no shutdown</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config-wlan)# no shutdown</code></td>
<td>Specifies not to shut down the WLAN.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>end</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config)# end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit global configuration mode.</td>
</tr>
</tbody>
</table>

### Related Topics

- [Information About Configuring Local Policies](#), on page 486
- [Restrictions for Configuring Local Policies](#), on page 485
- [Monitoring Local Policies](#), on page 496
- [Examples: Local Policies Configuration](#), on page 497
Configuring Local Policies (GUI)

To configure local policies, complete these procedures:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Create a service template.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Create a policy map.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Apply a local policy that you have created to a WLAN.</td>
<td></td>
</tr>
</tbody>
</table>

### Creating a Service Template (GUI)

#### Procedure

1. **Step 1** Choose Configuration > Security > Local Policies > Service Template to open the Service Template page.
2. **Step 2** Create a new template as follows:
   a) Click New to open the Service Template > New page.
   b) In the Service Template name text box, enter the new service template name.
   c) In the VLAN ID text box, enter the VLAN identifier that has to be associated with the policy. The value ranges from 1 to 4094.
   d) In the Session timeout text box, enter the maximum amount of time, in seconds, after which a client is forced to reauthenticate. The value ranges from 1 to 65535 seconds.
   e) From the Access control list drop-down list, choose the access control list to be mapped to the policy.
   f) From the Ingress QoS drop-down list, choose the ingress QoS policy to be applied.
   g) From the Egress QoS drop-down list, choose the egress QoS policy to be applied.
   h) Click Apply to save the configuration.
3. **Step 3** Edit a service template as follows:
   a) From the Service Template page, click the service template to open the Service Template > Edit page.
   b) In the VLAN ID text box, enter the VLAN identifier that has to be associated with the policy. The value ranges from 1 to 4094.
   c) In the Session timeout text box, enter the maximum amount of time, in seconds, after which a client is forced to reauthenticate. The value ranges from 1 to 65535 seconds.
   d) From the Access control list drop-down list, choose the access control list to be mapped to the policy.
   e) From the Ingress QoS drop-down list, choose the ingress QoS policy to be applied.
   f) From the Egress QoS drop-down list, choose the egress QoS policy to be applied.
   g) Click Apply to save the configuration.
4. **Step 4** Remove a service template as follows:
   a) From the Service Template page, select the service template.
   b) Click Remove.
   c) Click Apply to save the configuration.
Creating a Policy Map (GUI)

**Procedure**

**Step 1**  
Choose **Configuration > Security > Local Policies > Policy Map** to open the **Policy Map** page.

**Step 2**  
Create a new policy map as follows:

a) Click **New** to open the **Policy Map > New** page.
b) In the Policy Map name text box, enter the new policy map name.
c) Click **Add** to open the Match Criteria area.
d) From the Device Type drop-down list, choose the device type. The match criteria for the device type can be eq, not-eq, or regex with respect to the device type you are choosing.
e) From the User Role drop-down list, select the match criteria as eq, not-eq, or regex and enter the user type or user group of the user, for example, student, teacher, and so on.
f) From the Service Template drop-down list, choose the service template to be mapped to the policy.
g) Click **Add**. The match criteria is added to the Match Criteria Lists.
h) In the Match Criteria Lists area, click **Add** to add the match criteria to the policy.
i) Click **Apply** to save the configuration.

**Step 3**  
Edit a policy map as follows:

a) In the **Policy Map** page, select the policy map that you want to edit, and click **Edit** to open the **Policy Map > Edit** page.
b) In the Match Criteria area, choose the device type from the Device Type drop-down list. The match criteria for the device type can be eq, not-eq, or regex with respect to the device type you are choosing.
c) In the Match Criteria area, choose the user role from the User Role drop-down list. Select the match criteria as eq, not-eq, or regex and enter the user type or user group of the user.
d) From the Service Template drop-down list, choose the service template to be mapped to the policy.
e) Click **Ok** to save the configuration or **Cancel** to discard the configuration.
f) Click **Add** to add more match criteria based on device type, user role, and service template to the policy.
g) In the Match Criteria Lists area, select the match criteria and click **Move to** to move the match criteria with respect to a value entered in the row text box.
h) Select the match criteria and click **Move up** to move the match criteria up in the list.
i) Select the match criteria and click **Move down** to move the match criteria down in the list.
j) Select the match criteria and click **Remove** to remove the match criteria from the policy map list.
k) Click **Apply** to save the configuration.

**Step 4**  
Remove a policy map as follows:

a) From the **Policy Map** page, select the policy map.
b) Click **Remove**.
c) Click **Apply** to save the configuration.
Applying Local Policies to WLAN (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > WLAN** to open the **WLANs** page.

Step 2 Click the corresponding WLAN profile. The **WLANs > Edit** page is displayed.

Step 3 Click the **Policy-Mapping** tab.

Step 4 Check the **Device Classification** check box to enable classification based on device type.

Step 5 From the Local Subscriber Policy drop-down list, choose the policy that has to be applied for the WLAN.

Step 6 Select **Local HTTP Profiling** to enable profiling on devices based on HTTP (optional).

Step 7 Select **Radius HTTP Profiling** to enable profiling on devices based on RADIUS (optional).

Step 8 Click **Apply** to save the configuration.

Related Topics

- Information About Configuring Local Policies, on page 486
- Restrictions for Configuring Local Policies, on page 485
- Monitoring Local Policies, on page 496
- Examples: Local Policies Configuration, on page 497

Monitoring Local Policies

The following commands can be used to monitor local policies configured on the switch.

**Table 31: Monitoring Local Policies Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show access-session</code></td>
<td>Displays the summary of access session with authorization status, method and domain for each client or MAC address displayed.</td>
</tr>
<tr>
<td><code>show access-session cache</code></td>
<td>Displays the latest classification for the client.</td>
</tr>
<tr>
<td><code>show device classifier attached detail</code></td>
<td>Displays the latest classification for the client based on parameters such as Mac, DHCP, or HTTP.</td>
</tr>
</tbody>
</table>
show access-session mac mac-address details

Displays the policy mapped, service template used, and attributes for the client.

Note
If the show access-session detail command output is not displaying session timeout details, you should enable client profiling with session timeout in client access session and then run the show access-session mac mac-address details command to see the session timeout details.

show access-session mac mac-address policy

Displays the policy mapped, service template used, and attributes for the client.

In addition, you can view the Resultant Policy that displays the following information:

- The final attributes applied to the session when the session has locally configured attributes.
- Attributes applied from the server.

Related Topics

Creating a Parameter Map (CLI), on page 489
Creating a Class Map (CLI), on page 491
Creating a Policy Map (CLI), on page 491
Applying a Local Policy for a Device on a WLAN (CLI), on page 492
Creating an Interface Template (CLI), on page 489
Information About Configuring Local Policies, on page 486
Creating a Service Template (GUI), on page 494
Creating a Policy Map (GUI), on page 495
Applying Local Policies to WLAN (GUI), on page 496

Examples: Local Policies Configuration

This example shows how to create service template:

Switch(config)# service-template test3
Switch(config-service-template)# access-group josephacl
Switch(config-service-template)# vlan 137
Switch(config-service-template)# absolute-timer 500
Switch(config-service-template)# service-policy qos input qosingress
Switch(config-service-template)# end

This example shows how to create parameter map:

Switch(config)# parameter-map type subscriber attribute-to-service apple-tsim-param
Switch(config-parameter-map)# 1 map device-type eq "Apple-Device"
Switch(config-parameter-map)# 1 service-template test1
Switch(config-parameter-map)# 2 map device-type eq "Apple-Ipad"
Switch(config-parameter-map)# 1 service-template test2
Switch(config-parameter-map)# 3 map device-type eq "Android"
Switch(config-parameter-map)# l service-template test3
Switch(config-parameter-map)# end

At the end of each configuration command line, enter CTRL Z to execute the command and proceed to the next line.

This example shows how to create interface template:

Switch# configure terminal
Switch(config)#template cisco-phone-template
Switch(config-template)#switchport mode access
Switch(config-template)#switchport voice vlan 20
Switch(config-template)# end

This example shows how to create parameter map:

Switch# configure terminal
Switch(config)#parameter-map type subscriber attribute-to-service param-wired
Switch(config-parameter-map-filter)#10 map device-type regex Cisco-IP-Phone
Switch(config-parameter-map-filter-submode)#10 interface-template cisco-phone-template
Switch(config-parameter-map)# end

This example shows how to create policy map:

Switch(config)# policy-map type control subscriber apple-tsim
Switch(config-policy-map)# event identity-update match-all
Switch(config-policy-map)# 1 class always do-until-failure
Switch(config-policy-map)# 1 map attribute-to-service table apple-tsim-param
Switch(config-policy-map)# end

This example shows how to apply policy to a device on a WLAN:

Switch(config)# wlan wlan1
Switch(config-wlan)# client vlan VLAN0054
Switch(config-wlan)# profiling local http
Switch(config-wlan)# service-policy type control subscriber apple-tsim
Switch(config-wlan)# no shutdown
Switch# end

Related Topics
  Creating a Parameter Map (CLI), on page 489
  Creating a Class Map (CLI), on page 491
  Creating a Policy Map (CLI), on page 491
  Applying a Local Policy for a Device on a WLAN (CLI), on page 492
  Creating an Interface Template (CLI), on page 489
  Information About Configuring Local Policies, on page 486
  Creating a Service Template (GUI), on page 494
  Creating a Policy Map (GUI), on page 495
  Applying Local Policies to WLAN (GUI), on page 496
Additional References for Configuring Local Policies

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History for Performing Local Policies Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Prerequisites for SPAN and RSPAN

SPAN

• You can limit SPAN traffic to specific VLANs by using the filter vlan keyword. If a trunk port is being monitored, only traffic on the VLANs specified with this keyword is monitored. By default, all VLANs are monitored on a trunk port.

RSPAN

• We recommend that you configure an RSPAN VLAN before you configure an RSPAN source or a destination session.

Restrictions for SPAN and RSPAN

SPAN

The restrictions for SPAN are as follows:

• On each switch, you can configure 66 sessions. A maximum of source sessions can be configured and the remaining sessions can be configured as RSPAN destinations sessions. A source session is either a local SPAN session or an RSPAN source session.

• For SPAN sources, you can monitor traffic for a single port or VLAN or a series or range of ports or VLANs for each session. You cannot mix source ports and source VLANs within a single SPAN session.
Restrictions for SPAN and RSPAN

- The destination port cannot be a source port; a source port cannot be a destination port.
- You cannot have two SPAN sessions using the same destination port.
- When you configure a switch port as a SPAN destination port, it is no longer a normal switch port; only monitored traffic passes through the SPAN destination port.
- Entering SPAN configuration commands does not remove previously configured SPAN parameters. You must enter the `no monitor session {session_number | all | local | remote}` global configuration command to delete configured SPAN parameters.
- For local SPAN, outgoing packets through the SPAN destination port carry the original encapsulation headers—untagged, ISL, or IEEE 802.1Q—if the `encapsulate replicate` keywords are specified. If the keywords are not specified, the packets are sent in native form.
- You can configure a disabled port to be a source or destination port, but the SPAN function does not start until the destination port and at least one source port or source VLAN are enabled.
- You cannot mix source VLANs and filter VLANs within a single SPAN session.

Traffic monitoring in a SPAN session has the following restrictions:

- Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.
- Wireshark does not capture egress packets when egress span is active.
- You can run both a local SPAN and an RSPAN source session in the same switch or switch stack. The switch or switch stack supports a total of 66 source and RSPAN destination sessions.
- You can configure two separate SPAN or RSPAN source sessions with separate or overlapping sets of SPAN source ports and VLANs. Both switched and routed ports can be configured as SPAN sources and destinations.
- You can have multiple destination ports in a SPAN session, but no more than 64 destination ports per switch stack.
- SPAN sessions do not interfere with the normal operation of the switch. However, an oversubscribed SPAN destination, for example, a 10-Mb/s port monitoring a 100-Mb/s port, can result in dropped or lost packets.
- When SPAN or RSPAN is enabled, each packet being monitored is sent twice, once as normal traffic and once as a monitored packet. Monitoring a large number of ports or VLANs could potentially generate large amounts of network traffic.
- You can configure SPAN sessions on disabled ports; however, a SPAN session does not become active unless you enable the destination port and at least one source port or VLAN for that session.
- The switch does not support a combination of local SPAN and RSPAN in a single session.
  - An RSPAN source session cannot have a local destination port.
  - An RSPAN destination session cannot have a local source port.
  - An RSPAN destination session and an RSPAN source session that are using the same RSPAN VLAN cannot run on the same switch or switch stack.
RSPAN

The restrictions for RSPAN are as follows:

- RSPAN does not support BPDU packet monitoring or other Layer 2 switch protocols.
- The RSPAN VLAN is configured only on trunk ports and not on access ports. To avoid unwanted traffic in RSPAN VLANs, make sure that the VLAN remote-span feature is supported in all the participating switches.
- RSPAN VLANs are included as sources for port-based RSPAN sessions when source trunk ports have active RSPAN VLANs. RSPAN VLANs can also be sources in SPAN sessions. However, since the switch does not monitor spanned traffic, it does not support egress spanning of packets on any RSPAN VLAN identified as the destination of an RSPAN source session on the switch.
- If you enable VTP and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network for VLAN IDs that are lower than 1005.
- To use RSPAN, the switch must be running the LAN Base image.

Information About SPAN and RSPAN

SPAN and RSPAN

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source VLANs can be monitored by using SPAN; traffic routed to a source VLAN cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another VLAN to the source VLAN cannot be monitored; however, traffic that is received on the source VLAN and routed to another VLAN can be monitored.

You can use the SPAN or RSPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) sensor appliance to a destination port, the IDS device can send TCP reset packets to close down the TCP session of a suspected attacker.

Local SPAN

Local SPAN supports a SPAN session entirely within one switch; all source ports or source VLANs and destination ports are in the same switch or switch stack. Local SPAN copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis.
Remote SPAN

Remote SPAN supports source ports, source VLANs, and destination ports on different switches (or different switch stacks), enabling remote monitoring of multiple switches across your network.

```
Figure 37: Example of RSPAN Configuration
```

The figure below shows source ports on Switch A and Switch B. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches.
The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded over trunk ports carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN. Each RSPAN source switch must have either ports or VLANs as RSPAN sources. The destination is always a physical port, as shown on Switch C in the figure.

**SPAN and RSPAN Concepts and Terminology**

**SPAN Sessions**

SPAN sessions (local or remote) allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports.

A local SPAN session is an association of a destination port with source ports or source VLANs, all on a single network device. Local SPAN does not have separate source and destination sessions. Local SPAN sessions gather a set of ingress and egress packets specified by the user and form them into a stream of SPAN data, which is directed to the destination port.

RSPAN consists of at least one RSPAN source session, an RSPAN VLAN, and at least one RSPAN destination session. You separately configure RSPAN source sessions and RSPAN destination sessions on different network devices. To configure an RSPAN source session on a device, you associate a set of source ports or source VLANs with an RSPAN VLAN. The output of this session is the stream of SPAN packets that are sent to the RSPAN VLAN. To configure an RSPAN destination session on another device, you associate the destination port with the RSPAN VLAN. The destination session collects all RSPAN VLAN traffic and sends it out the RSPAN destination port.

An RSPAN source session is very similar to a local SPAN session, except for where the packet stream is directed. In an RSPAN source session, SPAN packets are relabeled with the RSPAN VLAN ID and directed over normal trunk ports to the destination switch.
An RSPAN destination session takes all packets received on the RSPAN VLAN, strips off the VLAN tagging, and presents them on the destination port. The session presents a copy of all RSPAN VLAN packets (except Layer 2 control packets) to the user for analysis.

A single RSPAN session with multiple source and destination ports can be in the same session but more than one source session with the source being the same remote VLAN is not allowed.

Traffic monitoring in a SPAN session has these restrictions:

- Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.
- You can run both a local SPAN and an RSPAN source session in the same switch or switch stack. The switch or switch stack supports a total of 66 source and RSPAN destination sessions.
- You can configure two separate SPAN or RSPAN source sessions with separate or overlapping sets of SPAN source ports and VLANs. Both switched and routed ports can be configured as SPAN sources and destinations.
- You can have multiple destination ports in a SPAN session, but no more than 64 destination ports per switch stack.
- SPAN sessions do not interfere with the normal operation of the switch. However, an oversubscribed SPAN destination, for example, a 10-Mb/s port monitoring a 100-Mb/s port, can result in dropped or lost packets.
- When SPAN or RSPAN is enabled, each packet being monitored is sent twice, once as normal traffic and once as a monitored packet. Therefore monitoring a large number of ports or VLANs could potentially generate large amounts of network traffic.
- You can configure SPAN sessions on disabled ports; however, a SPAN session does not become active unless you enable the destination port and at least one source port or VLAN for that session.
- The switch does not support a combination of local SPAN and RSPAN in a single session.
  - An RSPAN source session cannot have a local destination port.
  - An RSPAN destination session cannot have a local source port.
  - An RSPAN destination session and an RSPAN source session that are using the same RSPAN VLAN cannot run on the same switch or switch stack.

SPAN sessions can monitor these traffic types:

- Receive (Rx) SPAN—Receive (or ingress) SPAN monitors as much as possible all of the packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that SPAN session.
  
  Packets that are modified because of routing or Quality of Service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied before modification.

  Features that can cause a packet to be dropped during receive processing have no effect on ingress SPAN; the destination port receives a copy of the packet even if the actual incoming packet is dropped. These features include IP standard and extended input Access Control Lists (ACLs), ingress QoS policing, VLAN ACLs, and egress QoS policing.
• Transmit (Tx) SPAN—Transmit (or egress) SPAN monitors as much as possible all of the packets sent by the source interface after all modification and processing is performed by the switch. A copy of each packet sent by the source is sent to the destination port for that SPAN session. The copy is provided after the packet is modified.

Packets that are modified because of routing (for example, with modified time-to-live (TTL), MAC address, or QoS values) are duplicated (with the modifications) at the destination port.

Features that can cause a packet to be dropped during transmit processing also affect the duplicated copy for SPAN. These features include IP standard and extended output ACLs and egress QoS policing.

• Both—In a SPAN session, you can also monitor a port or VLAN for both received and sent packets. This is the default.

The default configuration for local SPAN session ports is to send all packets untagged. However, when you enter the encapsulation replicate keywords while configuring a destination port, these changes occur:

• Packets are sent on the destination port with the same encapsulation (untagged or IEEE 802.1Q) that they had on the source port.

• Packets of all types, including BPDU and Layer 2 protocol packets, are monitored.

Therefore, a local SPAN session with encapsulation replicate enabled can have a mixture of untagged and IEEE 802.1Q tagged packets appear on the destination port.

Switch congestion can cause packets to be dropped at ingress source ports, egress source ports, or SPAN destination ports. In general, these characteristics are independent of one another. For example:

• A packet might be forwarded normally but dropped from monitoring due to an oversubscribed SPAN destination port.

• An ingress packet might be dropped from normal forwarding, but still appear on the SPAN destination port.

• An egress packet dropped because of switch congestion is also dropped from egress SPAN.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination port. For example, a bidirectional (both Rx and Tx) SPAN session is configured for the Rx monitor on port A and Tx monitor on port B. If a packet enters the switch through port A and is switched to port B, both incoming and outgoing packets are sent to the destination port. Both packets are the same unless a Layer 3 rewrite occurs, in which case the packets are different because of the packet modification.

Source Ports

A source port (also called a monitored port) is a switched or routed port that you monitor for network traffic analysis.

In a local SPAN session or RSPAN source session, you can monitor source ports or VLANs for traffic in one or both directions.

The switch supports any number of source ports (up to the maximum number of available ports on the switch) and any number of source VLANs (up to the maximum number of VLANs supported).

However, the switch supports a maximum of two sessions (local or RSPAN) with source ports or VLANs. You cannot mix ports and VLANs in a single session.

A source port has these characteristics:
• It can be monitored in multiple SPAN sessions.
• Each source port can be configured with a direction (ingress, egress, or both) to monitor.
• It can be any port type (for example, EtherChannel, Gigabit Ethernet, and so forth).
• For EtherChannel sources, you can monitor traffic for the entire EtherChannel or individually on a
  physical port as it participates in the port channel.
• It can be an access port, trunk port, routed port, or voice VLAN port.
• It cannot be a destination port.
• Source ports can be in the same or different VLANs.
• You can monitor multiple source ports in a single session.

Source VLANs

VLAN-based SPAN (VSPAN) is the monitoring of the network traffic in one or more VLANs. The SPAN
or RSPAN source interface in VSPAN is a VLAN ID, and traffic is monitored on all the ports for that VLAN.
VSPAN has these characteristics:
• All active ports in the source VLAN are included as source ports and can be monitored in either or both
directions.
• On a given port, only traffic on the monitored VLAN is sent to the destination port.
• If a destination port belongs to a source VLAN, it is excluded from the source list and is not monitored.
• If ports are added to or removed from the source VLANs, the traffic on the source VLAN received by
  those ports is added to or removed from the sources being monitored.
• You cannot use filter VLANs in the same session with VLAN sources.
• You can monitor only Ethernet VLANs.

VLAN Filtering

When you monitor a trunk port as a source port, by default, all VLANs active on the trunk are monitored.
You can limit SPAN traffic monitoring on trunk source ports to specific VLANs by using VLAN filtering.
• VLAN filtering applies only to trunk ports or to voice VLAN ports.
• VLAN filtering applies only to port-based sessions and is not allowed in sessions with VLAN sources.
• When a VLAN filter list is specified, only those VLANs in the list are monitored on trunk ports or on
  voice VLAN access ports.
• SPAN traffic coming from other port types is not affected by VLAN filtering; that is, all VLANs are
  allowed on other ports.
• VLAN filtering affects only traffic forwarded to the destination SPAN port and does not affect the
  switching of normal traffic.
Each local SPAN session or RSPAN destination session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports or VLANs and sends the SPAN packets to the user, usually a network analyzer.

A destination port has these characteristics:

- For a local SPAN session, the destination port must reside on the same switch or switch stack as the source port. For an RSPAN session, it is located on the switch containing the RSPAN destination session. There is no destination port on a switch or switch stack running only an RSPAN source session.

- When a port is configured as a SPAN destination port, the configuration overwrites the original port configuration. When the SPAN destination configuration is removed, the port reverts to its previous configuration. If a configuration change is made to the port while it is acting as a SPAN destination port, the change does not take effect until the SPAN destination configuration had been removed.

  **Note** When QoS is configured on the SPAN destination port, QoS takes effect immediately.

- If the port was in an EtherChannel group, it is removed from the group while it is a destination port. If it was a routed port, it is no longer a routed port.

- It can be any Ethernet physical port.

- It cannot be a source port.

- It cannot be a secure port.

- It can be an EtherChannel group (**ON** mode only).

- It cannot be a VLAN.

- It can participate in only one SPAN session at a time (a destination port in one SPAN session cannot be a destination port for a second SPAN session).

- When it is active, incoming traffic is disabled. The port does not transmit any traffic except that required for the SPAN session. Incoming traffic is never learned or forwarded on a destination port.

- If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.

- It does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP).

- A destination port that belongs to a source VLAN of any SPAN session is excluded from the source list and is not monitored.

- The maximum number of destination ports in a switch or switch stack is 64.

Local SPAN and RSPAN destination ports function differently with VLAN tagging and encapsulation:

- For local SPAN, if the **encapsulation replicate** keywords are specified for the destination port, these packets appear with the original encapsulation (untagged, ISL, or IEEE 802.1Q). If these keywords are not specified, packets appear in the untagged format. Therefore, the output of a local SPAN session with **encapsulation replicate** enabled can contain a mixture of untagged, ISL, or IEEE 802.1Q-tagged packets.
For RSPAN, the original VLAN ID is lost because it is overwritten by the RSPAN VLAN identification. Therefore, all packets appear on the destination port as untagged.

**RSPAN VLAN**

The RSPAN VLAN carries SPAN traffic between RSPAN source and destination sessions. RSPAN VLAN has these special characteristics:

- All traffic in the RSPAN VLAN is always flooded.
- No MAC address learning occurs on the RSPAN VLAN.
- RSPAN VLAN traffic only flows on trunk ports.
- RSPAN VLANs must be configured in VLAN configuration mode by using the `remote-span VLAN` configuration mode command.
- STP can run on RSPAN VLAN trunks but not on SPAN destination ports.
- An RSPAN VLAN cannot be a private-VLAN primary or secondary VLAN.

For VLANs 1 to 1005 that are visible to VLAN Trunking Protocol (VTP), the VLAN ID and its associated RSPAN characteristic are propagated by VTP. If you assign an RSPAN VLAN ID in the extended VLAN range (1006 to 4094), you must manually configure all intermediate switches.

It is normal to have multiple RSPAN VLANs in a network at the same time with each RSPAN VLAN defining a network-wide RSPAN session. That is, multiple RSPAN source sessions anywhere in the network can contribute packets to the RSPAN session. It is also possible to have multiple RSPAN destination sessions throughout the network, monitoring the same RSPAN VLAN and presenting traffic to the user. The RSPAN VLAN ID separates the sessions.

**SPAN and RSPAN Interaction with Other Features**

SPAN interacts with these features:

- Routing—SPAN does not monitor routed traffic. VSPAN only monitors traffic that enters or exits the switch, not traffic that is routed between VLANs. For example, if a VLAN is being Rx-monitored and the switch routes traffic from another VLAN to the monitored VLAN, that traffic is not monitored and not received on the SPAN destination port.
- STP—A destination port does not participate in STP while its SPAN or RSPAN session is active. The destination port can participate in STP after the SPAN or RSPAN session is disabled. On a source port, SPAN does not affect the STP status. STP can be active on trunk ports carrying an RSPAN VLAN.
- CDP—A SPAN destination port does not participate in CDP while the SPAN session is active. After the SPAN session is disabled, the port again participates in CDP.
- VTP—You can use VTP to prune an RSPAN VLAN between switches.
- VLAN and trunking—You can modify VLAN membership or trunk settings for source or destination ports at any time. However, changes in VLAN membership or trunk settings for a destination port do not take effect until you remove the SPAN destination configuration. Changes in VLAN membership or trunk settings for a source port immediately take effect, and the respective SPAN sessions automatically adjust accordingly.
- EtherChannel—You can configure an EtherChannel group as a source port or a SPAN destination port. When a group is configured as a SPAN source, the entire group is monitored.
If a physical port is added to a monitored EtherChannel group, the new port is added to the SPAN source port list. If a port is removed from a monitored EtherChannel group, it is automatically removed from the source port list.

A physical port that belongs to an EtherChannel group can be configured as a SPAN source port and still be a part of the EtherChannel. In this case, data from the physical port is monitored as it participates in the EtherChannel. However, if a physical port that belongs to an EtherChannel group is configured as a SPAN destination, it is removed from the group. After the port is removed from the SPAN session, it rejoins the EtherChannel group. Ports removed from an EtherChannel group remain members of the group, but they are in the inactive or suspended state.

If a physical port that belongs to an EtherChannel group is a destination port and the EtherChannel group is a source, the port is removed from the EtherChannel group and from the list of monitored ports.

• Multicast traffic can be monitored. For egress and ingress port monitoring, only a single unedited packet is sent to the SPAN destination port. It does not reflect the number of times the multicast packet is sent.

• A private-VLAN port cannot be a SPAN destination port.

• A secure port cannot be a SPAN destination port.

For SPAN sessions, do not enable port security on ports with monitored egress when ingress forwarding is enabled on the destination port. For RSPAN source sessions, do not enable port security on any ports with monitored egress.

• An IEEE 802.1x port can be a SPAN source port. You can enable IEEE 802.1x on a port that is a SPAN destination port; however, IEEE 802.1x is disabled until the port is removed as a SPAN destination.

For SPAN sessions, do not enable IEEE 802.1x on ports with monitored egress when ingress forwarding is enabled on the destination port. For RSPAN source sessions, do not enable IEEE 802.1x on any ports that are egress monitored.

SPAN and RSPAN and Device Stacks

Because the stack of switches represents one logical switch, local SPAN source ports and destination ports can be in different switches in the stack. Therefore, the addition or deletion of switches in the stack can affect a local SPAN session, as well as an RSPAN source or destination session. An active session can become inactive when a switch is removed from the stack or an inactive session can become active when a switch is added to the stack.

Flow-Based SPAN

You can control the type of network traffic to be monitored in SPAN or RSPAN sessions by using flow-based SPAN (FSPAN) or flow-based RSPAN (FRSPAN), which apply access control lists (ACLs) to the monitored traffic on the source ports. The FSPAN ACLs can be configured to filter IPv4, IPv6, and non-IP monitored traffic.

You apply an ACL to a SPAN session through the interface. It is applied to all the traffic that is monitored on all interfaces in the SPAN session. The packets that are permitted by this ACL are copied to the SPAN destination port. No other packets are copied to the SPAN destination port.

The original traffic continues to be forwarded, and any port, VLAN, and router ACLs attached are applied. The FSPAN ACL does not have any effect on the forwarding decisions. Similarly, the port, VLAN, and router ACLs do not have any effect on the traffic monitoring. If a security input ACL denies a packet and it is not forwarded, the packet is still copied to the SPAN destination ports if the FSPAN ACL permits it. But if the
security output ACL denies a packet and it is not sent, it is not copied to the SPAN destination ports. However, if the security output ACL permits the packet to go out, it is only copied to the SPAN destination ports if the FSPAN ACL permits it. This is also true for an RSPAN session.

You can attach three types of FSPAN ACLs to the SPAN session:

- IPv4 FSPAN ACL—Filters only IPv4 packets.
- IPv6 FSPAN ACL—Filters only IPv6 packets.
- MAC FSPAN ACL—Filters only non-IP packets.

If a VLAN-based FSPAN session configured on a stack cannot fit in the hardware memory on one or more switches, it is treated as unloaded on those switches, and traffic meant for the FSPAN ACL and sourcing on that switch is not copied to the SPAN destination ports. The FSPAN ACL continues to be correctly applied, and traffic is copied to the SPAN destination ports on the switches where the FSPAN ACL fits in the hardware memory.

When an empty FSPAN ACL is attached, some hardware functions copy all traffic to the SPAN destination ports for that ACL. If sufficient hardware resources are not available, even an empty FSPAN ACL can be unloaded.

IPv4 and MAC FSPAN ACLs are supported on all feature sets. IPv6 FSPAN ACLs are supported only in the advanced IP Services feature set.

### Default SPAN and RSPAN Configuration

#### Table 32: Default SPAN and RSPAN Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPAN state (SPAN and RSPAN)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Source port traffic to monitor</td>
<td>Both received and sent traffic (both).</td>
</tr>
<tr>
<td>Encapsulation type (destination port)</td>
<td>Native form (untagged packets).</td>
</tr>
<tr>
<td>Ingress forwarding (destination port)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>VLAN filtering</td>
<td>On a trunk interface used as a source port, all VLANs are monitored.</td>
</tr>
<tr>
<td>RSPAN VLANs</td>
<td>None configured.</td>
</tr>
</tbody>
</table>

### Configuration Guidelines

#### SPAN Configuration Guidelines

- To remove a source or destination port or VLAN from the SPAN session, use the `no monitor session session_number source {interface interface-id | vlan vlan-id}` global configuration command or the `no monitor session session_number destination interface interface-id` global configuration command. For destination interfaces, the `encapsulation` options are ignored with the `no` form of the command.
• To monitor all VLANs on the trunk port, use the `no monitor session session_number filter` global configuration command.

**RSPAN Configuration Guidelines**

• All the SPAN configuration guidelines apply to RSPAN.

• As RSPAN VLANs have special properties, you should reserve a few VLANs across your network for use as RSPAN VLANs; do not assign access ports to these VLANs.

• You can apply an output ACL to RSPAN traffic to selectively filter or monitor specific packets. Specify these ACLs on the RSPAN VLAN in the RSPAN source switches.

• For RSPAN configuration, you can distribute the source ports and the destination ports across multiple switches in your network.

• Access ports (including voice VLAN ports) on the RSPAN VLAN are put in the inactive state.

• You can configure any VLAN as an RSPAN VLAN as long as these conditions are met:
  • The same RSPAN VLAN is used for an RSPAN session in all the switches.
  • All participating switches support RSPAN.

**FSPAN and FRSPAN Configuration Guidelines**

• FSPAN is not supported on LAN base.

• When at least one FSPAN ACL is attached, FSPAN is enabled.

• When you attach at least one FSPAN ACL that is not empty to a SPAN session, and you have not attached one or more of the other FSPAN ACLs (for instance, you have attached an IPv4 ACL that is not empty, and have not attached IPv6 and MAC ACLs), FSPAN blocks the traffic that would have been filtered by the unattached ACLs. Therefore, this traffic is not monitored.

**How to Configure SPAN and RSPAN**

**Creating a Local SPAN Session**

Follow these steps to create a SPAN session and specify the source (monitored) ports or VLANs and the destination (monitoring) ports.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; <code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Creating a Local SPAN Session

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>configure terminal</strong>&lt;br&gt;Example:&lt;br&gt;<code>Switch# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td><strong>no monitor session</strong> `{session_number</td>
<td>all</td>
</tr>
<tr>
<td>4</td>
<td><strong>monitor session</strong> <code>session_number source</code> `{interface interface-id</td>
<td>vlan vlan-id} [,</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• both—Monitors both received and sent traffic.</td>
<td></td>
</tr>
<tr>
<td>• rx—Monitors received traffic.</td>
<td></td>
</tr>
<tr>
<td>• tx—Monitors sent traffic.</td>
<td></td>
</tr>
</tbody>
</table>

### Note

You can use the `monitor session session_number source` command multiple times to configure multiple source ports.

### Step 5

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor session session_number destination [interface interface-id [, -] [encapsulation replicate]]</code></td>
<td>Specifies the SPAN session and the destination port (monitoring port). The port LED changes to amber when the configuration changes take effect. The LED returns to its original state (green) only after removing the SPAN destination configuration.</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2 encapsulation replicate
```

**Note**

For local SPAN, you must use the same session number for the source and destination interfaces.

- For `session_number`, specify the session number entered in step 4.
- For `interface-id`, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.
- (Optional) `[,] [-]` Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.

(Optional) `encapsulation replicate` specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).

**Note**

You can use `monitor session session_number destination` command multiple times to configure multiple destination ports.

### Step 6

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
end
```
Creating a Local SPAN Session and Configuring Incoming Traffic

Follow these steps to create a SPAN session, to specify the source ports or VLANs and the destination ports, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> no monitor session {session_number</td>
<td>all</td>
</tr>
<tr>
<td>Example:</td>
<td>• For session_number, the range is 1 to 4.</td>
</tr>
<tr>
<td>Switch(config)# no monitor session all</td>
<td>• all—Removes all SPAN sessions.</td>
</tr>
<tr>
<td></td>
<td>• local—Removes all local sessions.</td>
</tr>
<tr>
<td></td>
<td>• remote—Removes all remote SPAN sessions.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies the SPAN session and the source port (monitored port).</td>
</tr>
<tr>
<td>`monitor session session_number source {interface interface-id</td>
<td>vlan vlan-id} [ ,</td>
</tr>
<tr>
<td><code>Switch(config)# monitor session 2 source gigabitethernet0/1 rx</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specifies the SPAN session, the destination port, the packet encapsulation, and the ingress VLAN and encapsulation.</td>
</tr>
<tr>
<td>`monitor session session_number destination {interface interface-id [ ,</td>
<td>- ] [encapsulation replicate][ingress {dot1q vlan vlan-id</td>
</tr>
<tr>
<td><code>Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate ingress dot1q vlan 6</code></td>
<td>• For <code>session_number</code>, specify the session number entered in Step 4.</td>
</tr>
<tr>
<td></td>
<td>• For <code>interface-id</code>, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) `,</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <code>encapsulation replicate</code>—Specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).</td>
</tr>
<tr>
<td></td>
<td>• <code>ingress</code>—Enables forwarding of incoming traffic on the destination port and to specify the encapsulation type.</td>
</tr>
<tr>
<td></td>
<td>• <code>dot1q vlan vlan-id</code>—Accepts incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.</td>
</tr>
<tr>
<td></td>
<td>• <code>untagged vlan vlan-id or vlan vlan-id</code>—Accepts incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
### Specifying VLANs to Filter

Follow these steps to limit SPAN source traffic to specific VLANs.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2**        | Enters global configuration mode. |
| `configure terminal` | |
| `Switch# configure terminal` | |

| **Step 3**        | Removes any existing SPAN configuration for the session. |
| `no monitor session {session_number | all | local | remote}` | |
| `Switch(config)# no monitor session all` | |

| **Step 4**        | Specifies the characteristics of the source port (monitored port) and SPAN session. |
| `monitor session session_number source interface interface-id` | |
| `Switch(config)# monitor session session_number source interface interface-id` | |

---

**Specifying VLANs to Filter**

Follow these steps to limit SPAN source traffic to specific VLANs.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show running-config</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 8**        | (Optional) Saves your entries in the configuration file. |
| `copy running-config startup-config` | |
| `Switch# copy running-config startup-config` | |
### Command or Action

Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx

### Purpose

- For *interface-id*, specify the source port to monitor. The interface specified must already be configured as a trunk port.

### Step 5

**monitor session session_number filter vlan vlan-id [ , | - ]**

**Example:**

Switch(config)# monitor session 2 filter vlan 1 - 5 , 9

 Limits the SPAN source traffic to specific VLANs.

- For *session_number*, enter the session number specified in Step 4.
- For *vlan-id*, the range is 1 to 4094.
- (Optional) Use a comma (,) to specify a series of VLANs, or use a hyphen (-) to specify a range of VLANs. Enter a space before and after the comma; enter a space before and after the hyphen.

### Step 6

**monitor session session_number destination { (interface interface-id [ , | - ] [ encapsulation replicate ] ) }**

**Example:**

Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1

 Specifies the SPAN session and the destination port (monitoring port).

- For *session_number*, specify the session number entered in Step 4.
- For *interface-id*, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.
- (Optional) [ , | - ] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.
- (Optional) *encapsulation replicate* specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).

### Step 7

**end**

**Example:**

Switch(config)# end

Returns to privileged EXEC mode.

### Step 8

**show running-config**

**Example:**

Verifies your entries.
Configuring a VLAN as an RSPAN VLAN

Follow these steps to create a new VLAN, then configure it to be the RSPAN VLAN for the RSPAN session.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>vlan vlan-id</code></td>
<td>Enters a VLAN ID to create a VLAN, or enters the VLAN ID of an existing</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>VLAN, and enters VLAN configuration mode. The range is 2 to 1001 and</td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# vlan 100</code></td>
<td>1006 to 4094.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>through 1005 (reserved for Token Ring and FDDI VLANs).</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>remote-span</code></td>
<td>Configures the VLAN as an RSPAN VLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-vlan)# remote-span</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-vlan)# end</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Verifies your entries.</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Step 7           | copy running-config startup-config |
| Example:         | (Optional) Saves your entries in the configuration file. |
| Switch# copy running-config startup-config | |

### What to do next

You must create the RSPAN VLAN in all switches that will participate in RSPAN. If the RSPAN VLAN-ID is in the normal range (lower than 1005) and VTP is enabled in the network, you can create the RSPAN VLAN in one switch, and VTP propagates it to the other switches in the VTP domain. For extended-range VLANs (greater than 1005), you must configure RSPAN VLAN on both source and destination switches and any intermediate switches.

Use VTP pruning to get an efficient flow of RSPAN traffic, or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

To remove the remote SPAN characteristic from a VLAN and convert it back to a normal VLAN, use the `no remote-span` VLAN configuration command.

To remove a source port or VLAN from the SPAN session, use the `no monitor session session_number source {interface interface-id | vlan vlan-id}` global configuration command. To remove the RSPAN VLAN from the session, use the `no monitor session session_number destination remote vlan vlan-id`.

### Creating an RSPAN Source Session

Follow these steps to create and start an RSPAN source session and to specify the monitored source and the destination RSPAN VLAN.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| Step 2           | configure terminal |
| Example:         | Enters global configuration mode. |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Removes any existing SPAN configuration for the session.</td>
</tr>
<tr>
<td>no monitor session {session_number</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>• all—Removes all SPAN sessions.</td>
</tr>
<tr>
<td></td>
<td>• local—Removes all local sessions.</td>
</tr>
<tr>
<td>Example:</td>
<td>• remote—Removes all remote SPAN sessions.</td>
</tr>
<tr>
<td>Switch(config)# no monitor session 1</td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor session session_number source</td>
<td>Specifies the RSPAN session and the source port (monitored port).</td>
</tr>
<tr>
<td>{interface interface-id</td>
<td>vlan vlan-id} [ ,</td>
</tr>
<tr>
<td></td>
<td>• Enter a source port or source VLAN for the RSPAN session:</td>
</tr>
<tr>
<td></td>
<td>• For interface-id, specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel port-channel-number). Valid port-channel numbers are 1 to 48.</td>
</tr>
<tr>
<td></td>
<td>• For vlan-id, specifies the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN). A single session can include multiple sources (ports or VLANs), defined in a series of commands, but you cannot combine source ports and source VLANs in one session.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) [ ,</td>
</tr>
<tr>
<td></td>
<td>• (Optional) both</td>
</tr>
<tr>
<td></td>
<td>• both—Monitors both received and sent traffic.</td>
</tr>
</tbody>
</table>

Example:

Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
Specifying VLANs to Filter

Follow these steps to configure the RSPAN source session to limit RSPAN source traffic to specific VLANs.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td>Removes any existing SPAN configuration for the session.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>no monitor session</strong> {<strong>session_number</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# no monitor session 2</td>
</tr>
<tr>
<td></td>
<td>• For <strong>session_number</strong>, the range is 1 to 66.</td>
</tr>
<tr>
<td></td>
<td>• <strong>all</strong>—Removes all SPAN sessions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>local</strong>—Removes all local sessions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>remote</strong>—Removes all remote SPAN sessions.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>monitor session</strong> <strong>session_number</strong> source interface <strong>interface-id</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx</td>
</tr>
<tr>
<td></td>
<td>• For <strong>session_number</strong>, the range is 1 to 66.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>interface-id</strong>, specify the source port to monitor. The interface specified must already be configured as a trunk port.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>monitor session</strong> <strong>session_number</strong> filter vlan <strong>vlan-id</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# monitor session 2 filter vlan 1 - 5 , 9</td>
</tr>
<tr>
<td></td>
<td>• For <strong>session_number</strong>, enter the session number specified in step 4.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>vlan-id</strong>, the range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• (Optional),</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>monitor session</strong> <strong>session_number</strong> destination remote vlan <strong>vlan-id</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# monitor session 2 destination remote vlan 902</td>
</tr>
<tr>
<td></td>
<td>• For <strong>session_number</strong>, enter the session number specified in Step 4.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>vlan-id</strong>, specify the RSPAN VLAN to carry the monitored traffic to the destination port.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Creating an RSPAN Destination Session

You configure an RSPAN destination session on a different switch or switch stack; that is, not the switch or switch stack on which the source session was configured.

Follow these steps to define the RSPAN VLAN on that switch, to create an RSPAN destination session, and to specify the source RSPAN VLAN and the destination port.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vlan vlan-id</td>
<td>Specifies the VLAN ID of the RSPAN VLAN created from the source switch,</td>
</tr>
<tr>
<td>Example:</td>
<td>and enters VLAN configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# vlan 901</td>
<td>If both switches are participating in VTP and the RSPAN VLAN ID is from 2 to 1005, Steps 3 through 5 are not required because the RSPAN VLAN ID is propagated through the VTP network.</td>
</tr>
<tr>
<td><strong>Step 4</strong> remote-span</td>
<td>Identifies the VLAN as the RSPAN VLAN.</td>
</tr>
</tbody>
</table>
### Creating an RSPAN Destination Session

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-vlan)# remote-span</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

- **exit**  
  **Example:**  
  Switch(config-vlan)# exit  
  **Purpose:** Returns to global configuration mode.

**Step 6**

- **no monitor session [session_number | all | local | remote]**  
  **Example:**  
  Switch(config)# no monitor session 1  
  **Purpose:** Removes any existing SPAN configuration for the session.  
  - For **session_number**, the range is 1 to 66.  
  - **all**—Removes all SPAN sessions.  
  - **local**—Removes all local sessions.  
  - **remote**—Removes all remote SPAN sessions.

**Step 7**

- **monitor session session_number source remote vlan vlan-id**  
  **Example:**  
  Switch(config)# monitor session 1 source remote vlan 901  
  **Purpose:** Specifies the RSPAN session and the source RSPAN VLAN.  
  - For **session_number**, the range is 1 to 66.  
  - For **vlan-id**, specify the source RSPAN VLAN to monitor.

**Step 8**

- **monitor session session_number destination interface interface-id**  
  **Example:**  
  Switch(config)# monitor session 1 destination interface gigabitethernet2/0/1  
  **Purpose:** Specifies the RSPAN session and the destination interface.  
  - For **session_number**, enter the number defined in Step 7.  
  - In an RSPAN destination session, you must use the same session number for the source RSPAN VLAN and the destination port.  
  - For **interface-id**, specify the destination interface. The destination interface must be a physical interface.  
  - Though visible in the command-line help string, **encapsulation replicate** is not supported for RSPAN. The original VLAN ID is overwritten by the RSPAN VLAN ID, and all packets appear on the destination port as untagged.

**Step 9**

- **end**  
  **Example:**  
  **Purpose:** Returns to privileged EXEC mode.
Creating an RSPAN Destination Session and Configuring Incoming Traffic

Follow these steps to create an RSPAN destination session, to specify the source RSPAN VLAN and the destination port, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**      | |
| Switch# configure terminal | |

| **Step 3** no monitor session {session_number | all | local | remote} | Removes any existing SPAN configuration for the session. |
| **Example:** | • For session_number, the range is 1 to 66. |
| Switch(config)# no monitor session 2 | • all—Removes all SPAN sessions. |
| | • local—Removes all local sessions. |
| | • remote—Removes all remote SPAN sessions. |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 4** monitor session session_number source remote vlan vlan-id | Specifies the RSPAN session and the source RSPAN VLAN.  
  - For `session_number`, the range is 1 to 66.  
  - For `vlan-id`, specify the source RSPAN VLAN to monitor. |
| **Example:** Switch(config)# monitor session 2 source remote vlan 901 | |
| **Step 5** monitor session session_number destination {interface interface-id [s, | -] [ingress {dot1q vlan vlan-id | untagged vlan vlan-id | vlan vlan-id}]}} | Specifies the SPAN session, the destination port, the packet encapsulation, and the incoming VLAN and encapsulation.  
  - For `session_number`, enter the number defined in Step 5.  
  - In an RSPAN destination session, you must use the same session number for the source RSPAN VLAN and the destination port.  
  - For `interface-id`, specify the destination interface. The destination interface must be a physical interface.  
  - Though visible in the command-line help string, `encapsulation replicate` is not supported for RSPAN. The original VLAN ID is overwritten by the RSPAN VLAN ID, and all packets appear on the destination port as untagged.  
  - (Optional) [s, | -] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.  
  - Enter `ingress` with additional keywords to enable forwarding of incoming traffic on the destination port and to specify the encapsulation type:  
    - `dot1q vlan vlan-id`—Forwards incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.  
    - `untagged vlan vlan-id` or `vlan vlan-id`—Forwards incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN. |
| **Example:** Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6 | |
### Configuring an FSPAN Session

Follow these steps to create a SPAN session, specify the source (monitored) ports or VLANs and the destination (monitoring) ports, and configure FSPAN for the session.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Removes any existing SPAN configuration for the session.</td>
</tr>
<tr>
<td>no monitor session</td>
<td>For session_number, the range is 1 to 66.</td>
</tr>
<tr>
<td>{session_number</td>
<td>all</td>
</tr>
<tr>
<td>Example:</td>
<td>all—Removes all SPAN sessions.</td>
</tr>
<tr>
<td>Switch(config)# no monitor session 2</td>
<td>local—Removes all local sessions.</td>
</tr>
<tr>
<td></td>
<td>remote—Removes all remote SPAN sessions.</td>
</tr>
</tbody>
</table>
### Configuring an FSPAN Session

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies the SPAN session and the source port (monitored port).</td>
</tr>
</tbody>
</table>
| `monitor session session_number source`  
  `{interface interface-id | vlan vlan-id} [both | rx | tx]`  
  Example: `Switch(config)# monitor session 2 source interface gigabitethernet1/0/1` | - For `session_number`, the range is 1 to 66.  
- For `interface-id`, specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (`port-channel port-channel-number`). Valid port-channel numbers are 1 to 48.  
- For `vlan-id`, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN).  
  **Note** A single session can include multiple sources (ports or VLANs) defined in a series of commands, but you cannot combine source ports and source VLANs in one session.  
- (Optional) `[ | -]`—Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.  
- (Optional) `[both | rx | tx]`—Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the SPAN monitors both sent and received traffic.  
  - **both**—Monitors both sent and received traffic. This is the default.  
  - **rx**—Monitors received traffic.  
  - **tx**—Monitors sent traffic.  
  **Note** You can use the `monitor session session_number source` command multiple times to configure multiple source ports. |
| **Step 5** | Specifies the SPAN session and the destination port (monitoring port). |
| `monitor session session_number destination`  
  `{interface interface-id [, ] [encapsulation replicate]}`  
  Example: | - For `session_number`, specify the session number entered in Step 4. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate` | • For **destination**, specify the following parameters:  
  • For **interface-id**, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.  
  • (Optional) [ - ] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.  
  • (Optional) **encapsulation replicate** specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).  
  
  **Note** For local SPAN, you must use the same session number for the source and destination interfaces.  
  You can use `monitor session` **session_number destination** command multiple times to configure multiple destination ports. |

**Step 6**  
`monitor session session_number filter {ip | ipv6 | mac} access-group {access-list-number | name}`  
**Example:**  
`Switch(config)# monitor session 2 filter ipv6 access-group 4`

**Step 7**  
`end`  
**Example:**  
`Switch(config)# end`

**Step 8**  
`show running-config`  
**Example:**  
Verifies your entries.
Configuring an FRSPAN Session

Follow these steps to start an RSPAN source session, specify the monitored source and the destination RSPAN VLAN, and configure FRSPAN for the session.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  enable
  Example: Switch> enable | Enables privileged EXEC mode.
  • Enter your password if prompted. |
| **Step 2**
  configure terminal
  Example: Switch# configure terminal | Enters global configuration mode. |
| **Step 3**
  no monitor session session_number | Removes any existing SPAN configuration for the session.
  Example: Switch(config)# no monitor session 2
  • For session_number, the range is 1 to 66.
  • all—Removes all SPAN sessions.
  • local—Removes all local sessions.
  • remote—Removes all remote SPAN sessions. |
| **Step 4**
  monitor session session_number source interface interface-id vlan vlan-id both rx tx
  Example: Switch(config)# monitor session 2 source interface gigabitethernet1/0/1 | Specifies the SPAN session and the source port (monitored port).
  • For session_number, the range is 1 to 66.
  • For interface-id, specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel) |
**Purpose**

*port-channel-number*. Valid port-channel numbers are 1 to 48.

- For *vlan-id*, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN).

**Note** A single session can include multiple sources (ports or VLANs) defined in a series of commands, but you cannot combine source ports and source VLANs in one session.

- (Optional) [ , | - ]—Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.

- (Optional) [both | rx | tx]—Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the SPAN monitors both sent and received traffic.

  - **both**—Monitors both sent and received traffic. This is the default.
  - **rx**—Monitors received traffic.
  - **tx**—Monitors sent traffic.

**Note** You can use the `monitor session session_number source` command multiple times to configure multiple source ports.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor session session_number destination remote vlan vlan-id</code></td>
<td>Specifies the RSPAN session and the destination RSPAN VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>monitor session 2 destination remote vlan 5</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan vlan-id</code></td>
<td>Enters the VLAN configuration mode. For <em>vlan-id</em>, specify the source RSPAN VLAN to monitor.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>vlan 10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring an FRSPAN Session

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>remote-span</code></td>
<td>Specifies that the VLAN you specified in Step 5 is part of the RSPAN VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-vlan)# remote-span</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-vlan)# exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>`monitor session session_number filter {ip</td>
<td>ipv6</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# monitor session 2 filter ip access-group 7</code></td>
<td>• For <code>session_number</code>, specify the session number entered in Step 4.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For <code>access-list-number</code>, specify the ACL number that you want to use to filter traffic.</td>
</tr>
<tr>
<td></td>
<td>• For <code>name</code>, specify the ACL name that you want to use to filter traffic.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
Monitoring SPAN and RSPAN Operations

The following table describes the command used to display SPAN and RSPAN operations configuration and results to monitor operations:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show monitor</td>
<td>Displays the current SPAN, RSPAN, FSPAN, or FRSPAN configuration.</td>
</tr>
</tbody>
</table>

SPAN and RSPAN Configuration Examples

Example: Configuring Local SPAN

This example shows how to set up SPAN session 1 for monitoring source port traffic to a destination port. First, any existing SPAN configuration for session 1 is deleted, and then bidirectional traffic is mirrored from source Gigabit Ethernet port 1 to destination Gigabit Ethernet port 2, retaining the encapsulation method.

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
    encapsulation replicate
Switch(config)# end

This example shows how to remove port 1 as a SPAN source for SPAN session 1:

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# end

This example shows how to disable received traffic monitoring on port 1, which was configured for bidirectional monitoring:

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1 rx

The monitoring of traffic received on port 1 is disabled, but traffic sent from this port continues to be monitored.

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on all ports belonging to VLANs 1 through 3, and send it to destination Gigabit Ethernet port 2. The configuration is then modified to also monitor all traffic on all ports belonging to VLAN 10.

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on Gigabit Ethernet source port 1, and send it to destination Gigabit Ethernet port 2 with the same egress encapsulation type as the source port, and to enable ingress forwarding with VLAN 6 as the default ingress VLAN:

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation replicate ingress vlan 6
Switch(config)# end

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor traffic received on Gigabit Ethernet trunk port 2, and send traffic for only VLANs 1 through 5 and VLAN 9 to destination Gigabit Ethernet port 1:

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1
Switch(config)# end

This examples show how to create the RSPAN VLAN 901:

Switch> enable
Switch# configure terminal
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end

This example shows how to remove any existing RSPAN configuration for session 1, configure RSPAN session 1 to monitor multiple source interfaces, and configure the destination as RSPAN VLAN 901:

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 1 source interface port-channel 2
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end

This example shows how to remove any existing configuration on RSPAN session 2, configure RSPAN session 2 to monitor traffic received on trunk port 2, and send traffic for only VLANs 1 through 5 and 9 to destination RSPAN VLAN 902:
This example shows how to configure VLAN 901 as the source remote VLAN and port 1 as the destination interface:

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end

This example shows how to configure VLAN 901 as the source remote VLAN in RSPAN session 2, to configure Gigabit Ethernet source port 2 as the destination interface, and to enable forwarding of incoming traffic on the interface with VLAN 6 as the default receiving VLAN:

Switch> enable
Switch# configure terminal
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet2/0/1
Switch(config)# end

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Commands</td>
<td>Network Management Command Reference, Cisco IOS XE Release 3E</td>
</tr>
</tbody>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>-</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

**Description**
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.

To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.

Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.

**Link**
[http://www.cisco.com/support](http://www.cisco.com/support)

---

**Feature History and Information for SPAN and RSPAN**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>Switch Port Analyzer (SPAN): Allows monitoring of switch traffic on a port or VLAN using a sniffer/analyzer or RMON probe. This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>Flow-based Switch Port Analyzer (SPAN): Provides a method to capture only required data between end hosts by using specified filters. The filters are defined in terms of access lists that limit IPv4, IPv6 or IPv4 + IPv6, or non-IP traffic (MAC) between specified source and destination addresses. This feature was introduced.</td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>SPAN destination port support on EtherChannels: Provides the ability to configure a SPAN destination port on an EtherChannel. This feature was introduced.</td>
</tr>
<tr>
<td></td>
<td>Switch Port Analyzer (SPAN) - distributed egress SPAN: Provides distributed egress SPAN functionality onto line cards in conjunction with ingress SPAN already been distributed to line cards. By distributing egress SPAN functionalities onto line cards, the performance of the system is improved. This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 37

Configuring Wireshark

- Finding Feature Information, on page 541
- Prerequisites for Wireshark, on page 541
- Restrictions for Wireshark, on page 541
- Information About Wireshark, on page 543
- How to Configure Wireshark, on page 553
- Monitoring Wireshark, on page 568
- Configuration Examples for Wireshark, on page 568
- Additional References, on page 585
- Feature History and Information for WireShark, on page 586

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Wireshark

- Wireshark is supported on Supervisor Engine 7-E, Supervisor Engine 7L-E, Catalyst 3850, Catalyst 3650, Wireless LAN Controller 5700 Series, Catalyst 4500X-16, and Catalyst 4500X-32.

- IP Base image or IP Services image is required for Embedded Wireshark.

Restrictions for Wireshark

- Starting in Cisco IOS Release XE 3.3.0(SE), global packet capture on Wireshark is not supported.

- Capture filters are not supported.
• The CLI for configuring Wireshark requires that the feature be executed only from EXEC mode. Actions that usually occur in configuration submode (such as defining capture points), are handled at the EXEC mode instead. All key commands are not NVGEN’d and are not synchronized to the standby supervisor in NSF and SSO scenarios.

• Packets captured in the output direction of an interface might not reflect the changes made by switch rewrite (includes TTL, VLAN tag, CoS, checksum, MAC addresses, DSCP, precedent, UP, etc.).

• Limiting circular file storage by file size is not supported.

**Wireless Packet Capture**

• The only form of wireless capture is a CAPWAP tunnel capture.

• When capturing CAPWAP tunnels, no other interface types can be used as attachment points on the same capture point.

• Capturing multiple CAPWAP tunnels is supported.

• Core filters are not applied and should be omitted when capturing a CAPWAP tunnel.

• To capture a CAPWAP data tunnel, each CAPWAP tunnel is mapped to a physical port and an appropriate ACL will be applied to filter the traffic.

• To capture a CAPWAP non-data tunnel, the switch is set to capture traffic on all ports and apply an appropriate ACL to filter the traffic.

• To capture a CAPWAP tunnel, no matter what kind, the controller will be told to capture the traffic on all physical ports and apply an appropriate ACL to filter the traffic.

**Configuration Limitations**

• Starting from Cisco IOS release 16.1, as many as 8 capture points can be defined, but only one can be active at a time. You must stop one before you can start the other.

• You cannot use VRFs, management ports, and private VLANs as attachment points.

• Only one ACL (IPv4, IPv6 or MAC) is allowed in a Wireshark class map.

• Wireshark cannot capture packets on a destination SPAN port.

• Wireshark stops capturing packets when one of the attachment points (interfaces) attached to a capture point stops working. For example, if the device that is associated with an attachment point is unplugged from the switch. To resume capturing packets, restart manually.

• CPU-injected packets are considered control plane packets and are not captured on an interface egress capture.

• MAC ACL is only used for non-IP packets such as ARP. It will not be supported on a Layer 3 port or SVI.

• IPv6-based ACLs are not supported in VACL.

• Layer 2 EtherChannels are not supported. Individual members like GigabitEthernet 1 and GigabitEthernet 2 are supported on Layer 3 EtherChannels.
• ACL logging and Wireshark are incompatible. After Wireshark is activated, it takes priority. All traffic, including traffic captured by ACL logging on ports, will be redirected to Wireshark. We recommend that you deactivate ACL logging before you start Wireshark. Otherwise, Wireshark traffic is contaminated by ACL logging traffic.

• Wireshark does not capture packets dropped by floodblock.

• If you capture both PACL and RACL on the same port, only one copy is sent to the CPU. If you capture a DTLS-encrypted CAPWAP interface, two copies are sent to Wireshark, one encrypted and the other decrypted. The same behavior will occur if we capture a Layer 2 interface carrying DTLS-encrypted CAPWAP traffic. The core filter is based on the outer CAPWAP header.

• Control plane packets are not rate limited and do not impact performance. Use filters to limit control plane packet capture.

Information About Wireshark

Wireshark Overview

Wireshark is a packet analyzer program, formerly known as Ethereal, that supports multiple protocols and presents information in a text-based user interface.

The ability to capture and analyze traffic provides data on network activity. Prior to Cisco IOS Release XE 3.3.0(SE), only two features addressed this need: SPAN and debug platform packet. Both have limitations. SPAN is ideal for capturing packets, but can only deliver them by forwarding them to some specified local or remote destination; it provides no local display or analysis support.

So the need exists for a traffic capture and analysis mechanism that is applicable to both hardware and software forwarded traffic and that provides strong packet capture, display, and analysis support, preferably using a well known interface.

Wireshark dumps packets to a file using a well known format called .pcap, and is applied or enabled on individual interfaces. You specify an interface in EXEC mode along with the filter and other parameters. The Wireshark application is applied only when you enter a start command, and is removed only when Wireshark stops capturing packets either automatically or manually.

The current version of Wireshark installed on the switch is 1.10.8.

Capture Points

A capture point is the central policy definition of the Wireshark feature. The capture point describes all of the characteristics associated with a given instance of Wireshark: which packets to capture, where to capture them from, what to do with the captured packets, and when to stop. Capture points can be modified after creation, and do not become active until explicitly activated with a start command. This process is termed activating the capture point or starting the capture point. Capture points are identified by name and can also be manually or automatically deactivated or stopped.
Multiple capture points can be defined, but only one can be active at a time. You need to stop one before you can start the other.

In case of stacked systems, the capture point is activated on the active member. A switchover will terminate any active packet capture session and it will have to be restarted.

**Related Topics**
- Defining a Capture Point, on page 553
- Adding or Modifying Capture Point Parameters, on page 558
- Deleting Capture Point Parameters, on page 560
- Deleting a Capture Point, on page 562
- Activating and Deactivating a Capture Point, on page 563
- Clearing the Capture Point Buffer, on page 566
- Example: Simple Capture and Display, on page 571
- Example: Simple Capture and Store, on page 572
- Example: Using Buffer Capture, on page 575
- Example: Capture Sessions, on page 581
- Example: Capture and Store in Lock-step Mode, on page 582
- Example: Simple Capture and Store of Packets in Egress Direction, on page 583

**Attachment Points**

An attachment point is a point in the logical packet process path associated with a capture point. An attachment point is an attribute of the capture point. Packets that impact an attachment point are tested against capture point filters; packets that match are copied and sent to the associated Wireshark instance of the capture point. A specific capture point can be associated with multiple attachment points, with limits on mixing attachment points of different types. Some restrictions apply when you specify attachment points of different types. Attachment points are directional (input or output or both) with the exception of the Layer 2 VLAN attachment point, which is always bidirectional.

In case of stacked systems, the attachment points on all stack members are valid. EPC captures the packets from all the defined attachment points. However these packets are processed only on the active member.

**Related Topics**
- Defining a Capture Point, on page 553
- Adding or Modifying Capture Point Parameters, on page 558
- Deleting Capture Point Parameters, on page 560
- Deleting a Capture Point, on page 562
- Activating and Deactivating a Capture Point, on page 563
- Clearing the Capture Point Buffer, on page 566
- Example: Simple Capture and Display, on page 571
- Example: Simple Capture and Store, on page 572
- Example: Using Buffer Capture, on page 575
- Example: Capture Sessions, on page 581
- Example: Capture and Store in Lock-step Mode, on page 582
- Example: Simple Capture and Store of Packets in Egress Direction, on page 583
Filters

Filters are attributes of a capture point that identify and limit the subset of traffic traveling through the attachment point of a capture point, which is copied and passed to Wireshark. To be displayed by Wireshark, a packet must pass through an attachment point, as well as all of the filters associated with the capture point.

A capture point has the following types of filters:

- Core system filter—The core system filter is applied by hardware, and its match criteria is limited by hardware. This filter determines whether hardware-forwarded traffic is copied to software for Wireshark purposes.
- Display filter—The display filter is applied by Wireshark. Packets that fail the display filter are not displayed.

Core System Filter

You can specify core system filter match criteria by using the class map or ACL, or explicitly by using the CLI.

Note

When specifying CAPWAP as an attachment point, the core system filter is not used.

In some installations, you need to obtain authorization to modify the switch configuration, which can lead to extended delays if the approval process is lengthy. This can limit the ability of network administrators to monitor and analyze traffic. To address this situation, Wireshark supports explicit specification of core system filter match criteria from the EXEC mode CLI. The disadvantage is that the match criteria that you can specify is a limited subset of what class map supports, such as MAC, IP source and destination addresses, ether-type, IP protocol, and TCP/UDP source and destination ports.

If you prefer to use configuration mode, you can define ACLs or have class maps refer capture points to them. Explicit and ACL-based match criteria are used internally to construct class maps and policy maps.

Note The ACL and class map configuration are part of the system and not aspects of the Wireshark feature.

Display Filter

With the display filter, you can direct Wireshark to further narrow the set of packets to display when decoding and displaying from a .pcap file.

Related Topics

Additional References, on page 585

Actions

Wireshark can be invoked on live traffic or on a previously existing .pcap file. When invoked on live traffic, it can perform four types of actions on packets that pass its display filters:

- Captures to buffer in memory to decode and analyze and store
- Stores to a .pcap file
- Decodes and displays
Storage of Captured Packets to Buffer in Memory

Packets can be stored in the capture buffer in memory for subsequent decode, analysis, or storage to a .pcap file.

The capture buffer can be in linear or circular mode. In linear mode, new packets are discarded when the buffer is full. In circular mode, if the buffer is full, the oldest packets are discarded to accommodate the new packets. Although the buffer can also be cleared when needed, this mode is mainly used for debugging network traffic. However, it is not possible to only clear the contents of the buffer alone without deleting it. Stop the current captures and restart the capture again for this to take effect.

Note

If you have more than one capture that is storing packets in a buffer, clear the buffer before starting a new capture to avoid memory loss.

Storage of Captured Packets to a .pcap File

Note

When WireShark is used on switches in a stack, packet captures can be stored only on flash or USB flash devices connected to the active switch.

For example, if flash1 is connected to the active switch, and flash2 is connected to the secondary switch, only flash1 can be used to store packet captures.

Attempts to store packet captures on devices other than flash or USB flash devices connected to the active switch will probably result in errors.

Wireshark can store captured packets to a .pcap file. The capture file can be located on the following storage devices:

- Switch on-board flash storage (flash:)
- USB drive (usbflash0:)

Note

Attempts to store packet captures on unsupported devices or devices not connected to the active switch will probably result in errors.

When configuring a Wireshark capture point, you can associate a filename. When the capture point is activated, Wireshark creates a file with the specified name and writes packets to it. If the file already exists at the time of creation of the capture point, Wireshark queries you as to whether the file can be overwritten. If the file already exists at the time of activating the capture point, Wireshark will overwrite the existing file. Only one capture point may be associated with a given filename.
If the destination of the Wireshark writing process is full, Wireshark fails with partial data in the file. You must ensure that there is sufficient space in the file system before you start the capture session. With Cisco IOS Release IOS XE 3.3.0(SE), the file system full status is not detected for some storage devices.

You can reduce the required storage space by retaining only a segment, instead of the entire packet. Typically, you do not require details beyond the first 64 or 128 bytes. The default behavior is to store the entire packet. To avoid possible packet drops when processing and writing to the file system, Wireshark can optionally use a memory buffer to temporarily hold packets as they arrive. Memory buffer size can be specified when the capture point is associated with a .pcap file.

Packet Decoding and Display

Wireshark can decode and display packets to the console. This functionality is possible for capture points applied to live traffic and for capture points applied to a previously existing .pcap file.

Note
Decoding and displaying packets may be CPU intensive.

Wireshark can decode and display packet details for a wide variety of packet formats. The details are displayed by entering the `monitor capture name start` command with one of the following keyword options, which place you into a display and decode mode:

- **brief**—Displays one line per packet (the default).
- **detailed**—Decodes and displays all the fields of all the packets whose protocols are supported. Detailed modes require more CPU than the other two modes.
- **(hexadecimal) dump**—Displays one line per packet as a hexadecimal dump of the packet data and the printable characters of each packet.

When you enter the `capture` command with the decode and display option, the Wireshark output is returned to Cisco IOS and displayed on the console unchanged.

Live Traffic Display

Wireshark receives copies of packets from the core system. Wireshark applies its display filters to discard uninteresting packets, and then decodes and displays the remaining packets.

.pcap File Display

Wireshark can decode and display packets from a previously stored .pcap file and direct the display filter to selectively displayed packets.

Packet Storage and Display

Functionally, this mode is a combination of the previous two modes. Wireshark stores packets in the specified .pcap file and decodes and displays them to the console. Only the core filters are applicable here.
Wireshark Capture Point Activation and Deactivation

After a Wireshark capture point has been defined with its attachment points, filters, actions, and other options, it must be activated. Until the capture point is activated, it does not actually capture packets.

Before a capture point is activated, some functional checks are performed. A capture point cannot be activated if it has neither a core system filter nor attachment points defined. Attempting to activate a capture point that does not meet these requirements generates an error.*

*When performing a wireless capture with a CAPWAP tunneling interface, the core system filter is not required and cannot be used.

The display filters are specified as needed.

After Wireshark capture points are activated, they can be deactivated in multiple ways. A capture point that is storing only packets to a .pcap file can be halted manually or configured with time or packet limits, after which the capture point halts automatically.

When a Wireshark capture point is activated, a fixed rate policer is applied automatically in the hardware so that the CPU is not flooded with Wireshark-directed packets. The disadvantage of the rate policer is that you cannot capture contiguous packets beyond the established rate even if more resources are available.

The set packet capture rate is 1000 packets per sec (pps). The 1000 pps limit is applied to the sum of all attachment points. For example, if we have a capture session with 3 attachment points, the rates of all 3 attachment points added together is policed to 1000 pps.

Policer is not supported for control-plane packet capture. When activating control-plane capture points, you need to be extra cautious, so that it does not flood the CPU.

Wireshark Features

This section describes how Wireshark features function in the switch environment:

- If port security and Wireshark are applied on an ingress capture, a packet that is dropped by port security will still be captured by Wireshark. If port security is applied on an ingress capture, and Wireshark is applied on an egress capture, a packet that is dropped by port security will not be captured by Wireshark.

- Packets dropped by Dynamic ARP Inspection (DAI) are not captured by Wireshark.

- If a port that is in STP blocked state is used as an attachment point and the core filter is matched, Wireshark will capture the packets that come into the port, even though the packets will be dropped by the switch.

- Classification-based security features—Packets that are dropped by input classification-based security features (such as ACLs and IPSG) are not caught by Wireshark capture points that are connected to attachment points at the same layer. In contrast, packets that are dropped by output classification-based security features are caught by Wireshark capture points that are connected to attachment points at the same layer. The logical model is that the Wireshark attachment point occurs after the security feature lookup on the input side, and symmetrically before the security feature lookup on the output side.
On ingress, a packet goes through a Layer 2 port, a VLAN, and a Layer 3 port/SVI. On egress, the packet goes through a Layer 3 port/SVI, a VLAN, and a Layer 2 port. If the attachment point is before the point where the packet is dropped, Wireshark will capture the packet. Otherwise, Wireshark will not capture the packet. For example, Wireshark capture policies connected to Layer 2 attachment points in the input direction capture packets dropped by Layer 3 classification-based security features. Symmetrically, Wireshark capture policies attached to Layer 3 attachment points in the output direction capture packets dropped by Layer 2 classification-based security features.

- Routed ports and switch virtual interfaces (SVIs)—Wireshark cannot capture the output of an SVI because the packets that go out of an SVI's output are generated by CPU. To capture these packets, include the control plane as an attachment point.
- VLANs—Starting with Cisco IOS Release 16.1, when a VLAN is used as a Wireshark attachment point, packet capture is supported on L2 and L3 in both input and output directions.
- Redirection features—In the input direction, features traffic redirected by Layer 3 (such as PBR and WCCP) are logically later than Layer 3 Wireshark attachment points. Wireshark captures these packets even though they might later be redirected out another Layer 3 interface. Symmetrically, output features redirected by Layer 3 (such as egress WCCP) are logically prior to Layer 3 Wireshark attachment points, and Wireshark will not capture them.
- SPAN—Wireshark cannot capture packets on interface configured as a SPAN destination.
- SPAN—Wireshark is able to capture packets on interfaces configured as a SPAN source in the ingress direction, and may be available for egress direction too.
- You can capture packets from a maximum of 1000 VLANs at a time, if no ACLs are applied. If ACLs are applied, the hardware will have less space for Wireshark to use. As a result, the maximum number of VLANs than can be used for packet capture at a time will be lower. Using more than 1000 VLANs tunnels at a time or extensive ACLs might have unpredictable results. For example, mobility may go down.

Note: Capturing an excessive number of attachment points at the same time is strongly discouraged because it may cause excessive CPU utilization and unpredictable hardware behavior.

**Wireless Packet Capture in Wireshark**

- Wireless traffic is encapsulated inside CAPWAP packets. However, capturing only a particular wireless client's traffic inside a CAPWAP tunnel is not supported when using the CAPWAP tunnel as an attachment point. To capture only a particular wireless client's traffic, use the client VLAN as an attachment point and formulate the core filter accordingly.
- Limited decoding of inner wireless traffic is supported. Decoding of inner wireless packets inside encrypted CAPWAP tunnels is not supported.
- No other interface type can be used with the CAPWAP tunneling interface on the same capture point. A CAPWAP tunneling interface and a Level 2 port cannot be attachment points on the same capture point.
- You cannot specify a core filter when capturing packets for Wireshark via the CAPWAP tunnel. However, you can use the Wireshark display filters for filtering wireless client traffic against a specific wireless client.
Guidelines for Wireshark

- You can capture packets from a maximum of 135 CAPWAP tunnels at a time if no ACLs are applied. If ACLs are applied, the hardware memory will have less space for Wireshark to use. As a result, the maximum number of CAPWAP tunnels than can be used for packet capture at a time will be lower. Using more than 135 CAPWAP tunnels at a time or using extensive ACLs might have unpredictable results. For example, mobility may go down.

  **Note**  
  Capturing an excessive number of attachment points at the same time is strongly discouraged because it may cause excessive CPU utilization and unpredictable hardware behavior.

- During Wireshark packet capture, hardware forwarding happens concurrently.
- Before starting a Wireshark capture process, ensure that CPU usage is moderate and that sufficient memory (at least 200 MB) is available.
- If you plan to store packets to a storage file, ensure that sufficient space is available before beginning a Wireshark capture process.
- The CPU usage during Wireshark capture depends on how many packets match the specified conditions and on the intended actions for the matched packets (store, decode and display, or both).
- Where possible, keep the capture to the minimum (limit by packets, duration) to avoid high CPU usage and other undesirable conditions.
- Because packet forwarding typically occurs in hardware, packets are not copied to the CPU for software processing. For Wireshark packet capture, packets are copied and delivered to the CPU, which causes an increase in CPU usage.

  To avoid high CPU usage, do the following:
  - Attach only relevant ports.
  - Use a class map, and secondarily, an access list to express match conditions. If neither is viable, use an explicit, in-line filter.
  - Adhere closely to the filter rules. Restrict the traffic type (such as, IPv4 only) with a restrictive, rather than relaxed ACL, which elicits unwanted traffic.
  - Always limit packet capture to either a shorter duration or a smaller packet number. The parameters of the capture command enable you to specify the following:
    - Capture duration
    - Number of packets captured
    - File size
    - Packet segment size
  - Run a capture session without limits if you know that very little traffic matches the core filter.
• You might experience high CPU (or memory) usage if:
  • You leave a capture session enabled and unattended for a long period of time, resulting in unanticipated bursts of traffic.
  • You launch a capture session with ring files or capture buffer and leave it unattended for a long time, resulting in performance or system health issues.

• During a capture session, watch for high CPU usage and memory consumption due to Wireshark that may impact switch performance or health. If these situations arise, stop the Wireshark session immediately.

• Avoid decoding and displaying packets from a .pcap file for a large file. Instead, transfer the .pcap file to a PC and run Wireshark on the PC.

• You can define up to eight Wireshark instances. An active `show` command that decodes and displays packets from a .pcap file or capture buffer counts as one instance. However, only one of the instances can be active.

• Whenever an ACL that is associated with a running capture is modified, you must restart the capture for the ACL modifications to take effect. If you do not restart the capture, it will continue to use the original ACL as if it had not been modified.

• To avoid packet loss, consider the following:
  • Use store-only (when you do not specify the display option) while capturing live packets rather than decode and display, which is a CPU-intensive operation (especially in detailed mode).
  • If you have more than one capture that is storing packets in a buffer, clear the buffer before starting a new capture to avoid memory loss.
  • If you use the default buffer size and see that you are losing packets, you can increase the buffer size to avoid losing packets.
  • Writing to flash disk is a CPU-intensive operation, so if the capture rate is insufficient, you may want to use a buffer capture.
  • The Wireshark capture session always operates in streaming mode at the rate of 1000 pps.

• The streaming capture mode rate is 1000 pps.
• If you want to decode and display live packets in the console window, ensure that the Wireshark session is bounded by a short capture duration.

⚠️ Warning

A Wireshark session with either a longer duration limit or no capture duration (using a terminal with no auto-more support using the `term len 0` command) may make the console or terminal unusable.

• When using Wireshark to capture live traffic that leads to high CPU, usage, consider applying a QoS policy temporarily to limit the actual traffic until the capture process concludes.

• All Wireshark-related commands are in EXEC mode; no configuration commands exist for Wireshark. If you need to use access list or class-map in the Wireshark CLI, you must define an access list and class map with configuration commands.
• No specific order applies when defining a capture point; you can define capture point parameters in any order, provided that CLI allows this. The Wireshark CLI allows as many parameters as possible on a single line. This limits the number of commands required to define a capture point.

• All parameters except attachment points take a single value. Generally, you can replace the value with a new one by reentering the command. After user confirmation, the system accepts the new value and overrides the older one. A no form of the command is unnecessary to provide a new value, but it is necessary to remove a parameter.

• Wireshark allows you to specify one or more attachment points. To add more than one attachment point, reenter the command with the new attachment point. To remove an attachment point, use the no form of the command. You can specify an interface range as an attachment point. For example, enter `monitor capture mycap interface GigabitEthernet1/0/1 in` where interface GigabitEthernet1/0/1 is an attachment point.

If you also need to attach interface GigabitEthernet1/0/2, specify it in another line as follows:

`monitor capture mycap interface GigabitEthernet1/0/2 in`

• You cannot make changes to a capture point when the capture is active.

• The action you want to perform determines which parameters are mandatory. The Wireshark CLI allows you to specify or modify any parameter prior to entering the `start` command. When you enter the `start` command, Wireshark will start only after determining that all mandatory parameters have been provided.

• If the file already exists at the time of creation of the capture point, Wireshark queries you as to whether the file can be overwritten. If the file already exists at the time of activating the capture point, Wireshark will overwrite the existing file.

• The core filter can be an explicit filter, access list, or class map. Specifying a newer filter of these types replaces the existing one.

  **Note**  
  A core filter is required except when using a CAPWAP tunnel interface as a capture point attachment point.

• You can terminate a Wireshark session with an explicit `stop` command or by entering `q` in automore mode. The session could terminate itself automatically when a stop condition such as duration or packet capture limit is met, or if an internal error occurs, or resource is full (specifically if disk is full in file mode).

• Dropped packets will not be shown at the end of the capture. However, only the count of dropped, oversized packets will be displayed.

### Default Wireshark Configuration

The table below shows the default Wireshark configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>No limit</td>
</tr>
<tr>
<td>Packets</td>
<td>No limit</td>
</tr>
</tbody>
</table>
How to Configure Wireshark

To configure Wireshark, perform these basic steps.

1. Define a capture point.
2. (Optional) Add or modify the capture point's parameters.
3. Activate or deactivate a capture point.
4. Delete the capture point when you are no longer using it.

Related Topics
- Defining a Capture Point, on page 553
- Adding or Modifying Capture Point Parameters, on page 558
- Deleting Capture Point Parameters, on page 560
- Deleting a Capture Point, on page 562
- Activating and Deactivating a Capture Point, on page 563
- Clearing the Capture Point Buffer, on page 566
- Example: Simple Capture and Display, on page 571
- Example: Simple Capture and Store, on page 572
- Example: Using Buffer Capture, on page 575
- Example: Capture Sessions, on page 581
- Example: Capture and Store in Lock-step Mode, on page 582
- Example: Simple Capture and Store of Packets in Egress Direction, on page 583

Defining a Capture Point

The example in this procedure defines a very simple capture point. If you choose, you can define a capture point and all of its parameters with one instance of the monitor capture command.

Note

You must define an attachment point, direction of capture, and core filter to have a functional capture point. An exception to needing to define a core filter is when you are defining a wireless capture point using a CAPWAP tunneling interface. In this case, you do not define your core filter. It cannot be used.

Follow these steps to define a capture point.
## Defining a Capture Point

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show capwap summary</code></td>
<td>Displays the CAPWAP tunnels available as attachment points for a wireless capture.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show capwap summary</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`monitor capture {capture-name} {interface interface-type interface-id</td>
<td>control-plane} {in</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# monitor capture mycap interface GigabitEthernet1/0/1 in</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>• GigabitEthernet — Specifies the attachment point as GigabitEthernet.</td>
<td></td>
</tr>
<tr>
<td>• vlan — Specifies the attachment point as a VLAN.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>Only ingress capture (in) is allowed when using this interface as an attachment point.</td>
</tr>
<tr>
<td>• capwap — Specifies the attachment point as a CAPWAP tunnel.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>When using this interface as an attachment point, a core filter cannot be used.</td>
</tr>
<tr>
<td>• (Optional) control-plane — Specifies the control plane as an attachment point.</td>
<td></td>
</tr>
<tr>
<td>• in</td>
<td>out</td>
</tr>
</tbody>
</table>

**Step 4**

```
monitor capture {capture-name} [match {any | ipv4 any any | ipv6 any any}]]
```

**Example:**
```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in match any
```

Defines the core system filter.

**Note** When using the CAPWAP tunneling interface as an attachment point, do not perform this step because a core filter cannot be used.

The keywords have these meanings:

• *capture-name* — Specifies the name of the capture point to be defined (mycap is used in the example).

• *match* — Specifies a filter. The first filter defined is the core filter.

**Note** A capture point cannot be activated if it has neither a core system filter nor attachment points defined. Attempting to activate a capture point that does not meet these requirements generates an error.

• *ipv4* — Specifies an IP version 4 filter.

• *ipv6* — Specifies an IP version 6 filter.
### Defining a Capture Point

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>Displays the capture point parameters that you defined in Step 2 and confirms that you defined a capture point.</td>
</tr>
<tr>
<td><code>show monitor capture {capture-name} [parameter]</code></td>
<td>Displays the capture point parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>show monitor capture mycap parameter</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>monitor capture mycap interface GigabitEthernet1/0/1 in</td>
</tr>
<tr>
<td></td>
<td>monitor capture mycap match any</td>
</tr>
</tbody>
</table>

| **Step 6** | Verifies your entries. |
| `show running-config` | |
| **Example:** | |
| Switch# `show running-config` | |

| **Step 7** | (Optional) Saves your entries in the configuration file. |
| `copy running-config startup-config` | |
| **Example:** | |
| Switch# `copy running-config startup-config` | |

### Example

To define a capture point with a CAPWAP attachment point:

```
Switch# `show capwap summary`
```
CAPWAP Tunnels General Statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>PhyPortIf</th>
<th>Mode</th>
<th>McastIf</th>
</tr>
</thead>
<tbody>
<tr>
<td>data</td>
<td>Gi3/0/6</td>
<td>unicast</td>
<td>-</td>
</tr>
</tbody>
</table>

```
Name  APName          Type PhyPortIf Mode McastIf
-----  ---------------  ---- --------- --------- -----
Ca0    AP442b.03a9.6715 data Gi3/0/6 unicast -

```
```
Name  SrcIP SrcPort DestIP DstPort DtlsEn MTU Xact
-----  --------- -------- -------- -------- ------ ---- -----
Ca0    10.10.14.32 5247     10.10.14.2 38514  No     1449  0    |
```

Switch# `monitor capture mycap interface capwap 0 both`
Switch# `monitor capture mycap file location flash:mycap.pcap`
Switch# `monitor capture mycap file buffer-size 1`
Switch# `monitor capture mycap start`

*Aug 20 11:02:21.983: %BUFCAP-6-ENABLE: Capture Point mycap enabled.*

Switch# `show monitor capture mycap parameter`
```
monitor capture mycap interface capwap 0 in
monitor capture mycap interface capwap 0 out
monitor capture mycap file location flash:mycap.pcap buffer-size 1
```
Switch#
Switch# show monitor capture mycap

Status Information for Capture mycap
Target Type: CAPWAP
Interface: CAPWAP
Ingress: 0
Egress: 0
Status : Active
Filter Details:
Capture all packets
Buffer Details:
Buffer Type: LINEAR (default)
File Details:
Associated file name: flash:mycap.pcap
Size of buffer(in MB): 1
Limit Details:
Number of Packets to capture: 0 (no limit)
Packet Capture duration: 0 (no limit)
Packets per second: 0 (no limit)
Packet Size to capture: 0 (no limit)
Packet sampling rate: 0 (no sampling)

Switch# show monitor capture file flash:mycap.pcap

1 0.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
2 0.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
3 2.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
4 2.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
5 3.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
6 4.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
7 4.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
8 5.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
9 5.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
10 6.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
11 8.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
12 9.225986 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
13 9.225986 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
14 9.225986 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
15 9.231998 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
16 9.231998 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
17 9.231998 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
18 9.236987 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
19 10.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
20 10.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
21 12.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0, Flags=........
22 12.239993 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
23 12.244997 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
24 12.244997 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
25 12.250994 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
What to do next

You can add additional attachment points, modify the parameters of your capture point, then activate it, or if you want to use your capture point just as it is, you can now activate it.

**Note**

You cannot change a capture point's parameters using the methods presented in this topic.

If the user enters an incorrect capture name, or an invalid/non existing attachment point, the switch will show errors like "Capture Name should be less than or equal to 8 characters. Only alphanumeric characters and underscore (_) is permitted" and "%Invalid input detected at '^' marker" respectively.

**Related Topics**

- How to Configure Wireshark, on page 553
- Capture Points, on page 543
- Attachment Points, on page 544
- Example: Simple Capture and Display, on page 571
- Example: Simple Capture and Store, on page 572
- Example: Using Buffer Capture, on page 575
- Example: Capture Sessions, on page 581
- Example: Capture and Store in Lock-step Mode, on page 582
- Example: Simple Capture and Store of Packets in Egress Direction, on page 583

---

## Adding or Modifying Capture Point Parameters

Although listed in sequence, the steps to specify values for the parameters can be executed in any order. You can also specify them in one, two, or several lines. Except for attachment points, which can be multiple, you can replace any value with a more recent value by redefining the same option. You will need to confirm interactively when certain parameters already specified are being modified.

Follow these steps to modify a capture point's parameters.

### Before you begin

A capture point must be defined before you can use these instructions.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **1**  | enable            | Enables privileged EXEC mode.  
| Example: |                   | • Enter your password if prompted. |
### Command or Action

**Switch> enable**

### Purpose

**Step 2**

`monitor capture {capture-name} match {any | mac mac-match-string | ipv4 {any | host | protocol} {any | host} | ipv6 {any | host | protocol} {any | host}}`

**Example:**

```
Switch# monitor capture mycap match ipv4 any any
```

Defines the core system filter (**ipv4 any any**), defined either explicitly, through ACL or through a class map.

**Note** If you are defining a wireless capture point using a CAPWAP tunneling interface, this command will have no effect, so it should not be used.

**Step 3**

`monitor capture {capture-name} limit { [duration seconds] [packet-length size] [packets num] }`

**Example:**

```
Switch# monitor capture mycap limit
duration 60 packet-len 400
```

Specifies the session limit in seconds (60), packets captured, or the packet segment length to be retained by Wireshark (400).

**Step 4**

`monitor capture {capture-name} file {location filename}`

**Example:**

```
Switch# monitor capture mycap file
location flash:mycap.pcap
```

Specifies the file association, if the capture point intends to capture packets rather than only display them.

**Note** If the file already exists, you have to confirm if it can be overwritten.

**Note** File option does not exist on LAN base license.

**Step 5**

`monitor capture {capture-name} file {buffer-size size}`

**Example:**

```
Switch# monitor capture mycap file
buffer-size 100
```

Specifies the size of the memory buffer used by Wireshark to handle traffic bursts.

**Step 6**

`show monitor capture {capture-name} [parameter]`

**Example:**

```
Switch# show monitor capture mycap parameter
monitor capture mycap interface
GigabitEthernet1/0/1 in
  monitor capture mycap match ipv4 any any
  monitor capture mycap limit duration 60 packet-len 400
  monitor capture point mycap file
   location bootdisk:mycap.pcap
  monitor capture mycap file buffer-size 100
```

Displays the capture point parameters that you defined previously.
### Deleting Capture Point Parameters

Although listed in sequence, the steps to delete parameters can be executed in any order. You can also delete them in one, two, or several lines. Except for attachment points, which can be multiple, you can delete any parameter.

Follow these steps to delete a capture point's parameters.

### Before you begin

A capture point parameter must be defined before you can use these instructions to delete it.

---

**Deleting Capture Point Parameters**

Although listed in sequence, the steps to delete parameters can be executed in any order. You can also delete them in one, two, or several lines. Except for attachment points, which can be multiple, you can delete any parameter.

Follow these steps to delete a capture point's parameters.

### Before you begin

A capture point parameter must be defined before you can use these instructions to delete it.

---

**Examples**

**Modifying Parameters**

**Associating or Disassociating a Capture File**

Switch# monitor capture point mycap file location flash:mycap.pcap
Switch# no monitor capture mycap file

**Specifying a Memory Buffer Size for Packet Burst Handling**

Switch# monitor capture mycap buffer size 100

**Defining an Explicit Core System Filter to Match Both IPv4 and IPv6**

Switch# monitor capture mycap match any

**What to do next**

If your capture point contains all of the parameters you want, activate it.

**Related Topics**

- *How to Configure Wireshark*, on page 553
- *Capture Points*, on page 543
- *Attachment Points*, on page 544
- *Example: Simple Capture and Display*, on page 571
- *Example: Simple Capture and Store*, on page 572
- *Example: Using Buffer Capture*, on page 575
- *Example: Capture Sessions*, on page 581
- *Example: Capture and Store in Lock-step Mode*, on page 582
- *Example: Simple Capture and Store of Packets in Egress Direction*, on page 583
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Deletes all filters defined on capture point (mycap).</td>
</tr>
<tr>
<td><code>no monitor capture {capture-name} match</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>no monitor capture mycap match</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Deletes the session time limit and the packet segment length to be retained by Wireshark. It leaves other specified limits in place. Deletes all limits on Wireshark.</td>
</tr>
<tr>
<td><code>no monitor capture {capture-name} limit [duration] [packet-length] [packets]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>no monitor capture mycap limit duration packet-len</code></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>no monitor capture mycap limit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Deletes the file association. The capture point will no longer capture packets. It will only display them. Deletes the file location association. The file location will no longer be associated with the capture point. However, other defined file association will be unaffected by this action.</td>
</tr>
<tr>
<td><code>no monitor capture {capture-name} file [location] [buffer-size]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>no monitor capture mycap file location</code></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>no monitor capture mycap file location</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Displays the capture point parameters that remain defined after your parameter deletion operations. This command can be run at any point in the procedure to see what parameters are associated with a capture point.</td>
</tr>
<tr>
<td><code>show monitor capture {capture-name} [parameter]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>show monitor capture mycap parameter</code></td>
<td></td>
</tr>
<tr>
<td><code>monitor capture mycap interface GigabitEthernet1/0/1 in</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch{config)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

### What to do next

If your capture point contains all of the parameters you want, activate it.

### Note

If the parameters are deleted when the capture point is active, the switch will show an error "Capture is active".
Deleting a Capture Point

Follow these steps to delete a capture point.

**Before you begin**

A capture point must be defined before you can use these instructions to delete it. You have to stop the capture point before you can delete it.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>no monitor capture {capture-name}</td>
<td>Deletes the specified capture point (mycap).</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# no monitor capture mycap</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>show monitor capture {capture-name} [ parameter ]</td>
<td>Displays a message indicating that the specified capture point does not exist because it has been deleted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# show monitor capture mycap parameter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Capture mycap does not exist</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Activating and Deactivating a Capture Point

Follow these steps to activate or deactivate a capture point.

**Before you begin**

A capture point can be activated even if an attachment point and a core system filter have been defined and the associated filename already exists. In such an instance, the existing file will be overwritten.

A capture point with no associated filename can only be activated to display. When the filename is not specified, the packets are captured into the buffer. Live display (display during capture) is available in both file and buffer modes.

If no display filters are specified, packets are not displayed live, and all the packets captured by the core system filter are displayed. The default display mode is brief.

---

**Note**

When using a CAPWAP tunneling interface as an attachment point, core filters are not used, so there is no requirement to define them in this case.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><strong>copy running-config startup-config</strong></td>
<td><em>(Optional) Saves your entries in the configuration file.</em></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

---

**What to do next**

You can define a new capture point with the same name as the one you deleted. These instructions are usually performed when one wants to start over with defining a capture point.

**Related Topics**

- How to Configure Wireshark, on page 553
- Capture Points, on page 543
- Attachment Points, on page 544
- Example: Simple Capture and Display, on page 571
- Example: Simple Capture and Store, on page 572
- Example: Using Buffer Capture, on page 575
- Example: Capture Sessions, on page 581
- Example: Capture and Store in Lock-step Mode, on page 582
- Example: Simple Capture and Store of Packets in Egress Direction, on page 583
## Activating and Deactivating a Capture Point

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable` | Enables privileged EXEC mode.  

- Enter your password if prompted. |
| **Example:** | | |
| | `Switch> enable` |
| **Step 2** | `monitor capture {capture-name} start [display | display-filter | filter-string]} [brief | detailed | dump]`

- Activates a capture point and filters the display, so only packets containing "stp" are displayed. |
| **Example:** | | |
| | `Switch# monitor capture mycap start display display-filter "stp"` |
| **Step 3** | `monitor capture {capture-name} stop`

- Deactivates a capture point. |
| **Example:** | | |
| | `Switch# monitor capture name stop` |
| **Step 4** | `end`

- Returns to privileged EXEC mode. |
| **Example:** | | |
| | `Switch(config)# end` |
| **Step 5** | `show running-config`

- Verifies your entries. |
| **Example:** | | |
| | `Switch# show running-config` |
| **Step 6** | `copy running-config startup-config`

- (Optional) Saves your entries in the configuration file. |
| **Example:** | | |
| | `Switch# copy running-config startup-config` |

### What to do next

While activating and deactivating a capture point, you could encounter a few errors. Here are examples of some of the possible errors.

**Missing attachment point on activation**

```bash
Switch#monitor capture mycap match any
Switch#monitor capture mycap start
No Target is attached to capture failed to disable provision feature failed to remove policy failed to disable provision feature failed to remove policy failed to disable provision feature failed to remove policy
Capture statistics collected at software (Buffer):
```

---

Network Management |  
---
Capture duration - 0 seconds
Packets received - 0
Packets dropped - 0
Packets oversized - 0

Unable to activate Capture.
Switch# unable to get action unable to get action unable to get action
Switch#

monitor capture mycap interface g1/0/1 both
Switch#

monitor capture mycap start
Switch#

*Nov 5 12:33:43.906: %BUFCAP-6-ENABLE: Capture Point mycap enabled.

Missing filter on activation
Switch#monitor capture mycap int g1/0/1 both
Switch#monitor capture mycap start
Switch#

Capture statistics collected at software (Buffer):
Capture duration - 0 seconds
Packets received - 0
Packets dropped - 0
Packets oversized - 0

Unable to activate Capture.
Switch#monitor capture mycap match any
Switch#monitor capture mycap start
Switch#

*Nov 5 12:35:37.200: %BUFCAP-6-ENABLE: Capture Point mycap enabled.

Attempting to activate a capture point while another one is already active
Switch#monitor capture mycap start
PD start invoked while previous run is active Failed to start capture : Wireshark operation failure
Unable to activate Capture.
Switch#show monitor capture

Status Information for Capture test
Target Type:
Interface: GigabitEthernet1/0/13, Direction: both
Interface: GigabitEthernet1/0/14, Direction: both
Status : Active
Filter Details:
Capture all packets
Buffer Details:
Buffer Type: LINEAR (default)
Buffer Size (in MB): 10
File Details:
Associated file name: flash:cchh.pcap
Limit Details:
Number of Packets to capture: 0 (no limit)
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Maximum number of packets to capture per second: 1000
Packet sampling rate: 0 (no sampling)

Status Information for Capture mycap
Target Type:
Interface: GigabitEthernet1/0/1, Direction: both
Status : Inactive
Filter Details:
Capture all packets
Buffer Details:
Buffer Type: LINEAR (default)
Buffer Size (in MB): 10
Clearing the Capture Point Buffer

Follow these steps to clear the buffer contents or save them to an external file for storage.

Note

If you have more than one capture that is storing packets in a buffer, clear the buffer before starting a new capture to avoid memory loss. Do not try to clear buffer on an active capture point.

Note

Clearing buffer on an active capture point is supported only on Lan Base as this only clears the content. On all other licenses, it deletes the buffer itself, hence cannot be run during active capture.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

### Step 2

**monitor capture {capture-name} [clear | export filename]**

**Example:**

Switch# monitor capture mycap clear

**Clear - Completely deletes the buffer.**

**Note**

- When the clear command is run, the command deletes the buffer itself.
- On Lan base - the command clears the buffer contents without deleting the buffer.

**Export - Saves the captured packets in the buffer as well as deletes the buffer.**

### Step 3

**end**

**Example:**

Switch(config)# end

**Returns to privileged EXEC mode.**

### Step 4

**show running-config**

**Example:**

Switch# show running-config

**Verifies your entries.**

### Step 5

**copy running-config startup-config**

**Example:**

Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.

---

**Examples: Capture Point Buffer Handling**

**Exporting Capture to a File**

Switch# monitor capture mycap export flash:mycap.pcap

Storage configured as File for this capture

**Clearing Capture Point Buffer**

Switch# monitor capture mycap clear

Capture configured with file options
Monitoring Wireshark

The commands in this table are used to monitor Wireshark.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show monitor capture [capture-name ]</td>
<td>Displays the capture point state so that you can see what capture points are defined, what their attributes are, and whether they are active. When capture point name is specified, it displays specific capture point's details.</td>
</tr>
<tr>
<td>show monitor capture parameter</td>
<td>Displays the capture point parameters.</td>
</tr>
<tr>
<td>show capwap summary</td>
<td>Displays all the CAPWAP tunnels on the switch. Use this command to determine which CAPWAP tunnels are available to use for a wireless capture.</td>
</tr>
</tbody>
</table>

Configuration Examples for Wireshark

Example: Displaying a Brief Output from a .pcap File

You can display the output from a .pcap file by entering:

```
Switch# show monitor capture file flash:mycap.pcap brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
```
Example: Displaying Detailed Output from a .pcap File

You can display the detailed .pcap file output by entering:

Switch# show monitor capture file flash:mycap.pcap detailed
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Interface id: 0
Encapsulation type: Ethernet (1)
Arrival Time: Nov 6, 2015 11:44:48.322497000 UTC
[Time shift for this packet: 0.000000000 seconds]
Example: Displaying Detailed Output from a .pcap File

Epoch Time: 1446810288.322497000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 114 bytes (912 bits)
Capture Length: 114 bytes (912 bits)
[Frame is marked: False]
[Frame is ignored: False]


Destination: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
Address: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)

...0 . . . . . . . . . . . . = LG bit: Globally unique address (factory default)
...

...

Type: IP (0x0800)

Internet Protocol Version 4, Src: 10.10.10.2 (10.10.10.2), Dst: 10.10.10.1 (10.10.10.1)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

0000 00.. = Differentiated Services Codepoint: Default - (0x00)
.... .00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport)
(0x00)

Total Length: 100
Identification: 0x04ba (1210)
Flags: 0x00
 0... .... = Reserved bit: Not set
 .0. .... = Don't fragment: Not set
 ...0 .... = More fragments: Not set
Fragment offset: 0
Time to live: 254
Protocol: ICMP (1)
Header checksum: 0x8fc8 [validation disabled]
[Good: False]
[Bad: False]
Source: 10.10.10.2 (10.10.10.2)
Destination: 10.10.10.1 (10.10.10.1)

Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xe4db [correct]
Identifier (BE): 46 (0x002e)
Identifier (LE): 11776 (0x2e00)
Sequence number (BE): 0 (0x0000)
Sequence number (LE): 0 (0x0000)
Data (72 bytes)

0000 00 00 00 00 09 c9 8f 77 ab cd ab cd ab cd ab cd .........w........
0010 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd ................
0020 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd ............
0030 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd ............
0040 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd ............

Data: 0000000009c98f77abcdabccdcdaabcabccdcda...[Length: 72]

Frame 2: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Interface id: 0
Example: Simple Capture and Display

This example shows how to monitor traffic in the Layer 3 interface Gigabit Ethernet 1/0/1:

**Step 1:** Define a capture point to match on the relevant traffic by entering:

```
Switch# monitor capture mycap interface GigabitEthernet1/0/3 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap limit duration 60 packets 50
Switch# monitor capture mycap buffer size 100
```

To avoid high CPU utilization, a low packet count and duration as limits has been set.

**Step 2:** Confirm that the capture point has been correctly defined by entering:

```
Switch# show monitor capture mycap parameter
Switch# show monitor capture mycap
```

Status Information for Capture mycap

Target Type:
Interface: GigabitEthernet1/0/3, Direction: in
Status : Inactive
Filter Details:
IPv4
Source IP: any
Destination IP: any
Protocol: any
Buffer Details:
Buffer Type: LINEAR (default)
Buffer Size (in MB): 100
File Details:
File not associated
Limit Details:
Number of Packets to capture: 50
Packet Capture duration: 60
Packet Size to capture: 0 (no limit)
Packet sampling rate: 0 (no sampling)

**Step 3:** Start the capture process and display the results.

```
Switch# monitor capture mycap start display
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
```

```
1 0.000000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0030, seq=0/0, ttl=254
2 0.003682 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0030, seq=1/256, ttl=254
3 0.006586 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0030, seq=2/512, ttl=254
4 0.008941 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0030, seq=3/768, ttl=254
5 0.011138 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0030, seq=4/1024, ttl=254
6 0.014099 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0030, seq=5/1280, ttl=254
7 0.016868 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0030, seq=6/1536, ttl=254
8 0.019210 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0030,
```
Step 4: Delete the capture point by entering:

```
Switch# no monitor capture mycap
```

**Note**

A stop command is not required in this particular case since we have set a limit and the capture will automatically stop once that limit is reached.

For more information on syntax to be used for pcap statistics, refer the "Additional References" section.

**Related Topics**

- Defining a Capture Point, on page 553
- Adding or Modifying Capture Point Parameters, on page 558
- Deleting Capture Point Parameters, on page 560
- Deleting a Capture Point, on page 562
- Activating and Deactivating a Capture Point, on page 563
- Clearing the Capture Point Buffer, on page 566
- How to Configure Wireshark, on page 553
- Capture Points, on page 543
- Attachment Points, on page 544

**Example: Simple Capture and Store**

This example shows how to capture packets to a filter:

**Step 1:** Define a capture point to match on the relevant traffic and associate it to a file by entering:

```
Switch# monitor capture mycap interface GigabitEthernet1/0/3 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap limit duration 60 packets 50
Switch# monitor capture mycap file location flash:mycap.pcap
```

**Step 2:** Confirm that the capture point has been correctly defined by entering:

```
Switch# show monitor capture mycap parameter
  monitor capture mycap interface GigabitEthernet1/0/3 in
  monitor capture mycap match ipv4 any any
  monitor capture mycap file location flash:mycap.pcap
  monitor capture mycap limit packets 50 duration 60
```

```
Switch# show monitor capture mycap
```

**Status Information for Capture mycap**

- **Target Type:** Interface: GigabitEthernet1/0/3, Direction: in
- **Status:** Inactive
- **Filter Details:**
IPv4
Source IP: any
Destination IP: any
Protocol: any
Buffer Details:
  Buffer Type: LINEAR (default)
File Details:
  Associated file name: flash:mycap.pcap
Limit Details:
  Number of Packets to capture: 50
  Packet Capture duration: 60
  Packet Size to capture: 0 (no limit)
  Packet sampling rate: 0 (no sampling)

Step 3: Launch packet capture by entering:
Switch# monitor capture mycap start

Step 4: Display extended capture statistics during runtime by entering:
Switch# show monitor capture mycap capture-statistics
Capture statistics collected at software:
  Capture duration - 15 seconds
  Packets received - 40
  Packets dropped - 0
  Packets oversized - 0
  Packets errored - 0
  Packets sent - 40
  Bytes received - 7280
  Bytes dropped - 0
  Bytes oversized - 0
  Bytes errored - 0
  Bytes sent - 4560

Step 5: After sufficient time has passed, stop the capture by entering:
Switch# monitor capture mycap stop
Capture statistics collected at software (Buffer & Wireshark):
  Capture duration - 20 seconds
  Packets received - 50
  Packets dropped - 0
  Packets oversized - 0

Note
Alternatively, you could allow the capture operation stop automatically after the time has elapsed or the packet count has been met.
The mycap.pcap file now contains the captured packets.

Step 6: Display extended capture statistics after stop by entering:
Switch# show monitor capture mycap capture-statistics
Capture statistics collected at software:
  Capture duration - 20 seconds
  Packets received - 50
  Packets dropped - 0
  Packets oversized - 0
  Packets errored - 0
  Packets sent - 50
  Bytes received - 8190
Step 7: Display the packets by entering:

Switch# show monitor capture file flash:mycap.pcap
Starting the packet display .......... Press Ctrl + Shift + 6 to exit

1 0.000000000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0031, seq=0/0, ttl=254
2 0.002555000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0031, seq=1/256, ttl=254
3 0.006199000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0031, seq=2/512, ttl=254
4 0.009199000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0031, seq=3/768, ttl=254
5 0.011647000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0031, seq=4/1024, ttl=254
6 0.014168000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0031, seq=5/1280, ttl=254
7 0.016737000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0031, seq=6/1536, ttl=254
8 0.019403000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0031, seq=7/1792, ttl=254
9 0.022151000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0031, seq=8/2048, ttl=254
10 0.024722000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0031, seq=9/2304, ttl=254
11 0.026890000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0031, seq=10/2560, ttl=254
12 0.028862000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0031, seq=11/2816, ttl=254

--More--

For more information on syntax to be used for pcap statistics, refer the "Additional References" section.

Step 8: Delete the capture point by entering:

Switch# no monitor capture mycap

Related Topics
Defining a Capture Point, on page 553
Adding or Modifying Capture Point Parameters, on page 558
Deleting Capture Point Parameters, on page 560
Deleting a Capture Point, on page 562
Activating and Deactivating a Capture Point, on page 563
Clearing the Capture Point Buffer, on page 566
How to Configure Wireshark, on page 553
Capture Points, on page 543
Attachment Points, on page 544
Example: Using Buffer Capture

This example shows how to use buffer capture:

**Step 1:** Launch a capture session with the buffer capture option by entering:

```bash
Switch# monitor capture mycap interface GigabitEthernet1/0/3 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap buffer circular size 1
Switch# monitor capture mycap start
```

**Step 2:** Determine whether the capture is active by entering:

```bash
Switch# show monitor capture mycap
```

Status Information for Capture mycap
- **Target Type:** Interface: GigabitEthernet1/0/3, Direction: in
- **Status:** Active
- **Filter Details:**
  - IPv4
    - Source IP: any
    - Destination IP: any
  - Protocol: any
- **Buffer Details:**
  - Buffer Type: CIRCULAR
  - Buffer Size (in MB): 1
- **File Details:**
  - File not associated
- **Limit Details:**
  - Number of Packets to capture: 0 (no limit)
  - Packet Capture duration: 0 (no limit)
  - Packet Size to capture: 0 (no limit)
  - Maximum number of packets to capture per second: 1000
  - Packet sampling rate: 0 (no sampling)

**Step 3:** Display extended capture statistics during runtime by entering:

```bash
Switch# show monitor capture mycap capture-statistics
```

Capture statistics collected at software:
- Capture duration - 88 seconds
- Packets received - 1000
- Packets dropped - 0
- Packets oversized - 0
- Packets errored - 0
- Packets sent - 1000
- Bytes received - 182000
- Bytes dropped - 0
- Bytes oversized - 0
- Bytes errored - 0
- Bytes sent - 114000

**Step 4:** Stop the capture by entering:

```bash
Switch# monitor capture mycap stop
```

Capture statistics collected at software (Buffer):
- Capture duration - 2185 seconds
- Packets received - 51500
- Packets dropped - 0
- Packets oversized - 0

**Step 5:** Display extended capture statistics after stop by entering:
Switch# show monitor capture mycap capture-statistics
Capture statistics collected at software:
Capture duration - 156 seconds
Packets received - 2000
Packets dropped - 0
Packets oversized - 0
Packets errored - 0
Packets sent - 2000
Bytes received - 364000
Bytes dropped - 0
Bytes oversized - 0
Bytes errored - 0
Bytes sent - 228000

Step 6: Determine whether the capture is active by entering:

Switch# show monitor capture mycap
Status Information for Capture mycap
Target Type: Interface: GigabitEthernet1/0/3, Direction: in
Status : Inactive
Filter Details:
IPv4
Source IP: any
Destination IP: any
Protocol: any
Buffer Details:
Buffer Type: CIRCULAR
Buffer Size (in MB): 1
File Details:
File not associated
Limit Details:
Number of Packets to capture: 0 (no limit)
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Maximum number of packets to capture per second: 1000
Packet sampling rate: 0 (no sampling)

Step 7: Display the packets in the buffer by entering:

Switch# show monitor capture mycap buffer brief
Starting the packet display ......... Press Ctrl + Shift + 6 to exit

<table>
<thead>
<tr>
<th>Seq</th>
<th>Time</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>ID</th>
<th>Packet ID</th>
<th>TTL</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000000</td>
<td>10.10.10.2</td>
<td>10.10.10.1</td>
<td>ICMP</td>
<td>114</td>
<td>Echo (ping) request</td>
<td>0x0038,</td>
<td>154</td>
</tr>
<tr>
<td>2</td>
<td>0.000030</td>
<td>10.10.10.2</td>
<td>10.10.10.1</td>
<td>ICMP</td>
<td>114</td>
<td>Echo (ping) request</td>
<td>0x0038,</td>
<td>154</td>
</tr>
<tr>
<td>3</td>
<td>0.000052</td>
<td>10.10.10.2</td>
<td>10.10.10.1</td>
<td>ICMP</td>
<td>114</td>
<td>Echo (ping) request</td>
<td>0x0038,</td>
<td>154</td>
</tr>
<tr>
<td>4</td>
<td>0.000073</td>
<td>10.10.10.2</td>
<td>10.10.10.1</td>
<td>ICMP</td>
<td>114</td>
<td>Echo (ping) request</td>
<td>0x0038,</td>
<td>154</td>
</tr>
<tr>
<td>5</td>
<td>0.000094</td>
<td>10.10.10.2</td>
<td>10.10.10.1</td>
<td>ICMP</td>
<td>114</td>
<td>Echo (ping) request</td>
<td>0x0038,</td>
<td>154</td>
</tr>
<tr>
<td>6</td>
<td>0.000115</td>
<td>10.10.10.2</td>
<td>10.10.10.1</td>
<td>ICMP</td>
<td>114</td>
<td>Echo (ping) request</td>
<td>0x0038,</td>
<td>154</td>
</tr>
<tr>
<td>7</td>
<td>0.000137</td>
<td>10.10.10.2</td>
<td>10.10.10.1</td>
<td>ICMP</td>
<td>114</td>
<td>Echo (ping) request</td>
<td>0x0038,</td>
<td>154</td>
</tr>
<tr>
<td>8</td>
<td>0.000158</td>
<td>10.10.10.2</td>
<td>10.10.10.1</td>
<td>ICMP</td>
<td>114</td>
<td>Echo (ping) request</td>
<td>0x0038,</td>
<td>154</td>
</tr>
<tr>
<td>9</td>
<td>0.000179</td>
<td>10.10.10.2</td>
<td>10.10.10.1</td>
<td>ICMP</td>
<td>114</td>
<td>Echo (ping) request</td>
<td>0x0038,</td>
<td>154</td>
</tr>
<tr>
<td>10</td>
<td>0.000200</td>
<td>10.10.10.2</td>
<td>10.10.10.1</td>
<td>ICMP</td>
<td>114</td>
<td>Echo (ping) request</td>
<td>0x0038,</td>
<td>154</td>
</tr>
</tbody>
</table>
Notice that the packets have been buffered.

**Step 8: Display the packets in other display modes.**

Switch# show monitor capture mycap buffer detailed
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
  Interface id: 0
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 6, 2015 18:10:06.297972000 UTC
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1446833406.297972000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 114 bytes (912 bits)
  Capture Length: 114 bytes (912 bits)
  [Frame is marked: False]
  [Frame is ignored: False]

    Destination: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
    Address: Cisco_31:f1:c6 (00:e1:6d:31:f1:c6)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
    Internet Protocol Version 4, Src: 10.10.10.2 (10.10.10.2), Dst: 10.10.10.1 (10.10.10.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
       0000 00.. = Differentiated Services Codepoint: Default (0x00)
       .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport)
    (0x00)
    Total Length: 100
    Identification: 0xabdd (43997)
    Flags: 0x00
       0... .... = Reserved bit: Not set
       .0... .... = Don't fragment: Not set
       ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (1)
    Header checksum: 0xe8a4 [validation disabled]
       [Good: False]
       [Bad: False]
    Source: 10.10.10.2 (10.10.10.2)
    Destination: 10.10.10.1 (10.10.10.1)
    Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
Example: Using Buffer Capture

Checksum: 0xa620 [correct]
Identifier (BE): 56 (0x0038)
Identifier (LE): 14336 (0x3800)
Sequence number (BE): 40057 (0x9c79)
Sequence number (LE): 31132 (0x799c)
Data (72 bytes)

0000 00 00 00 0b 15 30 63 ab cd ab cd ab cd ab cd ........0c........
0010 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ...................
0020 ab cd ab cd ab cd ab cd ab cd ab cd ab cd .................
0030 ab cd ab cd ab cd ab cd ab cd ab cd ab cd .................
0040 ab cd ab cd ab cd ab cd ........

Data: 000000000b153063abcdabcdabcdabcdabcdabcdabcdabcdabcd...
[Length: 72]

Frame 2: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0

Switch# show monitor capture mycap buffer dump
Starting the packet display ......... Press Ctrl + Shift + 6 to exit

0000 00 e1 6d 31 f1 c6 00 e1 6d f3 63 46 08 00 45 00 ..m1....m.cF..E.
0010 00 64 ab de 00 00 fe 01 e8 a3 0a 0a 0a 02 0a 0a .d..............
0020 0a 01 08 00 a6 1d 00 38 9e 7a 00 00 00 0b 15 .......8.y......
0030 30 63 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd 0c................
0040 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd .................
0050 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd .................
0060 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd .................
0070 ab cd

0000 00 e1 6d 31 f1 c6 00 e1 6d f3 63 46 08 00 45 00 ..m1....m.cF..E.
0010 00 64 ab de 00 00 fe 01 e8 a3 0a 0a 0a 02 0a 0a .d..............
0020 0a 01 08 00 a6 1d 00 38 9e 7a 00 00 00 0b 15 .......8.y......
0030 30 65 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd 0e................
0040 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd .................
0050 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd .................
0060 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd .................
0070 ab cd

Step 9: Clear the buffer by entering:

Switch# monitor capture mycap clear

---

**Note**

NOTE - Clearing the buffer deletes the buffer along with the contents.

---

**Note**

If you require the buffer contents to be displayed, run the clear commands after show commands.

---

**Step 10:** Restart the traffic, wait for 10 seconds, then display the buffer contents by entering:
We cannot run show from buffer during an active capture. Capture should be stopped before running show from buffer. We can however run a show on a pcap file during an active capture in both file and buffer mode. In file mode, we can display the packets in the current capture session's pcap file as well when the capture is active.

```
Switch# monitor capture mycap start
Switch# show monitor capture mycap
```

Status Information for Capture mycap
Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Active
Filter Details:
   IPv4
   Source IP: any
   Destination IP: any
   Protocol: any
Buffer Details:
   Buffer Type: CIRCULAR
   Buffer Size (in MB): 1
File Details:
   File not associated
Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)

**Step 11:** Stop the packet capture and display the buffer contents by entering:

```
Switch# monitor capture mycap stop
Capture statistics collected at software (Buffer):
    Capture duration - 111 seconds
    Packets received - 5000
    Packets dropped - 0
    Packets oversized - 0
```

**Step 12:** Determine whether the capture is active by entering:

```
Switch# show monitor capture mycap
```

Status Information for Capture mycap
Target Type:
   Interface: GigabitEthernet1/0/3, Direction: in
   Status : Inactive
Filter Details:
   IPv4
   Source IP: any
   Destination IP: any
   Protocol: any
Buffer Details:
   Buffer Type: CIRCULAR
   Buffer Size (in MB): 1
File Details:
   File not associated
Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
Maximum number of packets to capture per second: 1000  
Packet sampling rate: 0 (no sampling)

**Step 13:** Display the packets in the buffer by entering:

```
Switch# show monitor capture mycap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
```

```
1 0.000000000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=0/0, ttl=254
2 0.000003000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=1/256, ttl=254
3 0.0000051000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=2/512, ttl=254
4 0.0000072000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=3/768, ttl=254
5 0.0000093000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=4/1024, ttl=254
6 0.000030000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=5/1280, ttl=254
7 0.000003000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=6/1536, ttl=254
8 0.000003000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=7/1792, ttl=254
9 0.000003000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=8/2048, ttl=254
10 0.000003000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=9/2304, ttl=254
11 0.000003000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=10/2560, ttl=254
12 0.000003000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=11/2816, ttl=254
--More
```

**Step 14:** Store the buffer contents to the mycap.pcap file in the internal flash: storage device by entering:

```
Switch# monitor capture mycap export flash:mycap.pcap
Exported Successfully
```

**Note**

The current implementation of export is such that when the command is run, export is "started" but not complete when it returns the prompt to the user. So we have to wait for a message display on the console from Wireshark before it can run a display of packets in the file.

**Step 15:** Display capture packets from the file by entering:

```
Switch# show monitor capture file flash:mycap.pcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
```

```
1 0.000000000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=0/0, ttl=254
2 0.000003000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=1/256, ttl=254
3 0.000003000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=2/512, ttl=254
4 0.000003000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=3/768, ttl=254
5 0.000003000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=4/1024, ttl=254
```
6 0.000114000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=5/1280, ttl=254
7 0.000136000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=6/1536, ttl=254
8 0.000157000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=7/1792, ttl=254
9 0.000178000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=8/2048, ttl=254
10 0.000200000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=9/2304, ttl=254
11 0.000220000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=10/2560, ttl=254
12 0.000240000 10.10.10.2 -> 10.10.10.1 ICMP 114 Echo (ping) request id=0x0039,
seq=11/2816, ttl=254

Step 16: Delete the capture point by entering:

Switch# no monitor capture mycap

Related Topics

- Defining a Capture Point, on page 553
- Adding or Modifying Capture Point Parameters, on page 558
- Deleting Capture Point Parameters, on page 560
- Deleting a Capture Point, on page 562
- Activating and Deactivating a Capture Point, on page 563
- Clearing the Capture Point Buffer, on page 566
- How to Configure Wireshark, on page 566
- Capture Points, on page 543
- Attachment Points, on page 544

Example: Capture Sessions

Switch# monitor capture mycap start display display-filter "stp"
0.000000 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
Cost = 0 Port = 0x8136
2.000000 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
Cost = 0 Port = 0x8136
4.000000 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
Cost = 0 Port = 0x8136
6.000000 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
Cost = 0 Port = 0x8136
7.998001 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
Cost = 0 Port = 0x8136
8.998001 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
Cost = 0 Port = 0x8136

Capture test is not active Failed to Initiate Wireshark

Switch# show monitor capture mycap parameter
- monitor capture mycap control-plane both
- monitor capture mycap match any
- monitor capture mycap file location flash:mycap1.1 buffer-size 90
- monitor capture mycap limit duration 10

Switch# no monitor capture mycap file
Switch# monitor capture mycap start display display-filter "udp.port == 20002" dump
Example: Capture and Store in Lock-step Mode

This example captures live traffic and stores the packets in lock-step mode.

The capture rate might be slow for the first 15 seconds. If possible and necessary, start the traffic 15 seconds after the capture session starts.

**Step 1**: Define a capture point to match on the relevant traffic and associate it to a file by entering:

```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap limit duration 60 packets 100
Switch# monitor capture mycap file location flash:mycap.pcap buffer-size 64
```

**Step 2**: Confirm that the capture point has been correctly defined by entering:

```
Switch# show monitor capture mycap parameter
    monitor capture mycap file location flash:mycap.pcap buffer-size 64
    monitor capture mycap limit packets 100 duration 60
```

```
Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: GigabitEthernet1/0/1, Direction: in
  Status : Inactive
  Filter Details:
    Filter not attached
  Buffer Details:
    Buffer Type: LINEAR (default)
  File Details:
    Associated file name: flash:mycap.pcap
```
Example: Simple Capture and Store of Packets in Egress Direction

This example shows how to capture packets to a filter:

**Step 1**: Define a capture point to match on the relevant traffic and associate it to a file by entering:

```
Switch# monitor capture mycap interface Gigabit 1/0/1 out match ipv4 any any
Switch# monitor capture mycap limit duration 60 packets 100
Switch# monitor capture mycap file location flash:mycap.pcap buffer-size 90
```
Step 2: Confirm that the capture point has been correctly defined by entering:

Switch# show monitor capture mycap parameter
    monitor capture mycap interface GigabitEthernet1/0/1 out
    monitor capture mycap match ipv4 any any
    monitor capture mycap file location flash:mycap.pcap buffer-size 90
    monitor capture mycap limit packets 100 duration 60

Switch# show monitor capture mycap

Status Information for Capture mycap
Target Type:
    Interface: GigabitEthernet1/0/1, Direction: out
    Status : Inactive
Filter Details:
    IPv4
    Source IP: any
    Destination IP: any
    Protocol: any
Buffer Details:
    Buffer Type: LINEAR (default)
File Details:
    Associated file name: flash:mycap.pcap
    Size of buffer(in MB): 90
Limit Details:
    Number of Packets to capture: 100
    Packet Capture duration: 60
    Packet Size to capture: 0 (no limit)
    Packets per second: 0 (no limit)
    Packet sampling rate: 0 (no sampling)

Step 3: Launch packet capture by entering:

Switch# monitor capture mycap start
A file by the same capture file name already exists, overwrite?[confirm]
Turning on lock-step mode

Switch# *
*Oct 14 09:35:32.661: %BUFCAP-6-ENABLE: Capture Point mycap enabled.

Note
Allow the capture operation stop automatically after the time has elapsed or the packet count has been met. When you see the following message in the output, will know that the capture operation has stopped:

*Oct 14 09:36:34.632: %BUFCAP-6-DISABLE_ASYNC: Capture Point mycap disabled. Reason : Wireshark Session Ended

The mycap.pcap file now contains the captured packets.

Step 4: Display the packets by entering:

Switch# show monitor capture file flash:mycap.pcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

0.000000 10.1.1.30 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
1.000000 10.1.1.31 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
2.000000 10.1.1.32 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
3.000000 10.1.1.33 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
4.000000 10.1.1.34 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
5.000000 10.1.1.35 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
6.000000 10.1.1.36 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
7.000000 10.1.1.37 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
8.000000 10.1.1.38 → 20.1.1.2  UDP Source port: 20001  Destination port: 20002
9.000000 10.1.1.39 → 20.1.1.2  UDP Source port: 20001  Destination port: 20002

**Step 5:** Delete the capture point by entering:

```
Switch# no monitor capture mycap
```

**Related Topics**
- Defining a Capture Point, on page 553
- Adding or Modifying Capture Point Parameters, on page 558
- Deleting Capture Point Parameters, on page 560
- Deleting a Capture Point, on page 562
- Activating and Deactivating a Capture Point, on page 563
- Clearing the Capture Point Buffer, on page 566
- How to Configure Wireshark, on page 553
- Capture Points, on page 543
- Attachment Points, on page 544

## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Packet Filtering</td>
<td>For general packet filtering, refer to: Display Filter Reference</td>
</tr>
</tbody>
</table>

### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>-</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

Filters, on page 545

Feature History and Information for WireShark

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
PART IX

QoS

• Configuring QoS, on page 589
Configuring QoS

- Finding Feature Information, on page 589
- Prerequisites for Quality of Service, on page 589
- QoS Components, on page 590
- QoS Terminology, on page 590
- Information About QoS, on page 591
- Guidelines for QoS Policies, on page 629
- Restrictions for QoS on Wired Targets, on page 629
- Restrictions for QoS on Wireless Targets, on page 632
- How to Configure QoS, on page 635
- Monitoring QoS, on page 689
- Configuration Examples for QoS, on page 692
- Additional References for QoS, on page 707
- Feature History and Information for QoS, on page 709

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Quality of Service

Before configuring standard QoS, you must have a thorough understanding of these items:

- Standard QoS concepts.
- Wireless concepts and network topologies.
- Classic Cisco IOS QoS.
• Modular QoS CLI (MQC).
• Understanding of QoS implementation.
• The types of applications used and the traffic patterns on your network.
• Traffic characteristics and needs of your network. For example, is the traffic on your network bursty? Do you need to reserve bandwidth for voice and video streams?
• Bandwidth requirements and speed of the network.
• Location of congestion points in the network.

Related Topics
Restrictions for QoS on Wired Targets, on page 629
Restrictions for QoS on Wireless Targets, on page 632

QoS Components

Quality of service (QoS) consists of the following key components:

• Classification—Classification is the process of distinguishing one type of traffic from another based upon access control lists (ACLs), Differentiated Services Code Point (DSCP), Class of Service (CoS), and other factors.

• Marking and mutation—Marking is used on traffic to convey specific information to a downstream device in the network, or to carry information from one interface in a switch to another. When traffic is marked, QoS operations on that traffic can be applied. This can be accomplished directly using the `set` command or through a table map, which takes input values and translates them directly to values on output.

• Shaping and policing—Shaping is the process of imposing a maximum rate of traffic, while regulating the traffic rate in such a way that downstream devices are not subjected to congestion. Shaping in the most common form is used to limit the traffic sent from a physical or logical interface. Policing is used to impose a maximum rate on a traffic class. If the rate is exceeded, then a specific action is taken as soon as the event occurs.

• Queuing—Queueing is used to prevent traffic congestion. Traffic is sent to specific queues for servicing and scheduling based upon bandwidth allocation. Traffic is then scheduled or sent out through the port.

• Bandwidth—Bandwidth allocation determines the available capacity for traffic that is subject to QoS policies.

• Trust—Trust enables traffic to pass through the switch, and the Differentiated Services Code Point (DSCP), precedence, or CoS values coming in from the end points are retained in the absence of any explicit policy configuration.

QoS Terminology

The following terms are used interchangeably in this QoS configuration guide:

• Upstream (direction towards the switch) is the same as ingress.
• Downstream (direction from the switch) is the same as egress.

Note
Upstream is wireless to wired. Downstream is wired to wireless. Wireless to wireless has no specific term.

Information About QoS

QoS Overview
By configuring the quality of service (QoS), you can provide preferential treatment to specific types of traffic at the expense of other traffic types. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size. The switch sends the packets without any assurance of reliability, delay bounds, or throughput.

The following are specific features provided by QoS:
• Low latency
• Bandwidth guarantee
• Buffering capabilities and dropping disciplines
• Traffic policing
• Enables the changing of the attribute of the frame or packet header
• Relative services

Related Topics
Restrictions for QoS on Wired Targets, on page 629
Restrictions for QoS on Wireless Targets, on page 632

Modular QoS Command-Line Interface
With the switch, QoS features are enabled through the Modular QoS command-line interface (MQC). The MQC is a command-line interface (CLI) structure that allows you to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to classify traffic, while the QoS features in the traffic policy determine how to treat the classified traffic. One of the main goals of MQC is to provide a platform-independent interface for configuring QoS across Cisco platforms.

Wireless QoS Overview
Wireless QoS can be configured on the following wireless targets:
• Wireless ports, including all physical ports to which an access point can be associated.
• Radio
• SSID (applicable on a per-radio, per-AP, and per-SSID)
• Client

From Cisco IOS XE Release 3E, marking and policing actions for ingress SSID and client policies are applied at the access point. The SSID and client ingress policies that you configure in the switch are moved to the access point. The access point performs policing and marking actions for each packet. However, the switch selects the QoS policies. Marking and policing of egress SSID and client policies are applied at the switch.

The following table displays how policies are supported for the wireless targets.

<table>
<thead>
<tr>
<th>Wireless Target</th>
<th>Policies on Wireless Targets Supported</th>
<th>Policies Supported Egress Direction</th>
<th>Policies Supported Ingress Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless port</td>
<td>Yes</td>
<td>Yes - user configurable</td>
<td>No</td>
</tr>
<tr>
<td>Radio</td>
<td>Yes</td>
<td>Yes - but not configurable by user</td>
<td>No</td>
</tr>
<tr>
<td>SSID</td>
<td>Yes</td>
<td>Yes - user configurable</td>
<td>Yes - user configurable</td>
</tr>
<tr>
<td>Client</td>
<td>Yes</td>
<td>Yes - user configurable</td>
<td>Yes - user configurable</td>
</tr>
</tbody>
</table>

**Note**

Additional polices that are user configured include multidestination policers and VLANs.

Wireless QoS supports the following features:

- Queuing in the egress direction.
- Policing of wireless traffic
- Marking of wireless traffic.
- Shaping of wireless traffic in the egress direction.
- Approximate Fair Drop (AFD) in the egress direction.
- Mobility support for QoS.
- Compatibility with precious metal QoS policies available on Cisco Unified Wireless Controllers.
- Combination of CLI/Traffic Class (TCLAS) and CLI/snooping.
- Application control (can drop or mark the data traffic) by configuring an AVC QoS client policy.
- Drop action for ingress policies.
- QoS statistics for client and SSID targets in the ingress direction.
- QoS attribute for local profiling policy.
- Hierarchical policies.

**QoS and IPv6 for Wireless**

The switch supports QoS for both IPv4 and IPv6 traffic, and client policies can now have IPv4 and IPv6 filters.
## Wired and Wireless Access Supported Features

The following table describes the supported features for both wired and wireless access.

*Table 35: Supported QoS Features for Wired and Wireless Access*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Wired</th>
<th>Wireless</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targets</td>
<td>• Gigabit Ethernet</td>
<td>• Wireless port (CAPWAP tunnel)</td>
</tr>
<tr>
<td></td>
<td>• 10 Gigabit Ethernet</td>
<td>• SSID</td>
</tr>
<tr>
<td></td>
<td>• VLAN</td>
<td>• Client</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Radio</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CAPWAP multicast tunnel</td>
</tr>
</tbody>
</table>

### Configuration Sequence

QoS policy installed using the `service-policy` command.

- When an access point joins the switch, the switch installs a policy on the port. The port policy has a child policy called `port_child_policy`.
- A policy is installed on the radio which has a shaper configured to the radio rate. The default radio policy (which cannot be modified) is attached to the radio.
- The default client policies take effect when a WMM client associates, and if admission control is enabled on the radio.
- User can modify the `port_child_policy` to add more classes.
- User can attach a user-defined policy at the SSID level.
- User can attach a user-defined policy at the client level.
- User can configure a port policy.
- User can configure an SSID policy.
- These policies can then be modified.
- The default radio policy (which cannot be modified) is attached to the radio.
- Optionally, the user can attach a client policy as required.
- The default client policies take effect when a WMM client associates, and if admission control is enabled on the radio.
**Supported QoS Features on Wireless Targets**

This table describes the various features available on wireless targets.

<table>
<thead>
<tr>
<th>Target</th>
<th>Features</th>
<th>Traffic</th>
<th>Direction Where Policies Are Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>• Port shaper</td>
<td>Non-Real Time (NRT), Real Time (RT)</td>
<td>Egress</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Priority queuing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Multicast policing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radio</td>
<td>• Shaping</td>
<td>Non-Real Time</td>
<td>Egress</td>
<td>Radio policies are not user configurable.</td>
</tr>
</tbody>
</table>
### Supported QoS Features on Wireless Targets

<table>
<thead>
<tr>
<th>Target</th>
<th>Features</th>
<th>Traffic</th>
<th>Direction Where Policies Are Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>• Police</td>
<td>Non-Real Time, Real Time</td>
<td>Ingress and egress</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table map</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shaping</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BRR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set actions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table map</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• set dscp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• set cos</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set actions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table map</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• set dscp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• set wlan user-priority</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Drop</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• set dscp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• set cos</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• set wlan user-priority</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client</td>
<td>Police</td>
<td>Non-Real Time, Real Time</td>
<td>Ingress and egress</td>
<td>For client policies, the following filters are supported:</td>
</tr>
<tr>
<td></td>
<td>Drop</td>
<td></td>
<td>Ingress</td>
<td>• ACL</td>
</tr>
<tr>
<td></td>
<td>Set actions</td>
<td></td>
<td>Ingress</td>
<td>• DSCP</td>
</tr>
<tr>
<td></td>
<td>• set dscp</td>
<td></td>
<td></td>
<td>• CoS (only for egress)</td>
</tr>
<tr>
<td></td>
<td>• set cos</td>
<td></td>
<td></td>
<td>• WLAN UP</td>
</tr>
<tr>
<td></td>
<td>Set actions</td>
<td></td>
<td>Egress</td>
<td>• protocol</td>
</tr>
<tr>
<td></td>
<td>• set dscp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• set wlan user-priority</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring Port Policies (GUI), on page 686
- Applying or Changing Port Policies (GUI), on page 687
- Applying a QoS Policy on a WLAN (GUI), on page 687
- Port Policies, on page 596
- Port Policy Format, on page 596
- Radio Policies, on page 598
- Applying an SSID or Client Policy on a WLAN (CLI), on page 654
- Configuring SSID Policies (GUI), on page 652
- SSID Policies, on page 598
- Configuring Client Policies (CLI)
- Configuring Client Policies (GUI), on page 642
**Port Policies**

**Note**

Port child policies only apply to wireless ports and not to wired ports on the switch. A wireless port is defined as a port to which APs join. A default port child policy is applied on the switch to the wireless ports at start up. The port shaper rate is limited to 1G.

Port shaper specifies the traffic policy applicable between the device and the AP. This is the sum of the radio rates supported on the access point.

The child policy determines the mapping between packets and queues defined by the port-child policy. The child policy can be configured to include voice, video, class-default, and non-client-nrt classes where voice and video are based on DSCP value (which is the outer CAPWAP header DSCP value). The definition of class-default is known to the system as any value other than voice and video DSCP.

The DSCP value is assigned when the packet reaches the port. Before the packet arrives at the port, the SSID policies are applied on the packet. Port child policy also includes multicast percentage for a given port traffic. By default, the port child policy allocates up to 10 percent of the available rate.

**Related Topics**

- Configuring Port Policies (GUI), on page 686
- Applying or Changing Port Policies (GUI), on page 687
- Applying a QoS Policy on a WLAN (GUI), on page 687
- Restrictions for QoS on Wireless Targets, on page 632
- Supported QoS Features on Wireless Targets, on page 594
- Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696

**Port Policy Format**

This section describes the behavior of the port policies on a switch. The ports on the switch do not distinguish between wired or wireless physical ports. Depending on the kind of device associated to the switch, the policies are applied. For example, when an access point is connected to a switch port, the switch detects it as a wireless device and applies the default hierarchical policy which is in the format of a parent-child policy. This policy is an hierarchical policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration. The switch is pre configured with a default class map and a policy map.

Default class map:

```plaintext
Class Map match-any non-client-nrt-class
    Match non-client-nrt
```

The above port policy processes all network traffic to the Q3 queue. You can view the class map by executing the `show class-map` command.

Default policy map:

```plaintext
Policy Map port_child_policy
    Class non-client-nrt-class
        bandwidth remaining ratio 10
```
The class map and policy map listed are system-defined policies and cannot be changed.

The following is the system-defined policy map available on the ports on which wireless devices are associated. The format consists of a parent policy and a service child policy (port_child_policy). To customize the policies to suite your network needs, you must configure the port child policy.

```plaintext
Policy-map policy_map_name
  Class class-default
    Shape average average_rate
    Service-policy port_child_policy
```

The parent policy is system generated and cannot be changed. You must configure the port_child_policy policy to suit the QoS requirements on your network.

Depending on the type of traffic in your network, you can configure the port child policy. For example, in a typical wireless network deployment, you can assign specific priorities to voice and video traffic. Here is an example:

```plaintext
Policy-map port_child_policy
  Class voice-policy-name (match dscp ef)
    Priority level 1
      Police (multicast-policer-name-voice) Multicast Policer
  Class video-policy-name (match dscp af41)
    Priority level 2
      Police (multicast-policer-name-video) Multicast Policer
  Class non-client-nrt-class traffic(match non-client-nrt)
    Bandwidth remaining ratio (brr-value-nrt-q2)
  Class class-default (NRT Data)
    Bandwidth remaining ratio (brr-value-q3)
```

In the above port child policy:

- **voice-policy-name** — Refers to the name of the class that specifies rules for the traffic for voice packets. Here the DSCP value is mapped to a value of 46 (represented by the keyword **ef**). The voice traffic is assigned the highest priority of 1.

- **video-policy-name** — Refers to the name of the class that specifies rules for the traffic for video packets. The DSCP value is mapped to a value of 34 (represented by the keyword **af41**).

- **multicast-policer-name-voice** — If you need to configure multicast voice traffic, you can configure policing for the voice class map.

- **multicast-policer-name-video** — If you need to configure multicast video traffic, you can configure policing for the video class map.

In the above sample configuration, all voice and video traffic is directed to the Q0 and Q1 queues, respectively. These queues maintain a strict priority. The packets in Q0 and Q1 are processed in that order. The bandwidth remaining ratios `brr-value-nrt-q2` and `brr-value-q3` are directed to the Q2 and Q3 respectively specified by the class maps and `class-default` and `non-client-nrt`. The processing of packets on Q2 and Q3 are based on a weighted round-robin approach. For example, if the `brr-value-nrtq2` has a value of 90 and `brr-value-nrtq3` is 10, the packets in queue 2 and queue 3 are processed in the ratio of 9:1.
The Cisco 5700 Series Wireless Controller does not contain a default port policy. Physical port policies must be configured for voice and video to function. Because a Cisco 5700 Series Wireless Controller contains six 10-gigabit ports, the policy map must be configured on all ports.

**Note**

The policy must be configured on all of the six physical ports on the controller even if LAG (Link Aggregation/Etherchannel) is configured.

The following basic port policy must be configured on the physical ports. You can add further classification if required:

```
Policy-map <port-policy-name>
  Class voice
      Priority level 1
  class video
      Priority level 2
```

**Related Topics**

- Configuring Port Policies (GUI), on page 686
- Applying or Changing Port Policies (GUI), on page 687
- Applying a QoS Policy on a WLAN (GUI), on page 687
- Restrictions for QoS on Wireless Targets, on page 632
- Supported QoS Features on Wireless Targets, on page 594
- Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696
- Wired and Wireless Access Supported Features, on page 593
- Policy Maps, on page 608

**Radio Policies**

The radio policies are system defined and are not user configurable. Radio wireless targets are only applicable in the egress direction.

Radio policies are applicable on a per-radio, per-access point basis. The rate limit on the radios is the practical limit of the AP radio rate. This value is equivalent to the sum of the radios supported by the access point.

The following radios are supported:

- 802.11 a/n
- 802.11 b/n
- 802.11 ac

**Related Topics**

- Restrictions for QoS on Wireless Targets, on page 632
- Supported QoS Features on Wireless Targets, on page 594

**SSID Policies**

You can create QoS policies on SSID BSSID (Basic Service Set Identification) in both the ingress and egress directions. By default, there is no SSID policy. All traffic is transmitted as best effort because the wireless traffic in untrusted. You can configure an SSID policy based on the SSID name. The policy is applicable on a per BSSID.
The types of policies you can create on SSID include marking by using table maps (table-maps), shape rate, and RT1 (Real Time 1) and RT2 (Real Time 2) policies. If traffic is ingress, you usually configure a marking and policing policy on the SSID. If traffic is downstream, you can configure marking and queuing.

There should be a one-to-one mapping between the policies configured on a port and an SSID. For example, if you configure class voice and class video on the port, you can have a similar policy on the SSID.

The policy on the port is mandatory if you want to preserve the voice and video behavior priority at the port level. Queuing policy is applicable in a downstream direction. When packets arrive from the AP, you can only configure policing and rate limiting.

SSID priorities can be specified by configuring bandwidth remaining ratio. Queuing SSID policies are applied in the egress direction.

**Related Topics**
- Applying an SSID or Client Policy on a WLAN (CLI), on page 654
- Configuring SSID Policies (GUI), on page 652
- Applying a QoS Policy on a WLAN (GUI), on page 687
- Supported QoS Features on Wireless Targets, on page 594
- Examples: SSID Policy
- Examples: Configuring Downstream SSID Policy, on page 697

**Client Policies**

Client policies are applicable in the ingress and egress direction. The wireless control module of the switch applies the default client policies when admission control is enabled for WMM clients. When admission control is disabled, there is no default client policy. You can configure policing and marking policies on clients.

---

**Note**

A client policy can have both IPv4 and IPv6 filters.

You can configure client policies in the following ways:

- Using AAA
- Using the Cisco IOS MQC CLI
  - You can use `service policy client` command in the WLAN configuration.
  - Using the default configuration
  - Using local policies (native profiling)

Use the `show wireless client mac address mac_address service-policy` command to display the source of the client policy (for example, local profiling policy, AAA, or CLI). The precedence order of client policies is AAA > local policy > WLAN service client policy CLI > default configuration.

---

**Note**

If you configured AAA by configuring the unified wireless controller procedure, and using the MQC QoS commands, the policy configuration performed through the MQC QoS commands takes precedence.
When applying client policies on a WLAN, you must disable the WLAN before modifying the client policy. SSID policies can be modified even if the WLAN is enabled.

The default client policy is enabled only on Wi-Fi Multimedia (WMM) clients that are admission control (ACM)-enabled.

**Policy Chaining**

Every packet has a maximum of two applicable policies, first at the client target and second at the SSID target. The client policing action is applied to the packet before the marking action that is specified in the client policy. After the client policing and marking actions are applied to the packet, the SSID policy action is applied to the updated packet. If no custom policies are specified, the system trust configuration is applied to the packet. Egress trust is based on DSCP, and ingress trust is based on WLAN user priority.

**Related Topics**

- Configuring Client Policies (CLI)
- Configuring Client Policies (GUI), on page 642
- Applying a QoS Policy on a WLAN (GUI), on page 687
- Supported QoS Features on Wireless Targets, on page 594
- Examples: Client Policies, on page 699

**Hierarchical QoS**

The switch supports hierarchical QoS (HQoS). HQoS allows you to perform:

- Hierarchical classification—Traffic classification is based upon other classes.
- Hierarchical policing—The process of having the policing configuration at multiple levels in a hierarchical policy.
- Hierarchical shaping—Shaping can also be configured at multiple levels in the hierarchy.

**Note**

Hierarchical shaping is only supported for the port shaper, where for the parent you only have a configuration for the class default, and the only action for the class default is shaping.

**Related Topics**

- Examples: Hierarchical Classification, on page 694
- Examples: Hierarchical Policy Configuration, on page 694

**Hierarchical Wireless QoS**

The switch supports hierarchical QoS for wireless targets. Hierarchical QoS policies are applicable on port, radio, SSID, and client. QoS policies configured on the device (including marking, shaping, policing) can be applied across the targets. If the network contains non-realtime traffic, the non-realtime traffic is subject to approximate fair drop. Hierarchy refers to the process of application of the various QoS policies on the packets arriving to the device. You can configure policing in both the parent and child policies.
For hierarchical client and SSID policies, you only configure marking either in the parent or child policy.

**Wireless Packet Format**

*Figure 38: Wireless Packet Path in the Egress Direction during First Pass*

This figure displays the wireless packet flow and encapsulation used in hierarchical wireless QoS. The incoming packet enters the switch. The switch encapsulates this incoming packet and adds the 802.11e and CAPWAP headers.

**Hierarchical AFD**

Approximate Fair Dropping (AFD) is a feature provided by the QoS infrastructure in Cisco IOS. For wireless targets, AFD can be configured on SSID (via shaping) and clients (via policing). AFD shaping rate is only applicable for downstream direction. Unicast real-time traffic is not subjected to AFD drops.
QoS Implementation

Typically, networks operate on a best-effort delivery basis, which means 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 the QoS feature, you can select 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 network makes network performance more predictable and bandwidth utilization more effective.

The QoS implementation is based on the Differentiated Services (Diff-Serv) architecture, a standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network.

The classification is carried in the IP packet header, using 6 bits from the deprecated IP type of service (ToS) field to carry the classification (class) information. Classification can also be carried in the Layer 2 frame.

Figure 39: QoS Classification Layers in Frames and Packets

The special bits in the Layer 2 frame or a Layer 3 packet are shown in the following figure:

Encapsulated Packet

<table>
<thead>
<tr>
<th>Layer 2 header</th>
<th>IP header</th>
<th>Data</th>
</tr>
</thead>
</table>

Layer 2 ISL Frame

<table>
<thead>
<tr>
<th>ISL header (26 bytes)</th>
<th>Encapsulated frame 1... (24.5 KB)</th>
<th>FCS (4 bytes)</th>
</tr>
</thead>
</table>

3 bits used for CoS

Layer 2 802.1Q and 802.1p Frame

<table>
<thead>
<tr>
<th>Preamble</th>
<th>Start frame delimiter</th>
<th>DA</th>
<th>SA</th>
<th>Tag</th>
<th>PT</th>
<th>Data</th>
<th>FCS</th>
</tr>
</thead>
</table>

3 bits used for CoS (user priority)

Layer 3 IPv4 Packet

<table>
<thead>
<tr>
<th>Version length</th>
<th>ToS (1 byte)</th>
<th>Len</th>
<th>ID</th>
<th>Offset</th>
<th>TTL</th>
<th>Proto</th>
<th>FCS</th>
<th>IP-SA</th>
<th>IP-DA</th>
<th>Data</th>
</tr>
</thead>
</table>

IP precedence or DSCP

Layer 3 IPv6 Packet

<table>
<thead>
<tr>
<th>Version</th>
<th>Traffic class (1 byte)</th>
<th>Flow label</th>
<th>Payload length</th>
<th>Next header</th>
<th>HOP limit</th>
<th>Source address</th>
<th>Dest. address</th>
</tr>
</thead>
</table>

IP precedence or DSCP

Related Topics

Restrictions for QoS on Wired Targets, on page 629
Restrictions for QoS on Wireless Targets, on page 632
Layer 2 Frame Prioritization Bits

Layer 2 Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries an IEEE 802.1p class of service (CoS) value in the three least-significant bits. On ports configured as Layer 2 ISL trunks, all traffic is in ISL frames.

Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most-significant bits, which are called the User Priority bits. On ports configured as Layer 2 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in the native VLAN.

Other frame types cannot carry Layer 2 CoS values.

Layer 2 CoS values range from 0 for low priority to 7 for high priority.

Layer 3 Packet Prioritization Bits

Layer 3 IP packets can carry either an IP precedence value or a Differentiated Services Code Point (DSCP) value. QoS supports the use of either value because DSCP values are backward-compatible with IP precedence values.

IP precedence values range from 0 to 7. DSCP values range from 0 to 63.

End-to-End QoS Solution Using Classification

All switches and routers that access the Internet rely on the class information to provide the same forwarding treatment to packets with the same class information and different treatment to packets with different class information. The class information in the packet can be assigned by end hosts or by switches or routers along the way, based on a configured policy, detailed examination of the packet, or both. Detailed examination of the packet is expected to occur closer to the edge of the network, so that the core switches and routers are not overloaded with this task.

Switches and routers along the path can use the class information to limit the amount of resources allocated per traffic class. The behavior of an individual device when handling traffic in the Diff-Serv architecture is called per-hop behavior. If all devices along a path provide a consistent per-hop behavior, you can construct an end-to-end QoS solution.

Implementing QoS in your network can be a simple task or complex task and depends on the QoS features offered by your internetworking devices, the traffic types and patterns in your network, and the granularity of control that you need over incoming and outgoing traffic.

Packet Classification

Packet classification is the process of identifying a packet as belonging to one of several classes in a defined policy, based on certain criteria. The Modular QoS CLI (MQC) is a policy-class based language. The policy class language is used to define the following:

- Class-map template with one or several match criteria
- Policy-map template with one or several classes associated to the policy map

The policy map template is then associated to one or several interfaces on the switch.

Packet classification is the process of identifying a packet as belonging to one of the classes defined in the policy map. The process of classification will exit when the packet being processed matches a specific filter in a class. This is referred to as first-match exit. If a packet matches multiple classes in a policy, irrespective
of the order of classes in the policy map, it would still exit the classification process after matching the first class.

If a packet does not match any of the classes in the policy, it would be classified into the default class in the policy. Every policy map has a default class, which is a system-defined class to match packets that do not match any of the user-defined classes.

Packet classification can be categorized into the following types:

• Classification based on information that is propagated with the packet
• Classification based on information that is switch specific
• Hierarchical classification

Classification Based on Information That is Propagated with the Packet

Classification that is based on information that is part of the packet and propagated either end-to-end or between hops, typically includes the following:

• Classification based on Layer 3 or 4 headers
• Classification based on Layer 2 information

Classification Based on Layer 3 or Layer 4 Header

This is the most common deployment scenario. Numerous fields in the Layer 3 and Layer 4 headers can be used for packet classification.

At the most granular level, this classification methodology can be used to match an entire flow. For this deployment type, an access control list (ACLs) can be used. ACLs can also be used to match based on various subsets of the flow (for example, source IP address only, or destination IP address only, or a combination of both).

Classification can also be done based on the precedence or DSCP values in the IP header. The IP precedence field is used to indicate the relative priority with which a particular packet needs to be handled. It is made up of three bits in the IP header's type of service (ToS) byte.

The following table shows the different IP precedence bit values and their names.

**Note** IP precedence is not supported for wireless QoS.

**Table 37: IP Precedence Values and Names**

<table>
<thead>
<tr>
<th>IP Precedence Value</th>
<th>IP Precedence Bits</th>
<th>IP Precedence Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>000</td>
<td>Routine</td>
</tr>
<tr>
<td>1</td>
<td>001</td>
<td>Priority</td>
</tr>
<tr>
<td>2</td>
<td>010</td>
<td>Immediate</td>
</tr>
<tr>
<td>3</td>
<td>011</td>
<td>Flash</td>
</tr>
<tr>
<td>4</td>
<td>100</td>
<td>Flash Override</td>
</tr>
<tr>
<td>5</td>
<td>101</td>
<td>Critical</td>
</tr>
</tbody>
</table>
### Classification Based on Layer 2 Header

A variety of methods can be used to perform classification based on the Layer 2 header information. The most common methods include the following:

- **MAC address-based classification (only for access groups)** — Classification is based upon the source MAC address (for policies in the input direction) and destination MAC address (for policies in the output direction).

- **Class-of-Service** — Classification is based on the 3 bits in the Layer 2 header based on the IEEE 802.1p standard. This usually maps to the ToS byte in the IP header.

- **VLAN ID** — Classification is based on the VLAN ID of the packet.

**Note** Some of these fields in the Layer 2 header can also be set using a policy.

### Classification Based on Information that is Device Specific (QoS Groups)

The switch also provides classification mechanisms that are available where classification is not based on information in the packet header or payload.

At times you might be required to aggregate traffic coming from multiple input interfaces into a specific class in the output interface. For example, multiple customer edge routers might be going into the same access switch on different interfaces. The service provider might want to police all the aggregate voice traffic going into the core to a specific rate. However, the voice traffic coming in from the different customers could have a different ToS settings. QoS group-based classification is a feature that is useful in these scenarios.

Policies configured on the input interfaces set the QoS group to a specific value, which can then be used to classify packets in the policy enabled on output interface.

---

<table>
<thead>
<tr>
<th>IP Precedence Value</th>
<th>IP Precedence Bits</th>
<th>IP Precedence Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>110</td>
<td>Internetwork control</td>
</tr>
<tr>
<td>7</td>
<td>111</td>
<td>Network control</td>
</tr>
</tbody>
</table>

---

Note

All routing control traffic in the network uses IP precedence value 6 by default. IP precedence value 7 also is reserved for network control traffic. Therefore, the use of IP precedence values 6 and 7 is not recommended for user traffic.

The DSCP field is made up of 6 bits in the IP header and is being standardized by the Internet Engineering Task Force (IETF) Differentiated Services Working Group. The original ToS byte contained the DSCP bits has been renamed the DSCP byte. The DSCP field is part of the IP header, similar to IP precedence. The DSCP field is a super set of the IP precedence field. Therefore, the DSCP field is used and is set in ways similar to what was described with respect to IP precedence.

**Note**

The DSCP field definition is backward-compatible with the IP precedence values.
The QoS group is a field in the packet data structure internal to the switch. It is important to note that a QoS group is an internal label to the switch and is not part of the packet header.

Hierarchical Classification

The switch permits you to perform a classification based on other classes. Typically, this action may be required when there is a need to combine the classification mechanisms (that is, filters) from two or more classes into a single class map.

QoS Wired Model

To implement QoS, the switch must perform the following tasks:

- Traffic classification—Distinguishes packets or flows from one another.
- Traffic marking and policing—Assigns a label to indicate the given quality of service as the packets move through the switch, and then make the packets comply with the configured resource usage limits.
- Queuing and scheduling—Provides different treatment in all situations where resource contention exists.
- Shaping—Ensures that traffic sent from the switch meets a specific traffic profile.

Ingress Port Activity

The following activities occur at the ingress port of the switch:

- Classification—Classifying a distinct path for a packet by associating it with a QoS label. For example, the switch maps the CoS or DSCP in the packet to a QoS label to distinguish one type of traffic from another. The QoS label that is generated identifies all future QoS actions to be performed on this packet.
- Policing—Policing determines whether a packet is in or out of profile by comparing the rate of the incoming traffic to the configured policer. The policer limits the bandwidth consumed by a flow of traffic. The result is passed to the marker.
- Marking—Marking evaluates the policer and configuration information for the action to be taken when a packet is out of profile and determines what to do with the packet (pass through a packet without modification, mark down the QoS label in the packet, or drop the packet).

Note

Applying polices on the wireless ingress port is not supported on the switch.

Egress Port Activity

The following activities occur at the egress port of the switch:

- Policing—Policing determines whether a packet is in or out of profile by comparing the rate of the incoming traffic to the configured policer. The policer limits the bandwidth consumed by a flow of traffic. The result is passed to the marker.
- Marking—Marking evaluates the policer and configuration information for the action to be taken when a packet is out of profile and determines what to do with the packet (pass through a packet without modification, mark down the QoS label in the packet, or drop the packet).
• Queueing—Queueing evaluates the QoS packet label and the corresponding DSCP or CoS value before selecting which of the egress queues to use. Because congestion can occur when multiple ingress ports simultaneously send data to an egress port, Weighted Tail Drop (WTD) differentiates traffic classes and subjects the packets to different thresholds based on the QoS label. If the threshold is exceeded, the packet is dropped.

Classification

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet. Classification is enabled only if QoS is enabled on the switch. By default, QoS is enabled on the switch.

During classification, the switch performs a lookup and assigns a QoS label to the packet. The QoS label identifies all QoS actions to be performed on the packet and from which queue the packet is sent.

Access Control Lists

You can use IP standard, IP extended, or Layer 2 MAC ACLs to define a group of packets with the same characteristics (class). You can also classify IP traffic based on IPv6 ACLs.

In the QoS context, the permit and deny actions in the access control entries (ACEs) have different meanings from security ACLs:

• If a match with a permit action is encountered (first-match principle), the specified QoS-related action is taken.

• If a match with a deny action is encountered, the ACL being processed is skipped, and the next ACL is processed.

Note

Deny action is supported in Cisco IOS Release 3.7.4E and later releases.

• If no match with a permit action is encountered and all the ACEs have been examined, no QoS processing occurs on the packet, and the switch offers best-effort service to the packet.

• If multiple ACLs are configured on a port, the lookup stops after the packet matches the first ACL with a permit action, and QoS processing begins.

Note

When creating an access list, note that by default the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.

After a traffic class has been defined with the ACL, you can attach a policy to it. A policy might contain multiple classes with actions specified for each one of them. A policy might include commands to classify the class as a particular aggregate (for example, assign a DSCP) or rate-limit the class. This policy is then attached to a particular port on which it becomes effective.

You implement IP ACLs to classify IP traffic by using the access-list global configuration command; you implement Layer 2 MAC ACLs to classify non-IP traffic by using the mac access-list extended global configuration command.
Class Maps

A class map is a mechanism that you use to name a specific traffic flow (or class) and isolate it from all other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it. The criteria can include matching the access group defined by the ACL or matching a specific list of DSCP or IP precedence values. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. After a packet is matched against the class-map criteria, you further classify it through the use of a policy map.

You create a class map by using the `class-map` global configuration command or the `class` policy-map configuration command. You should use the `class-map` command when the map is shared among many ports. When you enter the `class-map` command, the switch enters the class-map configuration mode. In this mode, you define the match criterion for the traffic by using the `match` class-map configuration command.

You can create a default class by using the `class class-default` policy-map configuration command. The default class is system-defined and cannot be configured. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as default traffic.

Related Topics

- Creating a Traffic Class (CLI), on page 635
- Examples: Classification by Access Control Lists, on page 692

Policy Maps

A policy map specifies which traffic class to act on. Actions can include the following:

- Setting a specific DSCP or IP precedence value in the traffic class
- Setting a CoS value in the traffic class
- Setting a QoS group
- Setting a wireless LAN (WLAN) value in the traffic class
- Specifying the traffic bandwidth limitations and the action to take when the traffic is out of profile

Before a policy map can be effective, you must attach it to a port.

You create and name a policy map using the `policy-map` global configuration command. When you enter this command, the switch enters the policy-map configuration mode. In this mode, you specify the actions to take on a specific traffic class by using the `class` or `set` policy-map configuration and policy-map class configuration commands.

The policy map can also be configured using the `police` and `bandwidth` policy-map class configuration commands, which define the policer, the bandwidth limitations of the traffic, and the action to take if the limits are exceeded. In addition, the policy-map can further be configured using the `priority` policy-map class configuration command, to schedule priority for the class or the queueing policy-map class configuration commands, `queue-buffers` and `queue-limit`.

To enable the policy map, you attach it to a port by using the `service-policy` interface configuration command.
You cannot configure both priority and set for a policy map. If both these commands are configured for a policy map, and when the policy map is applied to an interface, error messages are displayed. The following example shows this restriction:

```
Switch# configure terminal
Switch(config)# class-map cmap
Switch(config-cmap)# exit
Switch(config)# class-map classmap1
Switch(config-cmap)# exit
Switch(config)# policy-map pmap
Switch(config-pmap)# class cmap
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# class classmap1
Switch(config-pmap-c)# set
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# interface gigabitethernet 0/1/1
Switch(config-if)# service-policy output pmap
```

Non-queuing action only is unsupported in a queuing policy!!!
%QOS-6-POLICY_INST_FAILED:
Service policy installation failed

**Related Topics**
- Creating a Traffic Policy (CLI), on page 638
- Port Policy Format, on page 596

**Policy Map on Physical Port**

You can configure a nonhierarchical policy map on a physical port that specifies which traffic class to act on. Actions can include setting a specific DSCP or IP precedence value in the traffic class, specifying the traffic bandwidth limitations for each matched traffic class (policer), and taking action when the traffic is out of profile (marking).

A policy map also has these characteristics:

- A policy map can contain multiple class statements, each with different match criteria and policers.
- A policy map can contain a predefined default traffic class explicitly placed at the end of the map.

When you configure a default traffic class by using the class class-default policy-map configuration command, unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as the default traffic class (class-default).

- A separate policy-map class can exist for each type of traffic received through a port.

**Related Topics**
- Attaching a Traffic Policy to an Interface (CLI), on page 651

**Policy Map on VLANs**

The switch supports a VLAN QoS feature that allows the user to perform QoS treatment at the VLAN level (classification and QoS actions) using the incoming frame’s VLAN information. In VLAN-based QoS, a service policy is applied to an SVI interface. All physical interfaces belonging to a VLAN policy map then need to be programmed to refer to the VLAN-based policy maps instead of the port-based policy map.
Although the policy map is applied to the VLAN SVI, any policing (rate-limiting) action can only be performed on a per-port basis. You cannot configure the policer to take account of the sum of traffic from a number of physical ports. Each port needs to have a separate policer governing the traffic coming into that port.

**Related Topics**
- Classifying, Policing, and Marking Traffic on SVIs by Using Policy Maps (CLI), on page 658
- Examples: Policer VLAN Configuration, on page 704

### Wireless QoS Multicast

You can configure multicast policing rate at the port level.

There are two modes of a multicast configuration in the Cisco 5700 Series Wireless Controller:

- **multicast-unicast mode**—Multicast traffic is copied as unicast traffic to the APs. QoS on multicast traffic when multicast-unicast mode is not supported on the Cisco 5700 Series Wireless Controller.
- **multicast-multicast mode**—The controller sends the traffic to the multicast group. The APs in the multicast group then receive the multicast traffic.

**Related Topics**
- Configuring QoS Policies for Multicast Traffic (CLI), on page 685
- Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696

### Policing

After a packet is classified and has a DSCP-based, CoS-based, or QoS-group label assigned to it, the policing and marking process can begin.

Policing involves creating a policer that specifies the bandwidth limits for the traffic. Packets that exceed the limits are *out of profile* or *nonconforming*. Each policer decides on a packet-by-packet basis whether the packet is in or out of profile and specifies the actions on the packet. These actions, carried out by the marker, include passing through the packet without modification, dropping the packet, or modifying (marking down) the assigned DSCP or CoS value of the packet and allowing the packet to pass through.

To avoid out-of-order packets, both conform and nonconforming traffic typically exit the same queue.

**Note**

All traffic, regardless of whether it is bridged or routed, is subjected to a policer, if one is configured. As a result, bridged packets might be dropped or might have their DSCP or CoS fields modified when they are policed and marked.

You can only configure policing on a physical port.

After you configure the policy map and policing actions, attach the policy to an ingress port or SVI by using the `service-policy` interface configuration command.

**Related Topics**
- Configuring Police (CLI), on page 673
- Examples: Policing Action Configuration, on page 703
Token-Bucket Algorithm

Policing uses a token-bucket algorithm. As each frame is received by the switch, a token is added to the bucket. The bucket has a hole in it and leaks at a rate that you specify as the average traffic rate in bits per second. Each time a token is added to the bucket, the switch verifies that there is enough room in the bucket. If there is not enough room, the packet is marked as nonconforming, and the specified policer action is taken (dropped or marked down).

How quickly the bucket fills is a function of the bucket depth (burst-byte), the rate at which the tokens are removed (rate-bps), and the duration of the burst above the average rate. The size of the bucket imposes an upper limit on the burst length and limits the number of frames that can be transmitted back-to-back. If the burst is short, the bucket does not overflow, and no action is taken against the traffic flow. However, if a burst is long and at a higher rate, the bucket overflows, and the policing actions are taken against the frames in that burst.

You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the burst-byte option of the `police` policy-map class configuration command. You configure how fast (the average rate) that the tokens are removed from the bucket by using the rate option of the `police` policy-map class configuration command.

Related Topics
- Configuring Police (CLI), on page 673
- Examples: Policing Action Configuration, on page 703
- Examples: Policing Units, on page 704

Marking

Marking is used to convey specific information to a downstream device in the network, or to carry information from one interface in a switch to another.

Marking can be used to set certain field/bits in the packet headers, or marking can also be used to set certain fields in the packet structure that is internal to the switch. Additionally, the marking feature can be used to define mapping between fields. The following marking methods are available for QoS:

- Packet header
- Device (switch) specific information
- Table maps

Packet Header Marking

Marking on fields in the packet header can be classified into two general categories:

- IPv4/v6 header bit marking
- Layer 2 header bit marking

The marking feature at the IP level is used to set the precedence or the DSCP in the IP header to a specific value to get a specific per-hop behavior at the downstream device (switch or router), or it can also be used to aggregate traffic from different input interfaces into a single class in the output interface. The functionality is currently supported on both the IPv4 and IPv6 headers.
Marking in the Layer 2 headers is typically used to influence dropping behavior in the downstream devices (switch or router). It works in tandem with the match on the Layer 2 headers. The bits in the Layer 2 header that can be set using a policy map are class of service.

**Switch Specific Information Marking**

This form of marking includes marking of fields in the packet data structure that are not part of the packets header, so that the marking can be used later in the data path. This is not propagated between the switches. Marking of QoS-group falls into this category. This form of marking is only supported in policies that are enabled on the input interfaces. The corresponding matching mechanism can be enabled on the output interfaces on the same switch and an appropriate QoS action can be applied.

**Table Map Marking**

QoS marking is not supported on the 802.11ac Wave 2 APs. This is because table-maps used for QoS marking are not supported on the 802.11ac Wave 2 APs.

Table map marking enables the mapping and conversion from one field to another using a conversion table. This conversion table is called a table map.

Depending upon the table map attached to an interface, CoS, DSCP, and UP values (UP specific to wireless packets) of the packet are rewritten. The switch allows configuring both ingress table map policies and egress table map policies.

As an example, a table map can be used to map the Layer 2 CoS setting to a precedence value in Layer 3. This feature enables combining multiple set commands into a single table, which indicates the method to perform the mapping. This table can be referenced in multiple policies, or multiple times in the same policy.

The following table shows the currently supported forms of mapping:

<table>
<thead>
<tr>
<th>The To Packet-Marking Type</th>
<th>The From Packet-Marking Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precedence</td>
<td>CoS</td>
</tr>
<tr>
<td>Precedence</td>
<td>QoS Group</td>
</tr>
<tr>
<td>DSCP</td>
<td>CoS</td>
</tr>
<tr>
<td>DSCP</td>
<td>QoS Group</td>
</tr>
<tr>
<td>CoS</td>
<td>Precedence</td>
</tr>
<tr>
<td>CoS</td>
<td>DSCP</td>
</tr>
<tr>
<td>QoS Group</td>
<td>Precedence</td>
</tr>
<tr>
<td>QoS Group</td>
<td>DSCP</td>
</tr>
</tbody>
</table>

A table map-based policy supports the following capabilities:
• Mutation—You can have a table map that maps from one DSCP value set to another DSCP value set, and this can be attached to an egress port.

• Rewrite—Packets coming in are rewritten depending upon the configured table map.

• Mapping—Table map based policies can be used instead of set policies.

The following steps are required for table map marking:

1. Define the table map—Use the `table-map` global configuration command to map the values. The table does not know of the policies or classes within which it will be used. The default command in the table map is used to indicate the value to be copied into the `to` field when there is no matching from field.

2. Define the policy map—You must define the policy map where the table map will be used.

3. Associate the policy to an interface.

Note

A table map policy on an input port changes the trust setting of that port to the from type of qos-marking.

Related Topics

  Configuring Table Maps (CLI), on page 661
  Examples: Table Map Marking Configuration, on page 706

Traffic Conditioning

To support QoS in a network, traffic entering the service provider network needs to be policed on the network boundary routers to ensure that the traffic rate stays within the service limit. Even if a few routers at the network boundary start sending more traffic than what the network core is provisioned to handle, the increased traffic load leads to network congestion. The degraded performance in the network makes it difficult to deliver QoS for all the network traffic.

Traffic policing functions (using the police feature) and shaping functions (using the traffic shaping feature) manage the traffic rate, but differ in how they treat traffic when tokens are exhausted. The concept of tokens comes from the token bucket scheme, a traffic metering function.

Note

When running QoS tests on network traffic, you may see different results for the shaper and policing data. Network traffic data from shaping provides more accurate results.

This table compares the policing and shaping functions.

Table 39: Comparison Between Policing and Shaping Functions

<table>
<thead>
<tr>
<th>Policing Function</th>
<th>Shaping Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sends conforming traffic up to the line rate and allows bursts.</td>
<td>Smooths traffic and sends it out at a constant rate.</td>
</tr>
</tbody>
</table>
Policing Function | Shaping Function
---|---
When tokens are exhausted, action is taken immediately. | When tokens are exhausted, it buffers packets and sends them out later, when tokens are available. A class with shaping has a queue associated with it which will be used to buffer the packets.
Policing has multiple units of configuration – in bits per second, packets per second and cells per second. | Shaping has only one unit of configuration - in bits per second.
Policing has multiple possible actions associated with an event, marking and dropping being example of such actions. | Shaping does not have the provision to mark packets that do not meet the profile.
Works for both input and output traffic. | Implemented for output traffic only.
Transmission Control Protocol (TCP) detects the line at line speed but adapts to the configured rate when a packet drop occurs by lowering its window size. | TCP can detect that it has a lower speed line and adapt its retransmission timer accordingly. This results in less scope of retransmissions and is TCP-friendly.

Policing

The QoS policing feature is used to impose a maximum rate on a traffic class. The QoS policing feature can also be used with the priority feature to restrict priority traffic. If the rate is exceeded, then a specific action is taken as soon as the event occurs. The rate (committed information rate [CIR] and peak information rate [PIR] ) and the burst parameters (conformed burst size [BC] and extended burst size [BE] ) are all configured in bytes per second.

The following policing forms or policers are supported for QoS:

- Single-rate two-color policing
- Dual-rate three-color policing

**Note**

Single-rate three-color policing is not supported.

**Single-Rate Two-Color Policing**

Single-rate two-color policer is the mode in which you configure only a CIR and a BC.

The BC is an optional parameter, and if it is not specified it is computed by default. In this mode, when an incoming packet has enough tokens available, the packet is considered to be conforming. If at the time of packet arrival, enough tokens are not available within the bounds of BC, the packet is considered to have exceeded the configured rate.

**Note**

For information about the token-bucket algorithm, see [Token-Bucket Algorithm, on page 611](#).

**Related Topics**

[Configuring Police (CLI), on page 673](#)
Examples: Single-Rate Two-Color Policing Configuration, on page 705

Dual-Rate Three-Color Policing

With the dual rate policer, the switch supports only color-blind mode. In this mode, you configure a committed information rate (CIR) and a peak information rate (PIR). As the name suggests, there are two token buckets in this case, one for the peak rate, and one for the conformed rate.

\[ \text{Rate at which tokens are replenished} = \frac{(T2-T1) \times \text{CIR}}{8\text{ bytes}} \]

Related Topics

Configuring Police (CLI), on page 673
Examples: Dual-Rate Three-Color Policing Configuration, on page 705

Shaping

Shaping is the process of imposing a maximum rate of traffic, while regulating the traffic rate in such a way that the downstream switches and routers are not subjected to congestion. Shaping in the most common form is used to limit the traffic sent from a physical or logical interface.

Shaping has a buffer associated with it that ensures that packets which do not have enough tokens are buffered as opposed to being immediately dropped. The number of buffers available to the subset of traffic being shaped is limited and is computed based on a variety of factors. The number of buffers available can also be tuned using specific QoS commands. Packets are buffered as buffers are available, beyond which they are dropped.

Class-Based Traffic Shaping

The switch uses class-based traffic shaping. This shaping feature is enabled on a class in a policy that is associated to an interface. A class that has shaping configured is allocated a number of buffers to hold the packets that do not have tokens. The buffered packets are sent out from the class using FIFO. In the most common form of usage, class-based shaping is used to impose a maximum rate for an physical interface or logical interface as a whole. The following shaping forms are supported in a class:

- Average rate shaping
- Hierarchical shaping

Shaping is implemented using a token bucket. The values of CIR, \( B_c \) and \( B_e \) determine the rate at which the packets are sent out and the rate at which the tokens are replenished.

Note

For information about the token-bucket algorithm, see Token-Bucket Algorithm, on page 611.

In the color-blind mode, the incoming packet is first checked against the peak rate bucket. If there are not enough tokens available, the packet is said to violate the rate. If there are enough tokens available, then the tokens in the conformed rate buckets are checked to determine if there are enough tokens available. The tokens in the peak rate bucket are decremented by the size of the packet. If it does not have enough tokens available, the packet is said to have exceeded the configured rate. If there are enough tokens available, then the packet is said to conform, and the tokens in both the buckets are decremented by the size of the packet.

The rate at which tokens are replenished depends on the packet arrival. Assume that a packet comes in at time \( T_1 \) and the next one comes in at time \( T_2 \). The time interval between \( T_1 \) and \( T_2 \) determines the number of tokens that need to be added to the token bucket. This is calculated as:

\[ \text{Time interval between packets} = \frac{(T2-T1) \times \text{CIR}}{8\text{ bytes}} \]
Note

For information about the token-bucket algorithm, see Token-Bucket Algorithm, on page 611.

Average Rate Shaping

You use the shape average policy-map class command to configure average rate shaping.

This command configures a maximum bandwidth for a particular class. The queue bandwidth is restricted to this value even though the port has more bandwidth available. The switch supports configuring shape average by either a percentage or by a target bit rate value.

Related Topics

Configuring Shaping (CLI), on page 683
Examples: Average Rate Shaping Configuration, on page 701

Hierarchical Shaping

Shaping can also be configured at multiple levels in a hierarchy. This is accomplished by creating a parent policy with shaping configured, and then attaching child policies with additional shaping configurations to the parent policy.

There are two supported types of hierarchical shaping:

• Port shaper
• User-configured shaping

The port shaper uses the class default and the only action permitted in the parent is shaping. The queueing action is in the child with the port shaper. With the user configured shaping, you cannot have queueing action in the child.

Related Topics

Configuring Shaping (CLI), on page 683

Queueing and Scheduling

The switch uses both queueing and scheduling to help prevent traffic congestion. The switch supports the following queueing and scheduling features:

• Bandwidth
• Weighted Tail Drop
• Priority queues
• Queue buffers

When you define a queuing policy on a port, control packets are mapped to the best priority queue with the highest threshold. Control packets queue mapping works differently in the following scenarios:

• Without a quality of service (QoS) policy—If no QoS policy is configured, control packets with DSCP values 16, 24, 48, and 56 are mapped to queue 0 with the highest threshold of threshold2.
• With an user-defined policy—An user-defined queuing policy configured on egress ports can affect the default priority queue setting on control packets.
Control traffic is redirected to the best queue based on the following rules:

1. If defined in a user policy, the highest-level priority queue is always chosen as the best queue.

2. In the absence of a priority queue, Cisco IOS software selects queue 0 as the best queue. When the software selects queue 0 as the best queue, you must define the highest bandwidth to this queue to get the best QoS treatment to the control plane traffic.

3. If thresholds are not configured on the best queue, Cisco IOS software assigns control packets with Differentiated Services Code Point (DSCP) values 16, 24, 48, and 56 are mapped to threshold 2 and reassigns the rest of the control traffic in the best queue to threshold 1.

If a policy is not configured explicitly for control traffic, the Cisco IOS software maps all unmatched control traffic to the best queue with threshold 2, and the matched control traffic is mapped to the queue as configured in the policy.

---

**Note**

To provide proper QoS for Layer 3 packets, you must ensure that packets are explicitly classified into appropriate queues. When the software detects DSCP values in the default queue, then it automatically reassigns this queue as the best queue.

---

**Bandwidth**

The switch supports the following bandwidth configurations:

- Bandwidth percent
- Bandwidth remaining ratio

**Related Topics**

Configuring Bandwidth (CLI), on page 671

---

**Bandwidth Percent**

You can use the `bandwidth percent` policy-map class command to allocate a minimum bandwidth to a particular class. The total sum cannot exceed 100 percent and in case the total sum is less than 100 percent, then the rest of the bandwidth is divided equally among all bandwidth queues.

---

**Note**

A queue can oversubscribe bandwidth in case the other queues do not utilize the entire port bandwidth.

You cannot mix bandwidth types on a policy map. For example, you cannot configure bandwidth in a single policy map using both a bandwidth percent and in kilobits per second.

---

**Bandwidth Remaining Ratio**

You use the `bandwidth remaining ratio` policy-map class command to create a ratio for sharing unused bandwidth in specified queues. Any unused bandwidth will be used by these specific queues in the ratio that is specified by the configuration. Use this command when the `priority` command is also used for certain queues in the policy.
When you assign ratios, the queues will be assigned certain weights which are in line with these ratios.

You can specify ratios using a range from 0 to 100. For example, you can configure a bandwidth remaining ratio of 2 on one class, and another queue with a bandwidth remaining ratio of 4 on another class. The bandwidth remaining ratio of 4 will be scheduled twice as often as the bandwidth remaining ratio of 2.

The total bandwidth ratio allocation for the policy can exceed 100. For example, you can configure a queue with a bandwidth remaining ratio of 50, and another queue with a bandwidth remaining ratio of 100.

### Weighted Tail Drop

The switch egress queues use an enhanced version of the tail-drop congestion-avoidance mechanism called weighted tail drop (WTD). WTD is implemented on queues to manage the queue lengths and to provide drop precedences for different traffic classifications.

As a frame is enqueued to a particular queue, WTD uses the frame’s assigned QoS label to subject it to different thresholds. If the threshold is exceeded for that QoS label (the space available in the destination queue is less than the size of the frame), the switch drops the frame.

Each queue has three configurable threshold values. The QoS label determines which of the three threshold values is subjected to the frame.

**Figure 40: WTD and Queue Operation**

The following figure shows an example of WTD operating on a queue whose size is 1000 frames. Three drop percentages are configured: 40 percent (400 frames), 60 percent (600 frames), and 100 percent (1000 frames). These percentages indicate that up to 400 frames can be queued at the 40-percent threshold, up to 600 frames at the 60-percent threshold, and up to 1000 frames at the 100-percent threshold.

In the example, CoS value 6 has a greater importance than the other CoS values, and is assigned to the 100-percent drop threshold (queue-full state). CoS values 4 is assigned to the 60-percent threshold, and CoS values 3 is assigned to the 40-percent threshold. All of these threshold values are assigned using the `queue-limit cos` command.

Assuming the queue is already filled with 600 frames, and a new frame arrives. It contains CoS value 4 and is subjected to the 60-percent threshold. If this frame is added to the queue, the threshold will be exceeded, so the switch drops it.

**Related Topics**

- Configuring Queue Limits (CLI), on page 680
- Examples: Queue-limit Configuration, on page 702

### Weighted Tail Drop Default Values

The following are the Weighted Tail Drop (WTD) default values and the rules for configuring WTD threshold values.

- If you configure less than three queue-limit percentages for WTD, then WTD default values are assigned to these thresholds.
The following are the WTD threshold default values:

Table 48: WTD Threshold Default Values

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Default Value Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>80</td>
</tr>
<tr>
<td>1</td>
<td>90</td>
</tr>
<tr>
<td>2</td>
<td>400</td>
</tr>
</tbody>
</table>

- If 3 different WTD thresholds are configured, then the queues are programmed as configured.
- If 2 WTD thresholds are configured, then the maximum value percentage will be 400.
- If a WTD single threshold is configured as x, then the maximum value percentage will be 400.
  - If the value of x is less than 90, then threshold1=90 and threshold 0= x.
  - If the value of x equals 90, then threshold1=90, threshold 0=80.
  - If the value x is greater than 90, then threshold1=x, threshold 0=80.

Priority Queues

Each port supports eight egress queues, of which two can be given a priority.

You use the priority level policy class-map command to configure the priority for two classes. One of the classes has to be configured with a priority queue level 1, and the other class has to be configured with a priority queue level 2. Packets on these two queues are subjected to less latency with respect to other queues.

Note

You can configure a priority only with a level.

Only one strict priority or a priority with levels is allowed in one policy map. Multiple priorities with the same priority levels without kbps/percent are allowed in a policy map only if all of them are configured with police.

Related Topics

Configuring Priority (CLI), on page 675

Queue Buffer

In Cisco IOS XE Release 3.7.5 E and later releases, all downlink ports are allocated 1 GB port buffer, even though the downlink port size is 10GB. Prior to this change, all 1 GB downlink ports had 1 GB buffer and 10 GB downlink ports had 10 GB buffer.

At boot time, when there is no policy map enabled on the wired port, there are two queues created by default. Wired ports can have a maximum of 8 queues configured using MQC-based policies. The following table shows which packets go into which one of the queues:
You can guarantee the availability of buffers, set drop thresholds, and configure the maximum memory allocation for a queue. You use the `queue-buffers` policy-map class command to configure the queue buffers. You use the `queue-limit` policy-map class command to configure the maximum thresholds.

There are two types of buffer allocations: hard buffers, which are explicitly reserved for the queue, and soft buffers, which are available for other ports when unused by a given port.

For the wireless port default, Queue 0 will be given 40 percent of the buffers that are available for the interface as hard buffers, that is 67 buffers are allocated for Queue 0 in the context of 1-gigabit ports. The soft maximum for this queue is set to 268 (calculated as 67 * 400/100) for 1-gigabit ports, where 400 is the default maximum threshold that is configured for any queue.

For the wired port default, Queue 0 will be given 40 percent of the buffers that are available for the interface as hard buffers, that is 120 buffers are allocated for Queue 0 in the context of 1-gigabit ports, and 720 buffers in the context of 10-gigabit ports. The soft maximum for this queue is set to 480 (calculated as 120 * 400/100) for 1-gigabit ports and 2880 for 10-gigabit ports, where 400 is the default maximum threshold that is configured for any queue.

### Queue Buffer Allocation

The buffer allocation to any queue can be tuned using the `queue-buffers ratio` policy-map class configuration command.

#### Related Topics

- [Configuring Queue Buffers (CLI)](onpage678)
- [Examples: Queue Buffers Configuration](onpage703)

### Dynamic Threshold and Scaling

Traditionally, reserved buffers are statically allocated for each queue. No matter whether the queue is active or not, its buffers are held up by the queue. In addition, as the number of queues increases, the portion of the reserved buffers allocated for each queue can become smaller and smaller. Eventually, a situation may occur where there are not enough reserved buffers to support a jumbo frame for all queues.

The switch supports Dynamic Thresholding and Scaling (DTS), which is a feature that provides a fair and efficient allocation of buffer resources. When congestion occurs, this DTS mechanism provides an elastic buffer allocation for the incoming data based on the occupancy of the global/port resources. Conceptually, DTS scales down the queue buffer allocation gradually as the resources are used up to leave room for other queues, and vice versa. This flexible method allows the buffers to be more efficiently and fairly utilized.

As mentioned in the previous sections, there are two limits configured on a queue—a hard limit and a soft limit.

Hard limits are not part of DTS. These buffers are available only for that queue. The sum of the hard limits should be less than the globally set up hard maximum limit. The global hard limit configured for egress
Queuing is currently set to 5705. In the default scenario when there are no MQC policies configured, the 24 1-gigabit ports would take up $24 \times 67 = 1608$, and the 4 10-gigabit ports would take up $4 \times 720 = 2880$, for a total of 4488 buffers, allowing room for more hard buffers to be allocated based upon the configuration.

Soft limit buffers participate in the DTS process. Additionally, some of the soft buffer allocations can exceed the global soft limit allocation. The global soft limit allocation for egress queuing is currently set to 7607. The sum of the hard and soft limits add up to 13312, which in turn translates to 3.4 MB. Because the sum of the soft buffer allocations can exceed the global limit, it allows a specific queue to use a large number of buffers when the system is lightly loaded. The DTS process dynamically adjusts the per-queue allocation as the system becomes more heavily loaded.

Queuing in Wireless

Queuing in the wireless component is performed based on the port policy and is applicable only in the downstream direction. The wireless module supports the following four queues:

- **Voice**—This is a strict priority queue. Represented by Q0, this queue processes control traffic and multicast or unicast voice traffic. All control traffic (such as CAPWAP packets) is processed through the voice queue. The QoS module uses a different threshold within the voice queue to process control and voice packets to ensure that control packets get higher priority over other non-control packets.

- **Video**—This is a strict priority queue. Represented by Q1, this queue processes multicast or unicast video traffic.

- **Data NRT**—Represented by Q2, this queue processes all non-real-time unicast traffic.

- **Multicast NRT**—Represented by Q3, this queue processes Multicast NRT traffic. Any traffic that does not match the traffic in Q0, Q1, or Q2 is processed through Q3.

By default, the queues Q0 and Q1 are not enabled.

A weighted round-robin policy is applied for traffic in the queues Q2 and Q3.

For upstream direction only one queue is available. Port and radio policies are applicable only in the downstream direction.

The wired ports support eight queues.

Trust Behavior

Trust Behavior for Wired and Wireless Ports

For wired or wireless ports that are connected to the switch (end points such as IP phones, laptops, cameras, telepresence units, or other devices), their DSCP, precedence, or CoS values coming in from these end points are trusted by the switch and therefore are retained in the absence of any explicit policy configuration.
This trust behavior is applicable to both upstream and downstream QoS.

The packets are enqueued to the appropriate queue per the default initial configuration. No priority queuing at the switch is done by default. This is true for unicast and multicast packets.

In scenarios where the incoming packet type differs from the outgoing packet type, the trust behavior and the queuing behavior are explained in the following table. Note that the default trust mode for a port is DSCP based. The trust mode ‘falls back’ to CoS if the incoming packet is a pure Layer 2 packet. You can also change the trust setting from DSCP to CoS. This setting change is accomplished by using an MQC policy that has a class default with a 'set cos cos table default default-cos' action, where default-cos is the name of the table map created (which only performs a default copy).

### Table 42: Trust and Queueing Behavior

<table>
<thead>
<tr>
<th>Incoming Packet</th>
<th>Outgoing Packet</th>
<th>Trust Behavior</th>
<th>Queuing Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 3</td>
<td>Layer 3</td>
<td>Preserve DSCP/Precedence</td>
<td>Based on DSCP</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Layer 2</td>
<td>Not applicable</td>
<td>Based on CoS</td>
</tr>
<tr>
<td>Tagged</td>
<td>Tagged</td>
<td>Preserve DSCP and CoS</td>
<td>Based on DSCP (trust DSCP takes precedence)</td>
</tr>
<tr>
<td>Layer 3</td>
<td>Tagged</td>
<td>Preserve DSCP, CoS is set to 0</td>
<td>Based on DSCP</td>
</tr>
</tbody>
</table>

The Cisco IOS XE 3.2 Release supported different trust defaults for wired and wireless ports. The trust default for wired ports was the same as for this software release. For wireless ports, the default system behavior was non-trust, which meant that when the switch came up, all markings for the wireless ports were defaulted to zero and no traffic received priority treatment. For compatibility with an existing wired switch, all traffic went to the best-effort queue by default. The access point performed priority queuing by default. In the downstream direction, the access point maintained voice, video, best-effort, and background queues for queuing. The access selected the queuing strategy based on the 11e tag information. By default, the access point treated all wireless packets as best effort.

### Related Topics
- Configuring Trust Behavior for Wireless Traffic (CLI), on page 664
- Example: Table Map Configuration to Retain CoS Markings, on page 707

### Port Security on a Trusted Boundary for Cisco IP Phones

In a typical network, you connect a Cisco IP Phone to a switch port and cascade devices that generate data packets from the back of the telephone. The Cisco IP Phone guarantees the voice quality through a shared data link by marking the CoS level of the voice packets as high priority (CoS = 5) and by marking the data packets as low priority (CoS = 0). Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the class of service (CoS) 3-bit field, which is the priority of the packet.

For most Cisco IP Phone configurations, the traffic sent from the telephone to the switch should be trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the trust device interface configuration command, you configure the switch port to which the telephone is connected to trust the traffic received on that port.
The `trust device device_type` command available in interface configuration mode is a stand-alone command on the switch. When using this command in an AutoQoS configuration, if the connected peer device is not a corresponding device (defined as a device matching your trust policy), both CoS and DSCP values are set to "0" and any input policy will not take effect. If the connected peer device is a corresponding device, input policy will take effect.

With the trusted setting, you also can use the trusted boundary feature to prevent misuse of a high-priority queue if a user bypasses the telephone and connects the PC directly to the switch. Without trusted boundary, the CoS labels generated by the PC are trusted by the switch (because of the trusted CoS setting). By contrast, trusted boundary uses CDP to detect the presence of a Cisco IP Phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue. Note that the trusted boundary feature is not effective if the PC and Cisco IP Phone are connected to a hub that is connected to the switch.

**Wireless QoS Mobility**

Wireless QoS mobility enables you to configure QoS policies so that the network provides the same service anywhere in the network. A wireless client can roam from one location to another and as a result the client can get associated to different access points associated with a different switch. Wireless client roaming can be classified into two types:

- Intra-switch roaming
- Inter-switch roaming

The client policies must be available on all of the switches in the mobility group. The same SSID and port policy must be applied to all switches in the mobility group so that the clients get consistent treatment.

**Inter-Switch Roaming**

When a client roams from one location to another, the client can get associated to access points either associated to the same switch (anchor switch) or a different switch (foreign switch). Inter-switch roaming refers to the scenario where the client gets associated to an access point that is not associated to the same device before the client roamed. The host device is now foreign to the device to which the client was initially anchored.

In the case of inter-switch roaming, the client QoS policy is always executed on the foreign controller. When a client roams from anchor switch to foreign switch, the QoS policy is uninstalled on the anchor switch and installed on the foreign switch. In the mobility handoff message, the anchor device passes the name of the policy to the foreign switch. The foreign switch should have a policy with the same name configured for the QoS policy to be applied correctly.

In the case of inter-switch roaming, all of the QoS policies are moved from the anchor device to the foreign device. While the QoS policies are in transition from the anchor device to the foreign device, the traffic on the foreign device is provided the default treatment. This is comparable to a new policy installation on the client target.
If the foreign device is not configured with the user-defined physical port policy, the default port policy is applicable to all traffic is routed through the NRT queue, except the control traffic which goes through RT1 queue. The network administrator must configure the same physical port policy on both the anchor and foreign devices symmetrically.

During inter-switch roaming, client and SSID policy statistics are collected only for the duration that the client is associated with the foreign switch. Cumulative statistics for the whole roaming (anchor switch and foreign switch) are not collected.

**Intra-Switch Roaming**

With intra-switch roaming, the client gets associated to an access point that is associated to the same switch before the client roamed, but this association to the device occurs through a different access point.

**Note**

QoS policies remain intact in the case of intra-switch roaming.

**Precious Metal Policies for Wireless QoS**

Wireless QoS is backward compatible with the precious metal policies offered by the unified wireless controller platforms. The precious metal policies are system-defined policies that are available on the controller.

The following policies are available:

- Platinum—Used for VoIP clients.
- Gold—Used for video clients.
- Silver—Used for traffic that can be considered best-effort.
- Bronze—Used for NRT traffic.

These policies (also known as profiles) can be applied to a WLAN based on the traffic. We recommend the configuration using the Cisco IOS MQC configuration. The policies are available in the system based on the precious metal policy required. You can configure precious metal policies only for SSID ingress and egress policies.

Based on the policies applied, the 802.1p, 802.11e (WMM), and DSCP fields in the packets are affected. These values are preconfigured and installed when the switch is booted.

**Note**

Unlike the precious metal policies that were applicable in the Cisco Unified Wireless controllers, the attributes rt-average-rate, nrt-average-rate, and peak rates are not applicable for the precious metal policies configured on this switch platform.

**Note**

The 802.1p protocol priority is applicable on the Cisco 5700 Series Wireless Controller.
Standard QoS Default Settings

Default Wired QoS Configuration

There are two queues configured by default on each wired interface on the switch. All control traffic traverses and is processed through queue 0. All other traffic traverses and is processed through queue 1.

DSCP Maps

Default CoS-to-DSCP Map

When DSCP transparency mode is disabled, the DSCP values are derived from CoS as per the following table. If these values are not appropriate for your network, you need to modify them.

Note: The DSCP transparency mode is disabled by default. If it is enabled (no mls qos rewrite ip dscp interface configuration command), DSCP rewrite will not happen.

Table 43: Default CoS-to-DSCP Map

<table>
<thead>
<tr>
<th>CoS Value</th>
<th>DSCP Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>5</td>
<td>40</td>
</tr>
<tr>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>7</td>
<td>56</td>
</tr>
</tbody>
</table>

Default IP-Precedence-to-DSCP Map

You use the IP-precedence-to-DSCP map to map IP precedence values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic. The following table shows the default IP-precedence-to-DSCP map. If these values are not appropriate for your network, you need to modify them.

Table 44: Default IP-Precedence-to-DSCP Map

<table>
<thead>
<tr>
<th>IP Precedence Value</th>
<th>DSCP Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
</tr>
</tbody>
</table>
Default DSCP-to-CoS Map

You use the DSCP-to-CoS map to generate a CoS value, which is used to select one of the four egress queues. The following table shows the default DSCP-to-CoS map. If these values are not appropriate for your network, you need to modify them.

Table 45: Default DSCP-to-CoS Map

<table>
<thead>
<tr>
<th>IP Precedence Value</th>
<th>DSCP Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>5</td>
<td>40</td>
</tr>
<tr>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>7</td>
<td>56</td>
</tr>
</tbody>
</table>

Default Wireless QoS Configuration

The ports on the switch do not distinguish between wired or wireless physical ports. Depending on the kind of device associated to the switch, the policies are applied. For example, when an access point is connected to a switch port, the switch detects it as a wireless device and applies the default hierarchical policy which is in the format of a parent-child policy. This policy is an hierarchical policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suite the QoS configuration. The switch is preconfigured with a default class map and a policy map.
Configuring Auto QoS for Wireless

Information About Auto QoS for Wireless

Auto QoS for Wireless feature, introduced in Cisco IOS XE Release 3.7.0, is supported on the following platforms:

- Cisco 5760 Wireless Controller
- Catalyst 3850 Series Switches
- Catalyst 3650 Series Switches
- Cisco Catalyst 4500E Supervisor Engine 8-E

The following pre-defined global configuration templates/profiles are available:

- Enterprise
- Voice
- Guest

You can customize these templates to suit your needs. Auto QoS for Wireless can be configured using both CLI and GUI. Auto QoS for Wireless can be applied on a per-WLAN basis.

Precedence applicable:

1. AAA QoS
2. Native Profile QoS
3. Auto QoS/CLI-based QoS

Policy Names

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>AutoQos-4.0-wlan-ET-Client-Input-Policy</td>
</tr>
<tr>
<td>P2</td>
<td>AutoQos-4.0-wlan-ET-SSID-Output-Policy</td>
</tr>
<tr>
<td>P3</td>
<td>platinum-up (Auto generated system policy at boot-up)</td>
</tr>
<tr>
<td>P4</td>
<td>platinum (Auto generated system policy at boot-up)</td>
</tr>
<tr>
<td>P5</td>
<td>AutoQos-4.0-wlan-GT-SSID-Input-Policy</td>
</tr>
<tr>
<td>P6</td>
<td>AutoQos-4.0-wlan-GT-SSID-Output-Policy</td>
</tr>
<tr>
<td>P7</td>
<td>port_child_policy</td>
</tr>
<tr>
<td>P8</td>
<td>AutoQos-4.0-wlan-Port-Output-Policy</td>
</tr>
<tr>
<td>P9</td>
<td>Capwap-SRND4-Queuing-Policy</td>
</tr>
</tbody>
</table>
List of Targets

- Client
- BSSID
- Radio
- AP Port (Catalyst 3850 Switch)
- Uplink Port (Catalyst 3850 Switch)
- Cisco 5760 WLC physical port
- Catalyst 4500E Supervisor Engine 8-E Front Panel Ports

Auto QoS for Wireless - Wireless QoS Matrix

<table>
<thead>
<tr>
<th>Topology</th>
<th>Client</th>
<th>BSSID</th>
<th>Radio</th>
<th>AP Port (Catalyst 3850 Switch)</th>
<th>Uplink Port (Catalyst 3850 Switch)</th>
<th>Cisco 5760 WLC physical port</th>
<th>Catalyst 4500E Supervisor Engine 8-E Front Panel Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
</tr>
<tr>
<td>Enterprise</td>
<td>P1</td>
<td>N/A</td>
<td>N/A</td>
<td>P2</td>
<td>N/A</td>
<td>P7</td>
<td>N/A</td>
</tr>
<tr>
<td>Voice</td>
<td>N/A</td>
<td>N/A</td>
<td>P3</td>
<td>P4</td>
<td>N/A</td>
<td>P7</td>
<td>N/A</td>
</tr>
<tr>
<td>Guest</td>
<td>N/A</td>
<td>N/A</td>
<td>P5</td>
<td>P6</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Guidelines for Auto QoS for Wireless

- The Catalyst 3850 Switch uplink ports should not be configured along with Auto QoS for Wireless. This should be managed using Wired Auto QoS.
- The Catalyst 3850 Switch AP Port Policy (port_child_policy) and Cisco 5760 WLC physical ports should be automatically configured for Enterprise and Voice templates.
- AP Control traffic must go through the P0 queue (should be given highest priority among all traffic).
- All the Auto QoS policies for Wireless applied through the GUI have the prefix 'AutoQos-4.0'. This enables you to recognize the policies that are applied through templates.
- On the CLI, it is not possible to create a policy name that starts with 'AutoQos-4.0' because this is reserved for policies generated through templates.

Configuring Auto QoS for Wireless (GUI)

Procedure

Step 1 Choose Configuration > Wireless > WLAN.
Step 2  Click the WLAN ID.
Step 3  Click the QoS tab.
Step 4  In the Auto QoS section, choose the policy from the drop-down list.

Note  By default, the Auto QoS policy applied for a WLAN is 'None'.

Step 5  Save the configuration.

Configuring Auto QoS for Wireless (CLI)

Switch(config-wlan)# auto qos {enterprise | guest | voice}

Guidelines for QoS Policies

Follow these guidelines to prevent clients from getting excluded due to malformed QoS policies:

• When a new QoS policy is added to the switch, a QoS policy with the same name should be added to other switch within the same roam or mobility domain.

• When a switch is loaded with a software image of a later release, the new policy formats are supported. If you have upgraded the software image from an earlier release to a later release, you should save the configuration separately. When an earlier release image is loaded, some QoS policies might show as not supported, and you should restore those QoS policies to supported policy formats.

Restrictions for QoS on Wired Targets

A target is an entity where a policy is applied. You can apply a policy to either a wired or wireless target. A wired target can be either a port or VLAN. A wireless target can be either a port, radio, SSID, or client. Only port, SSID, and client policies are user configurable. Radio policies are not user configurable. Wireless QoS policies for port, radio, SSID, and client are applied in the downstream direction, and for upstream only SSID and client targets are supported. Downstream indicates that traffic is flowing from the switch to the wireless client. Upstream indicates that traffic is flowing from wireless client to the switch.

The following are restrictions for applying QoS features on the switch for the wired target:

• A maximum of 8 queuing classes are supported on the switch port for the wired target.

• A maximum of 63 policers are supported per policy on the wired port for the wired target.

• In Cisco IOS XE Release 3.7.5E and later releases, by default all downlink ports are allocated 1 GB port buffer, even though the downlink port size is 10 GB. Prior to this change, all 1 GB downlink ports had 1 GB buffer and 10 GB downlink ports had 10 GB buffer.

• A maximum of 1599 policy-maps can be created.

• No more than two levels are supported in a QoS hierarchy.

• In a hierarchical policy, overlapping actions between parent and child are not allowed, except when a policy has the port shaper in the parent and queueing features in the child policy.

• A QoS policy cannot be attached to any EtherChannel interface.
• Policing in both the parent and child is not supported in a QoS hierarchy.
• Marking in both the parent and child is not supported in a QoS hierarchy.
• A mixture of queue limit and queue buffer in the same policy is not supported.

---

**Note**
The queue-limit percent is not supported on the switch because the **queue-buffer** command handles this functionality. Queue limit is only supported with the DSCP and CoS extensions.

---

• With shaping, there is an IPG overhead of 20Bytes for every packet that is accounted internally in the hardware. Shaping accuracy will be affected by this, specially for packets of small size.
• The classification sequence for all wired queuing-based policies should be the same across all wired upstream ports (10-Gigabit Ethernet), and the same for all downstream wired ports (1-Gigabit Ethernet).
• Empty classes are not supported.
• Class-maps with empty actions are not supported. If there are two policies with the same order of class-maps and if there are class-maps with no action in one of the policies, there may be traffic drops. As a workaround, allocate minimal bandwidth for all the classes in PRIORITY_QUEUE.
• A maximum of 256 classes are supported per policy on the wired port for the wired target.
• The actions under a policer within a policy map have the following restrictions:
  • The conform action must be transmit.
  • The exceed/violate action for markdown type can only be cos2cos, prec2prec, dscp2dscp.
  • The markdown types must be the same within a policy.
• A port-level input marking policy takes precedence over an SVI policy; however, if no port policy is configured, the SVI policy takes precedence. For a port policy to take precedence, define a port-level policy; so that the SVI policy is overwritten.
• Classification counters have the following specific restrictions:
  • Classification counters count packets instead of bytes.
  • Filter-based classification counters are not supported
  • Only QoS configurations with marking or policing trigger the classification counter.
  • The classification counter is not port based. This means that the classification counter aggregates all packets belonging to the same class of the same policy which attach to different interfaces.
  • As long as there is policing or marking action in the policy, the class-default will have classification counters.
  • When there are multiple match statements in a class, then the classification counter only shows the traffic counter for one of the match statements.
• Table maps have the following specific restrictions:
  • Only one table map for policing exceeding the markdown and one table map for policing violating the markdown per direction per target is supported.
Restrictions for QoS on Wired Targets

Table maps must be configured under the class-default; table maps are unsupported for a user-defined class.

Hierarchical policies are required for the following:
- Port-shapers
- Aggregate policers
- PV policy
- Parent shaping and child marking/policing

In a HQoS policy with parent shaping and child policy having priority level queuing and priority level policing, the statistics for policing are not updated. Only QoS shaper statistics are updated. To view the QoS shaper statistics, use the `show policy-map interface` command in global configuration mode.

For ports with wired targets, these are the only supported hierarchical policies:
- Police chaining in the same policy is unsupported, except for wireless client.
- Hierarchical queueing is unsupported in the same policy (port shaper is the exception).
- In a parent class, all filters must have the same type. The child filter type must match the parent filter type with the following exceptions:
  - If the parent class is configured to match IP, then the child class can be configured to match the ACL.
  - If the parent class is configured to match CoS, then the child class can be configured to match the ACL.

The `trust device device_type` command available in interface configuration mode is a stand-alone command on the switch. When using this command in an AutoQoS configuration, if the connected peer device is not a corresponding device (defined as a device matching your trust policy), both CoS and DSCP values are set to "0" and any input policy will not take effect. If the connected peer device is a corresponding device, input policy will take effect.

The following are restrictions for applying QoS features on the VLAN to the wired target:
- For a flat or nonhierarchical policy, only marking or a table map is supported.

The following are restrictions and considerations for applying QoS features on EtherChannel and channel member interfaces:
- QoS is not supported on an EtherChannel interface.
- QoS is supported on EtherChannel member interfaces in both ingress and egression directions. All EtherChannel members must have the same QoS policy applied. If the QoS policy is not the same, each individual policy on the different link acts independently.
- On attaching a service policy to channel members, the following warning message appears to remind the user to make sure the same policy is attached to all ports in the EtherChannel: 'Warning: add service policy will cause inconsistency with port xxx in ether channel xxx.'
- Auto QoS is not supported on EtherChannel members.
On attaching a service policy to an EtherChannel, the following message appears on the console: 'Warning: add service policy will cause inconsistency with port xxx in etherchannel xxx.' This warning message should be expected. This warning message is a reminder to attach the same policy to other ports in the same EtherChannel. The same message will be seen during boot up. This message does not mean there is a discrepancy between the EtherChannel member ports.

Related Topics
- Restrictions for QoS on Wireless Targets, on page 632
- Prerequisites for Quality of Service, on page 589
- QoS Overview, on page 591
- QoS Implementation, on page 602

Restrictions for QoS on Wireless Targets

General Restrictions

A target is an entity where a policy is applied. You can apply a policy to either a wired or wireless target. A wired target can be either a port or VLAN. A wireless target can be either a port, radio, SSID, or client. Only port, SSID, and client policies are user configurable. Radio polices are not user configurable. Wireless QoS policies for port, radio, SSID, and client are applied in the downstream direction, and for upstream only SSID and client targets are supported. Downstream indicates that traffic is flowing from the switch to the wireless client. Upstream indicates that traffic is flowing from wireless client to the switch.

Note

On attaching a service policy to an EtherChannel, the following message appears on the console: 'Warning: add service policy will cause inconsistency with port xxx in etherchannel xxx.' This warning message should be expected. This warning message is a reminder to attach the same policy to other ports in the same EtherChannel. The same message will be seen during boot up. This message does not mean there is a discrepancy between the EtherChannel member ports.

Note

On attaching a service policy to an EtherChannel, the following message appears on the console: 'Warning: add service policy will cause inconsistency with port xxx in etherchannel xxx.' This warning message should be expected. This warning message is a reminder to attach the same policy to other ports in the same EtherChannel. The same message will be seen during boot up. This message does not mean there is a discrepancy between the EtherChannel member ports.

Note

Auto QOS SRND is enabled by default on the Cisco Catalyst 4500E Supervisor Engine 8-E. When AP is connected, egress QoS policy is automatically applied on the AP connected ports and the QoS policy is removed when the AP is disconnected. This policy classification is applied through DSCP, so the drop threshold can be configured for voice and CAPWAP control packets. All other traffic goes to different queues. If you prefer to have a different QoS policy to prioritize different class of traffic, you can configure it using the 'no auto qos srnd4' command. This will remove the Auto QOS SRND4 policies attached to AP connected port and BB-DC inter-link port, and a default policy to protect CAPWAP control and voice traffic will be attached to BB-DC inter-link port.

• Only port, SSID, and client (using AAA and Cisco IOS command-line interface) policies are user-configurable. Radio policies are set by the wireless control module and are not user-configurable.
• Port and radio policies are applicable only in the egress direction.
• SSID and client targets can be configured only with marking and policing policies.
• One policy per target per direction is supported.
• For the egress class-default SSID policy, you must configure the queue buffer ratio as 0 after you configure the average shape rate.
• Class maps in a policy map can have different types of filters. However, only one marking action (either table map, or set dscp, or set cos) is supported in a map in egress direction.
• For hierarchical client and SSID ingress policies, you cannot configure marking in both the parent and child policies. You can only configure marking either in the parent or child policy.
• You cannot configure multiple set actions in the same class.
• For both SSID and client ingress policies, supported set actions are only for DSCP, and CoS values.
• You cannot delete a group of WLANs or QoS policy.

Wireless QoS Restrictions on Ports

The following are restrictions for applying QoS features on a wireless port target:

• All wireless ports have similar parent policy with one class-default and one action shape under class-default. Shape rates are dependent on the 802.11a/b/g/ac bands.
• You can create a maximum of four classes in a child policy by modifying the port_child_policy.
• If there are four classes in the port_child_policy at the port level, one must be a non-client-nrt class and one must be class-default.
• No two classes can have the same priority level. Only priority level 1 (for voice traffic and control traffic) and 2 (for video) are supported.
• Priority is not supported in the multicast NRT class (non-client-nrt class) and class-default.
• If four classes are configured, two of them have to be priority classes. If only three classes are configured, at least one of them should be a priority class. If three classes are configured and there is no non-client-nrt class, both priority levels must be present.
• Only match DSCP is supported.
• The port policy applied by the wireless control module cannot be removed using the CLI.
• Both priority rate and police CIR (using MQC) in the same class is unsupported.
• Queue limit (which is used to configure Weighted Tail Drop) is unsupported.

Wireless QoS Restrictions on SSID

The following are restrictions for applying QoS features on SSID:

• One table map is supported at the ingress policy.
• Table maps are supported for the parent class-default only. Up to two table maps are supported in the egress direction and three table-maps can be configured when a QoS group is involved.

Note: Table-maps are not supported at the client targets.

• If a wireless port has a default policy with only two queues (one for multicast-NRT, one for class-default), the policy at SSID level cannot have voice and video class in the egress direction.
• Policing without priority is not supported in the egress direction.
• Priority configuration at the SSID level is used only to configure the RT1 and RT2 policers (AFD for policer). Priority configuration does not include the shape rate. Therefore, priority is restricted for SSID policies without police.
Restrictions for QoS on Wireless Targets

- If `set` is not enabled in class-default, the classification at the SSID for voice or video must be a subset of the classification for the voice or video class at the port level.
- The mapping in the DSCP2DSCP and COS2COS table should be based on the classification function for the voice and video classes in the port level policy.
- No action is allowed under the class-default of a child policy.
- For SSID ingress policies, only UP and DSCP filters (match criteria) are supported. ACL and protocol match criteria are not supported.
- For a flat policy (non-hierarchical), in the ingress direction, the policy configuration must be a set (table map) or policing or both.

**Wireless QoS Restrictions on Clients**

The following are restrictions for applying QoS policies on client targets:

- The default client policy is enabled only on WMM clients that are ACM-enabled.
- Queuing is not supported.
- Attaching, removing, or modifying client policies on a WLAN in the enabled state is not supported. You must shut down the WLAN to apply, remove, or modify a policy.
- Table-map configuration is not supported for client targets.
- Policing and set configured together in class-default is blocked in egress direction:

```
policy-map foo
  class class-default
  police X
  set dscp Y
```

- Child policy is not supported under class-default if the parent policy contains other user-defined class maps in it.
- For flat egress client policy, policing in class-default and marking action in other classes are not supported.
- Only set marking actions are supported in the client policies.
- For client ingress policies, only ACL, UP, DSCP, and protocol filters (match criteria) are supported.
- All the filters in classes in a policy map for client policy must have the same attributes. Filters matching on protocol-specific attributes such as IPv4 or IPv6 addresses are considered as different attribute sets.
- For filters matching on ACLs, all ACEs (Access Control Entry) in the access list should have the same type and number of attributes.
- In client egress policies, all filters in the policy-map must match on the same marking attribute for filters matching on marking attributes. For example, If filter matches on DSCP, then all filters in the policy must match on DSCP.
- ACL matching on port ranges and subnet are only supported in ingress direction.

**Related Topics**

- Configuring Port Policies (GUI), on page 686
How to Configure QoS

Configuring Class, Policy, and Table Maps

Creating a Traffic Class (CLI)

To create a traffic class containing match criteria, use the `class-map` command to specify the traffic class name, and then use the following `match` commands in class-map configuration mode, as needed.

**Before you begin**

All match commands specified in this configuration task are considered optional, but you must configure at least one match criterion for a class.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
</tbody>
</table>

<p>| <strong>Step 2</strong> | Enters class map configuration mode. |
| <code>class-map class-map name{ match-any | match-all}</code> | |
| Example: | Switch(config)# class-map test_1000 Switch(config-cmap)# |
| - Creates a class map to be used for matching packets to the class whose name you specify. |
| - <strong>match-any</strong>: Any one of the match criteria must be met for traffic entering the traffic class to be classified as part of it. |
| - <strong>match-all</strong>: All of the match criteria must be met for traffic entering the traffic class to be classified as part of the traffic class. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>This is the default. If <strong>match-any</strong> or <strong>match-all</strong> is not explicitly defined, <strong>match-all</strong> is chosen by default.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>match access-group {index number</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-cmap)# match access-group 100 Switch(config-cmap)#</td>
</tr>
<tr>
<td></td>
<td>The following parameters are available for this command:</td>
</tr>
<tr>
<td></td>
<td>• access-group</td>
</tr>
<tr>
<td></td>
<td>• class-map</td>
</tr>
<tr>
<td></td>
<td>• cos</td>
</tr>
<tr>
<td></td>
<td>• dscp</td>
</tr>
<tr>
<td></td>
<td>• ip</td>
</tr>
<tr>
<td></td>
<td>• non-client-nrt</td>
</tr>
<tr>
<td></td>
<td>• precedence</td>
</tr>
<tr>
<td></td>
<td>• qos-group</td>
</tr>
<tr>
<td></td>
<td>• vlan</td>
</tr>
<tr>
<td></td>
<td>• wlan user priority</td>
</tr>
<tr>
<td>(Optional)</td>
<td>For this example, enter the access-group ID:</td>
</tr>
<tr>
<td></td>
<td>• Access list index (value from 1 to 2799)</td>
</tr>
<tr>
<td></td>
<td>• Named access list</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>match class-map class-map name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-cmap)# match class-map test_2000 Switch(config-cmap)#</td>
</tr>
<tr>
<td>(Optional)</td>
<td>Matches to another class-map name.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>match cos cos value</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-cmap)# match cos 2 3 4 5 Switch(config-cmap)#</td>
</tr>
<tr>
<td>(Optional)</td>
<td>Matches IEEE 802.1Q or ISL class of service (user) priority values.</td>
</tr>
<tr>
<td></td>
<td>• Enters up to 4 CoS values separated by spaces (0 to 7).</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>match dscp dscp value</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>(Optional) Matches the DSCP values in IPv4 and IPv6 packets.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| Switch(config-cmap)# match dscp af11 af12  
Switch(config-cmap)# | (Optional) Matches IP values including the following:
  * `dscp`—Matches IP DSCP (DiffServ codepoints).
  * `precedence`—Matches IP precedence (0 to 7).

**Note** Since CPU generated packets are not marked at egress, the packet will not match the configured class-map. |
| Step 7 match ip {dscp dscp value | precedence precedence value }  
Example:  
Switch(config-cmap)# match ip dscp af11 af12  
Switch(config-cmap)# | (Optional) Matches non-client NRT (Non-Real-Time).

**Note** This match is applicable only for policies on a wireless port. It carries all the multi-destination and AP (non-client) bound traffic. |
| Step 8 match non-client-nrt  
Example:  
Switch(config-cmap)# match non-client-nrt  
Switch(config-cmap)# | (Optional) Matches QoS group value (from 0 to 31). |
| Step 9 match qos-group qos group value  
Example:  
Switch(config-cmap)# match qos-group 10  
Switch(config-cmap)# | (Optional) Matches a VLAN ID (from 1 to 4095). |
| Step 10 match vlan vlan value  
Example:  
Switch(config-cmap)# match vlan 210  
Switch(config-cmap)# | (Optional) Matches 802.11e specific values. Enter the user priority 802.11e user priority (0 to 7). |
| Step 11 match wlan user-priority wlan value  
Example:  
Switch(config-cmap)# match wlan user priority 7  
Switch(config-cmap)# | Saves the configuration changes. |
| Step 12 end | |
What to do next

Configure the policy map.

Related Topics

- Class Maps, on page 608
- Examples: Classification by Access Control Lists, on page 692

Creating a Traffic Policy (CLI)

To create a traffic policy, use the `policy-map` global configuration command to specify the traffic policy name.

The traffic class is associated with the traffic policy when the `class` command is used. The `class` command must be entered after you enter the policy map configuration mode. After entering the `class` command, the switch is automatically in policy map class configuration mode, which is where the QoS policies for the traffic policy are defined.

The following policy map class-actions are supported:

- `admit`—Admits the request for Call Admission Control (CAC).
- `bandwidth`—Bandwidth configuration options.
- `exit`—Exits from the QoS class action configuration mode.
- `no`—Negates or sets default values for the command.
- `police`—Policer configuration options.
- `priority`—Strict scheduling priority configuration options for this class.
- `queue-buffers`—Queue buffer configuration options.
- `queue-limit`—Queue maximum threshold for Weighted Tail Drop (WTD) configuration options.
- `service-policy`—Configures the QoS service policy.
- `set`—Sets QoS values using the following options:
  - CoS values
  - DSCP values
  - Precedence values
  - QoS group values
  - WLAN values
- `shape`—Traffic-shaping configuration options.
Before you begin
You should have first created a class map.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.</td>
</tr>
<tr>
<td>policy-map policy-name</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config)# policy-map test_2000 Switch(config-pmap)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the name of the class whose policy you want to create or change. You can also create a system default class for unclassified packets.</td>
</tr>
<tr>
<td>class {class-name</td>
<td>class-default}</td>
</tr>
<tr>
<td>Example: Switch(config-pmap)# class test_1000 Switch(config-pmap-c)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Admits the request for Call Admission Control (CAC). For a more detailed example of this command and its usage, see the section Configuring Call Admission Control.</td>
</tr>
<tr>
<td>admit</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-pmap-c)# admit cac wmm-tspec Switch(config-pmap-c)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Sets the bandwidth using one of the following:</td>
</tr>
<tr>
<td>bandwidth {kb/s</td>
<td>kb/s value</td>
</tr>
<tr>
<td>Example: Switch(config-pmap-c)# bandwidth 50 Switch(config-pmap-c)#</td>
<td></td>
</tr>
</tbody>
</table>

Note This command only configures CAC for wireless QoS.

For a more detailed example of this command and its usage, see Configuring Bandwidth (CLI), on page 671.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **6** | exit | (Optional) Exits from QoS class action configuration mode.  
**Example:**  
Switch(config-pmap-c)# exit  
Switch(config-pmap-c)# |
| **7** | no | (Optional) Negates the command.  
**Example:**  
Switch(config-pmap-c)# no  
Switch(config-pmap-c)# |
| **8** | police \{target\_bit\_rate \| cir \| rate\} | (Optional) Configures the policer:  
**Example:**  
Switch(config-pmap-c)# police 100000  
Switch(config-pmap-c)#  

- **target\_bit\_rate**—Enter the bit rate per second, enter a value between 8000 and 10000000000.  
- **cir**—Committed Information Rate  
- **rate**—Specify policer rate, PCR for hierarchical policies or SCR for single-level ATM 4.0 policer policies.  

For a more detailed example of this command and its usage, see Configuring Police (CLI), on page 673. |
| **9** | priority \{kb/s \| level level value \| percent percentage value\} | (Optional) Sets the strict scheduling priority for this class. Command options include:  
**Example:**  
Switch(config-pmap-c)# priority percent 50  
Switch(config-pmap-c)#  

- **kb/s**—Kilobits per second, enter a value between 1 and 2000000.  
- **level**—Establishes a multi-level priority queue. Enter a value (1 or 2).  
- **percent**—Enter a percent of the total bandwidth for this priority.  

For a more detailed example of this command and its usage, see Configuring Priority (CLI), on page 675. |
| **10** | queue-buffers ratio ratio limit | (Optional) Configures the queue buffer for the class. Enter the queue buffers ratio limit (0 to 100).  
**Example:**  
Switch(config-pmap-c)# queue-buffers ratio 10  
Switch(config-pmap-c)#  

For a more detailed example of this command and its usage, see Configuring Queue Buffers (CLI), on page 678. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 11   | queue-limit \{packets | cos | dscp | percent\} | (Optional) Specifies the queue maximum threshold for the tail drop:  
  • packets—Packets by default, enter a value between 1 to 2000000.  
  • cos—Enter the parameters for each COS value.  
  • dscp—Enter the parameters for each DSCP value.  
  • percent—Enter the percentage for the threshold.  
Example:  
Switch(config-pmap-c) # queue-limit cos 7 percent 50  
Switch(config-pmap-c) # |
| 12   | service-policy policy-map name | (Optional) Configures the QoS service policy.  
Example:  
Switch(config-pmap-c) # service-policy test_2000  
Switch(config-pmap-c) # |
| 13   | set \{cos | dscp | ip | precedence | qos-group | wlan\} | (Optional) Sets the QoS values. Possible QoS configuration values include:  
  • cos—Sets the IEEE 802.1Q/ISL class of service/user priority.  
  • dscp—Sets DSCP in IP(v4) and IPv6 packets.  
  • ip—Sets IP specific values.  
  • precedence—Sets precedence in IP(v4) and IPv6 packet.  
  • qos-group—Sets the QoS Group.  
  • wlan—Sets the WLAN user-priority.  
Example:  
Switch(config-pmap-c) # set cos 7  
Switch(config-pmap-c) # |
| 14   | shape average \{target_bit_rate | percent\} | (Optional) Sets the traffic shaping. Command parameters include:  
  • target_bit_rate—Target bit rate.  
  • percent—Percentage of interface bandwidth for Committed Information Rate.  
Example:  
Switch(config-pmap-c) # shape average percent 50  
Switch(config-pmap-c) # |
## Configuring Client Policies (GUI)

### Procedure

1. Choose **Configuration > Wireless**.
2. Expand the **QoS** node by clicking on the left pane and choose **QoS-Policy**.
   
   The **QoS-Policy** page is displayed.

3. Click **Add New** to create a new QoS Policy.
   
   The **Create QoS Policy** page is displayed.

4. Select **Client** from the **Policy Type** drop-down menu.

5. Select the direction into which the policy needs to be applied from the **Policy Direction** drop-down menu.
   
   The available options are:
   - **Ingress**
   - **Egress**

6. Specify a policy name in the **Policy Name** text box.

7. Provide a description to the policy in the **Description** text box.

8. (Optional) Configure the default voice or video configuration parameters by checking the **Enable Voice** or **Enable Video** checkbox.

   The following options are available:
   - **Trust**—Specify the classification type behavior on this policy. The options available are:
     - **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
- **User Priority**—This option is available when the Policy Direction is ingress. Enter the 802.11e user priority. The range is from 0 to 7.

- **COS**—This option is available when the Policy Direction is egress. Matches IEEE 802.1Q class of service. The range is from 0 to 7.

- **Mark**—Specify the marking label for each packet. The following options are available:
  - **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  - **CoS**—Matches IEEE 802.1Q class of service. The range is from 0 to 7.
  - **User Priority**—Enter the 802.11e user priority. The range is from 0 to 7.

- **Police(kbps)**—Specify the policing rate in kbps.

**Note**  The marking and policing options are optional.

**Step 9**  Specify the Class-default parameters.

The following options are available:

- **Mark**—Specify the marking label for each packet. The following options are available:
  - **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  - **CoS**—Matches IEEE 802.1Q class of service. The range is from 0 to 7.
  - **User Priority**—Enter the 802.11e user priority. The range is from 0 to 7.

- **Police(kbps)**—This option is available when the Policy Direction is egress. This option Specify the policing rate in kbps.

**Note**  You can choose either Mark or Police action for the class-default class when creating an egress client policy.

**Step 10**  (Optional) To configure the AVC class map for a client policy, check the Enable Application Recognition check box

**Note**  For an egress client policy, when you enable Application Recognition, the Voice, Video, and User Defined check boxes are disabled.

The following options are available:

- **Trust**—Specify a classification type for this policy.
  - **Protocol**—Allows you to choose the protocols and configure the marking and policing of the packets.
  - **Category**—Allows you to choose the category of the application. For example, browsing.
  - **Subcategory**—Allows you to choose the subcategory of the application. For example, file-sharing.
  - **Application-Group**—Allows you to choose the application group. For example, ftp-group.

- **Protocol Choice**—Choose the protocols, category, subcategory, or application group from the Available Protocols list into the Assigned Protocols to apply the marking and policing of the packets.

- **Mark**—Specify the marking label for each packet. The following options are available:
• **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.

• **CoS**—Matches IEEE 802.1Q class of service. The range is from 0 to 7.

• **None**—Choose this option when you do not want to mark the packets.

• **Police (kbps)**—Specifies the policing rate in kbps. This option is available when the **Policy Direction** is egress.

• **Drop**—Drops the ingress packets that correspond to the chosen protocols.

**Step 11**
(Optional) To configure user defined classes, check the **User Defined Classes** checkbox.

The following options are available:

• **Trust**—Specify the classification type behavior on this policy.
  
  • **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  
  • **User Priority**—This option is available when the **Policy Direction** is ingress. Enter the 802.11e user priority. The range is from 0 to 7.
  
  • **COS**—This option is available when the **Policy Direction** is egress. Matches IEEE 802.1Q class of service. The range is from 0 to 7.

• **Mark**—Specify the marking label for each packet. The following options are available:
  
  • **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  
  • **CoS**—Matches IEEE 802.1Q class of service. The range is from 0 to 7.
  
  • **User Priority**—Enter the 802.11e user priority. The range is from 0 to 7.

• **Police (kbps)**—This option is available when the **Policy Direction** is egress. This option specifies the policing rate in kbps.

**Note** You can add a maximum of five user-defined classes for each client policy.

**Step 12** Click **Add** to add the policy.

**Related Topics**
- **Client Policies**, on page 599
- **Supported QoS Features on Wireless Targets**, on page 594
- **Examples: Client Policies**, on page 699

**Configuring Client Policies**

You can configure client policies using one of the following methods:
The wireless control module of the switch applies the default client policies when admission control (ACM) is enabled for WMM clients. When ACM is disabled, there is no default client policy.

The default policies are:
- **Ingress**—cldef from WMM
- **Egress**—cldef to WMM

You can verify if ACM is enabled by using the `show ap dot11 {5ghz | 24ghz}` command. To enable ACM, use the `ap dot11 {5ghz | 24ghz} cac voice acm` command.

<table>
<thead>
<tr>
<th>Method</th>
<th>Topic/Details</th>
</tr>
</thead>
</table>
| Default client policies                          | The wireless control module of the switch applies the default client policies when admission control (ACM) is enabled for WMM clients. When ACM is disabled, there is no default client policy. The default policies are:
|                                                 | • Ingress—cldef from WMM
|                                                 | • Egress—cldef to WMM
| Apply the client policy on the WLAN using the GUI | Configuring Client Policies (GUI)                                              |
| Apply the client policy on the WLAN using the CLI | Applying an SSID or Client Policy on a WLAN (CLI)                             |
| Apply the QoS attributes policy using a local profiling policy using the CLI | Applying a Local Policy for a Device on a WLAN (CLI)                         |
| Apply the QoS attributes policy using a local profiling policy using the GUI | • Choose Configuration > Security > Local Policies to create a local profiling policy.
|                                                 | • Choose Configuration > Wireless > WLAN > Policy Mapping to apply a local profiling policy on a WLAN.
|                                                 | For more information, see Applying Local Policies to WLAN (GUI), on page 496 |
| Apply policy map through a AAA server (ACS/ISE)  | Cisco Identity Services Engine User Guide
|                                                 | Cisco Secure Access Control System User Guide                                 |

**Configuring Class-Based Packet Marking (CLI)**

This procedure explains how to configure the following class-based packet marking features on your switch:

- CoS value
- DSCP value
- IP value
- Precedence value
- QoS group value
- WLAN value
Before you begin

You should have created a class map and a policy map before beginning this procedure.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

| Step 2 | policy-map policy name | Enters policy map configuration mode. |
| Example: | Switch(config)# policy-map policy1 | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |

| Step 3 | class class name | Enters policy class map configuration mode. |
| Example: | Switch(config-pmap)# class class1 | Specifies the name of the class whose policy you want to create or change. |

Command options for policy class map configuration mode include the following:

- **admit**—Admits the request for Call Admission Control (CAC).
- **bandwidth**—Bandwidth configuration options.
- **exit**—Exits from the QoS class action configuration mode.
- **no**—Negates or sets default values for the command.
- **police**—Policer configuration options.
- **priority**—Strict scheduling priority configuration options for this class.
- **queue-buffers**—Queue buffer configuration options.
- **queue-limit**—Queue maximum threshold for Weighted Tail Drop (WTD) configuration options.
- **service-policy**—Configures the QoS service policy.
- **set**—Sets QoS values using the following options:
### Purpose

**Command or Action**

- CoS values
- DSCP values
- Precedence values
- QoS group values
- WLAN values

**Purpose**

- **shape**—Traffic-shaping configuration options.

**Note**

This procedure describes the available configurations using `set` command options. The other command options (`admit`, `bandwidth`, etc.) are described in other sections of this guide. Although this task lists all of the possible `set` commands, only one `set` command is supported per class.

### Step 4

**set cos**

**(Optional)** Sets the specific IEEE 802.1Q Layer 2 CoS value of an outgoing packet. Values are from 0 to 7.

You can also set the following values using the `set cos` command:

- **cos table**—Sets the CoS value based on a table map.
- **dscp table**—Sets the code point value based on a table map.
- **precedence table**—Sets the code point value based on a table map.
- **qos-group table**—Sets the CoS value from QoS group based on a table map.
- **wlan user-priority table**—Sets the CoS value from the WLAN user priority based on a table map.

**Example:**

```
Switch(config-pmap)# set cos 5
Switch(config-pmap)#
```

### Step 5

**set dscp**

**(Optional)** Sets the DSCP value.

In addition to setting specific DSCP values, you can also set the following using the `set dscp` command:

- **default**—Matches packets with default DSCP value (000000).

**Example:**

```
```
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config-pmap)# set dscp af11</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-pmap)#</code></td>
<td></td>
</tr>
</tbody>
</table>

- **dscp table**—Sets the packet DSCP value from DSCP based on a table map.
- **ef**—Matches packets with EF DSCP value (101110).
- **precedence table**—Sets the packet DSCP value from precedence based on a table map.
- **qos-group table**—Sets the packet DSCP value from a QoS group based upon a table map.
- **wlan user-priority table**—Sets the packet DSCP value based upon a WLAN user-priority based upon a table map.

### Step 6

**set ip {dscp | precedence}**

**Example:**

```
Switch(config-pmap)# set ip dscp c3
Switch(config-pmap)#
```

(Optional) Sets IP specific values. These values are either IP DSCP or IP precedence values.

You can set the following values using the **set ip dscp** command:

- **dscp value**—Sets a specific DSCP value.
- **default**—Matches packets with default DSCP value (000000).
- **dscp table**—Sets the packet DSCP value from DSCP based on a table map.
- **ef**—Matches packets with EF DSCP value (101110).
- **precedence table**—Sets the packet DSCP value from precedence based on a table map.
- **qos-group table**—Sets the packet DSCP value from a QoS group based upon a table map.
- **wlan user-priority table**—Sets the packet DSCP value based upon a WLAN user-priority based upon a table map.

You can set the following values using the **set ip precedence** command:

- **precedence value**—Sets the precedence value (from 0 to 7).
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• cos table—Sets the packet precedence value from Layer 2 CoS based on a table map.</td>
<td></td>
</tr>
<tr>
<td>• dscp table—Sets the packet precedence from DSCP value based on a table map.</td>
<td></td>
</tr>
<tr>
<td>• precedence table—Sets the precedence value from precedence based on a table map</td>
<td></td>
</tr>
<tr>
<td>• qos-group table—Sets the precedence value from a QoS group based upon a table map.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 7**

```plaintext
set precedence { precedence value | cos table table-map name | dscp table table-map name | precedence table table-map name | qos-group table table-map name}
```

(Optional) Sets precedence values in IPv4 and IPv6 packets.

You can set the following values using the `set precedence` command:

- **precedence value**—Sets the precedence value (from 0 to 7).
- **cos table**—Sets the packet precedence value from Layer 2 CoS on a table map.
- **dscp table**—Sets the packet precedence from DSCP value on a table map.
- **precedence table**—Sets the precedence value from precedence based on a table map.
- **qos-group table**—Sets the precedence value from a QoS group based upon a table map.

**Example:**

```plaintext
Switch(config-pmap)# set precedence 5
Switch(config-pmap)#
```

**Step 8**

```plaintext
set qos-group { qos-group value | dscp table table-map name | precedence table table-map name }
```

(Optional) Sets QoS group values. You can set the following values using this command:

- **qos-group value**—A number from 1 to 31.
- **dscp table**—Sets the code point value from DSCP based on a table map.
- **precedence table**—Sets the code point value from precedence based on a table map.

**Example:**

```plaintext
Switch(config-pmap)# set qos-group 10
Switch(config-pmap)#
```
### Configuring Class Maps for Voice and Video (CLI)

To configure class maps for voice and video traffic, follow these steps:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>class-map class-map-name</code></td>
<td>Creates a class map.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>class-map voice</code></td>
<td></td>
</tr>
</tbody>
</table>

---

*(Optional) Sets the WLAN user priority value. You can set the following values using this command:*

- **wlan user-priority value** — A value between 0 to 7.
- **cos table** — Sets the WLAN user priority value from CoS based on a table map.
- **dscp table** — Sets the WLAN user priority value from DSCP based on a table map.
- **qos-group table** — Sets the WLAN user priority value from QoS group based on a table map.
- **wlan table** — Sets the WLAN user priority value from the WLAN user priority based on a table map.

---

### What to do next

Attach the traffic policy to an interface using the `service-policy` command.

---

*(Optional) Displays policy configuration information for all classes configured for all service policies.*

---

Switch# `show policy-map`
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Matches the DSCP value in the IPv4 and IPv6 packets. Set this value to 46.</td>
</tr>
<tr>
<td><code>match dscp dscp-value-for-voice</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-cmap)# match dscp 46</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures a class map.</td>
</tr>
<tr>
<td><code>class-map class-map-name</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# class-map video</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Matches the DSCP value in the IPv4 and IPv6 packets. Set this value to 34.</td>
</tr>
<tr>
<td><code>match dscp dscp-value-for-video</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-cmap)# match dscp 34</code></td>
<td></td>
</tr>
</tbody>
</table>

### Attaching a Traffic Policy to an Interface (CLI)

After the traffic class and traffic policy are created, you must use the `service-policy` interface configuration command to attach a traffic policy to an interface, and to specify the direction in which the policy should be applied (either on packets coming into the interface or packets leaving the interface).

**Before you begin**

A traffic class and traffic policy must be created before attaching a traffic policy to an interface.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters interface configuration mode and configures an interface.</td>
</tr>
<tr>
<td><code>interface type</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Command parameters for the interface configuration include:</td>
</tr>
<tr>
<td><code>Switch(config)# interface GigabitEthernet1/0/1</code></td>
<td>• Auto Template—Auto-template interface</td>
</tr>
<tr>
<td><code>Switch(config-if)#</code></td>
<td>• Capwap—CAPWAP tunnel interface</td>
</tr>
<tr>
<td></td>
<td>• GigabitEthernet—Gigabit Ethernet IEEE 802</td>
</tr>
<tr>
<td></td>
<td>• GroupVI—Group virtual interface</td>
</tr>
<tr>
<td></td>
<td>• Internal Interface—Internal interface</td>
</tr>
<tr>
<td></td>
<td>• Loopback—Loopback interface</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>• Null — Null interface</td>
<td></td>
</tr>
<tr>
<td>• Port-channel — Ethernet Channel of interface</td>
<td></td>
</tr>
<tr>
<td>• TenGigabitEthernet — 10-Gigabit Ethernet</td>
<td></td>
</tr>
<tr>
<td>• Tunnel — Tunnel interface</td>
<td></td>
</tr>
<tr>
<td>• Vlan — Catalyst VLANs</td>
<td></td>
</tr>
<tr>
<td>• Range — Interface range</td>
<td></td>
</tr>
</tbody>
</table>

### Step 3

```
service-policy {input policy-map | output policy-map }
```

**Example:**

```
Switch(config-if)# service-policy output policy_map_01
Switch(config-if)#
```

Attaches a policy map to an input or output interface. This policy map is then used as the service policy for that interface.

In this example, the traffic policy evaluates all traffic leaving that interface.

### Step 4

```
end
```

**Example:**

```
Switch(config-if)# end
Switch#
```

Saves configuration changes.

### Step 5

```
show policy map
```

**Example:**

```
Switch# show policy map
```

(Optional) Displays statistics for the policy on the specified interface.

### What to do next

Proceed to attach any other traffic policy to an interface, and to specify the direction in which the policy should be applied.

### Related Topics

- Policy Map on Physical Port, on page 609

### Configuring SSID Policies (GUI)

#### Procedure

1. **Step 1** Choose **Configuration > Wireless**.
2. **Step 2** Expand the QoS node by clicking on the left pane and choose **QOS-Policy**.
The Create QoS Policy page is displayed.

**Step 3**

Click Add New to create a new QoS Policy.

The QoS Policy page is displayed.

**Step 4**

Select SSID from the Policy Type drop-down menu.

**Step 5**

Select the direction into which the policy needs to be applied from the Policy Direction drop-down list.

The available options are:

- Ingress
- Egress

**Note**
Voice and video configurations are available only in the egress direction.

**Note**
When creating an egress SSID policy for voice and video classes, if the port_child_policy is already configured with voice and video classes having priority level, the existing port_child_policy is used. If a port_child_policy does not exist with voice and video classes, the switch will create voice and video classes with priority levels 1 and 2 under port_child_policy for voice and video traffic.

**Step 6**
Specify a policy name in the Policy Name text box.

**Step 7**
Provide a description to the policy in the Description text box.

**Step 8**
Select the trust parameter from the Trust drop-down list.

The following options are available:

- DSCP—Assigns a label to indicate the given quality of service as DSCP.
- COS—Matches IEEE 802.1Q class of service. This option is not available when the Policy Direction is ingress.
- User Priority—Enter the 802.11e user priority. This option is not available when the Policy Direction is egress.
- None—This option is available when the Policy Direction is egress. This option is available only for egress policies.

**Step 9**
If you chose Egress policy above, the following options are available:

- Bandwidth—Specifies the bandwidth rate. The following options are available:
  - Rate—Specifies the bandwidth in kbps. Enter a value in kbps in the Value field.
  - Remaining Ratio—Specifies the bandwidth in BRR (bandwidth remaining ratio). Enter the percentage in the Percent field.

**Note**
If you choose the Rate option for the Bandwidth parameter, this value must be greater than the sum of the policings values for voice and video traffic.

- Enable Voice—Check the Enable Voice check box to enable voice traffic on this policy. Specify the following properties:
  - Priority—Sets the priority for this policy for strict scheduling. The priority level is set to 1.
  - Police (kbps)—Specifies the police rate in Kilobits per second.
  - CAC—Enables or disables CAC. If CAC is enabled, you must specify the following options:
• **User priority**—This option is available when the **Policy Direction** is ingress. Enter the 802.11e user priority. The range is from 0 to 7. By default, a value of 6 is assigned.

• **Rate (kbps)**

  **Note**  The CAC rate must be less than the police rate.

• **Enable Video**—Check the **Enable Video** check box to enable video traffic on this policy. Specify the following properties:

• **Priority**—Sets the priority for this policy for strict scheduling.

• **Police (kbps)**—Specifies the police rate in kilobits per second.

**Step 10** Click **Apply**.

---

**Related Topics**

- SSID Policies, on page 598
- Supported QoS Features on Wireless Targets, on page 594
- Examples: SSID Policy
- Examples: Configuring Downstream SSID Policy, on page 697

---

**Applying an SSID or Client Policy on a WLAN (CLI)**

**Before you begin**

You must have a service-policy map configured before applying it on an SSID.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>wlan profile-name</td>
<td>Enters WLAN configuration submode. The profile-name is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# wlan test4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>service-policy [ input</td>
<td>output ] policy-name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-wlan)# service-policy input policy-map-ssid</td>
<td>• input—Assigns the policy map to WLAN ingress traffic.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• output—Assigns the policy map to WLAN egress traffic.</td>
</tr>
</tbody>
</table>
## Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps (CLI)

You can configure a nonhierarchical policy map on a physical port that specifies which traffic class to act on. Actions supported are remarking and policing.

### Before you begin

You should have already decided upon the classification, policing, and marking of your network traffic by policy maps prior to beginning this procedure.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters class map configuration mode.</td>
</tr>
<tr>
<td>class-map [class-map name</td>
<td>match-any ]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# class-map ipclass1</td>
<td></td>
</tr>
<tr>
<td>Switch(config-cmap)# exit</td>
<td></td>
</tr>
<tr>
<td>Switch(config)#</td>
<td></td>
</tr>
<tr>
<td>• Creates a class map to be used for matching packets to the class whose name you specify.</td>
<td></td>
</tr>
<tr>
<td>• If you specify <strong>match-any</strong>, one of the match criteria must be met for traffic entering the traffic class to be classified as part of the traffic class. This is the default.</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 3    | `match access-group { access list index | access list name }` | Specifies the classification criteria to match to the class map. You can match on the following criteria:  
  - `access-group`—Matches to access group.  
  - `class-map`—Matches to another class map.  
  - `cos`—Matches to a CoS value.  
  - `dscp`—Matches to a DSCP value.  
  - `ip`—Matches to a specific IP value.  
  - `non-client-nrt`—Matches non-client NRT.  
  - `precedence`—Matches precedence in IPv4 and IPv6 packets.  
  - `qos-group`—Matches to a QoS group.  
  - `vlan`—Matches to a VLAN. |
| 4    | `policy-map policy-map-name` | Creates a policy map by entering the policy map name, and enters policy-map configuration mode. |
| 5    | `class {class-map-name | class-default}` | Defines a traffic classification, and enter policy-map class configuration mode. |
|      |                  | By default, no policy map class-maps are defined. |
|      |                  | If a traffic class has already been defined by using the `class-map` global configuration command, specify its name for `class-map-name` in this command. A `class-default` traffic class is predefined and can be added to any policy. It is always placed at the end of a policy map. With an implied `match any` included in the `class-default` class, all packets that have not already matched the other traffic classes will match `class-default`. |
| 6    | `set {cos | dscp | ip | precedence | qos-group | wlan user-priority}` | (Optional) Sets the QoS values. Possible QoS configuration values include:  
  - `cos`—Sets the IEEE 802.1Q/ISL class of service/user priority. |
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config-pmap-c)# set dscp 45</code></td>
</tr>
</tbody>
</table>

#### Purpose

- **dscp**—Sets DSCP in IPv4 and IPv6 packets.
- **ip**—Sets IP specific values.
- **precedence**—Sets precedence in IPv4 and IPv6 packet.
- **qos-group**—Sets QoS group.
- **wlan user-priority**—Sets WLAN user priority.

In this example, the `set dscp` command classifies the IP traffic by setting a new DSCP value in the packet.

#### Step 7

**police** `{target_bit_rate | cir | rate}`

**Example:**

```
Switch(config-pmap-c)# police 100000
conform-action transmit exceed-action drop
Switch(config-pmap-c)#
```

(Optional) Configures the policer:

- **target_bit_rate**—Specifies the bit rate per second, enter a value between 8000 and 10000000000.
- **cir**—Committed Information Rate.
- **rate**—Specifies the police rate, PCR for hierarchical policies, or SCR for single-level ATM 4.0 policer policies.

In this example, the `police` command adds a policer to the class where any traffic beyond the 100000 set target bit rate is dropped.

#### Step 8

**exit**

**Example:**

```
Switch(config-pmap-c)# exit
```

Returns to policy map configuration mode.

#### Step 9

**exit**

**Example:**

```
Switch(config-pmap)# exit
```

Returns to global configuration mode.

#### Step 10

**interface** `interface-id`

**Example:**

```
Switch(config)# interface gigabitethernet 2/0/1
```

Specifies the port to attach to the policy map, and enters interface configuration mode.

Valid interfaces include physical ports.
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 11** | Service-policy input *policy-map-name*  
**Example:**  
Switch(config-if)# service-policy input flowit |
| Specifies the policy-map name, and applies it to an ingress port. Only one policy map per ingress port is supported. |
| **Step 12** | End  
**Example:**  
Switch(config-if)# end |
| Returns to privileged EXEC mode. |
| **Step 13** | Show policy-map [policy-map-name [class class-map-name]]  
**Example:**  
Switch# show policy-map |
| (Optional) Verifies your entries. |
| **Step 14** | Copy running-config startup-config  
**Example:**  
Switch# copy-running-config startup-config |
| (Optional) Saves your entries in the configuration file. |

### What to do next

If applicable to your QoS configuration, configure classification, policing, and marking of traffic on SVIs by using policy maps.

### Classifying, Policing, and Marking Traffic on SVIs by Using Policy Maps (CLI)

#### Before you begin

You should have already decided upon the classification, policing, and marking of your network traffic by using policy maps prior to beginning this procedure.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | Configure terminal  
**Example:**  
Switch# configure terminal |
<p>| Enters global configuration mode. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;class-map {class-map name</td>
<td>match-any }&lt;br&gt;Example:&lt;br&gt;Switch(config)# class-map class_vlan100</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;match vlan vlannumber</td>
<td>Specifies the VLAN to match to the class map.</td>
</tr>
<tr>
<td>Example:&lt;br&gt;Switch(config-cmap)# match vlan 100&lt;br&gt;Switch(config-cmap)# exit&lt;br&gt;Switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;policy-map policy-map-name</td>
<td>Creates a policy map by entering the policy map name, and enters policy-map configuration mode.&lt;br&gt;By default, no policy maps are defined.</td>
</tr>
<tr>
<td>Example:&lt;br&gt;Switch(config)# policy-map policy_vlan100&lt;br&gt;Switch(config-pmap)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong>&lt;br&gt;description description</td>
<td>(Optional) Enters a description of the policy map.</td>
</tr>
<tr>
<td>Example:&lt;br&gt;Switch(config-pmap)# description vlan 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong>&lt;br&gt;class {class-map-name</td>
<td>class-default}&lt;br&gt;Example:&lt;br&gt;Switch(config-pmap)# class class_vlan100&lt;br&gt;Switch(config-pmap-c)#</td>
</tr>
</tbody>
</table>
### Classifying, Policing, and Marking Traffic on SVIs by Using Policy Maps (CLI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>set {cos</td>
<td>dscp</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-pmap-c)# set dscp af23</td>
<td>- <strong>cos</strong>—Sets the IEEE 802.1Q/ISL class of service/user priority.</td>
</tr>
<tr>
<td></td>
<td>Switch(config-pmap-c)#</td>
<td>- <strong>dscp</strong>—Sets DSCP in IP(v4) and IPv6 packets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>ip</strong>—Sets IP specific values.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>precedence</strong>—Sets precedence in IP(v4) and IPv6 packet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>qos-group</strong>—Sets QoS group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>wlan user-priority</strong>—Sets WLAN user-priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In this example, the set dscp command classifies the IP traffic by matching the packets with a DSCP value of AF23 (010010).</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>police {target_bit_rate</td>
<td>cir</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-pmap-c)# police 200000 conform-action transmit exceed-action drop</td>
<td>- <strong>target_bit_rate</strong>—Specifies the bit rate per second. Enter a value between 8000 and 10000000000.</td>
</tr>
<tr>
<td></td>
<td>Switch(config-pmap-c)#</td>
<td>- <strong>cir</strong>—Committed Information Rate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>rate</strong>—Specifies the police rate, PCR for hierarchical policies, or SCR for single-level ATM 4.0 policer policies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In this example, the police command adds a policer to the class where any traffic beyond the 200000 set target bit rate is dropped.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>exit</td>
<td>Returns to policy map configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-pmap-c)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-pmap)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>interface interface-id</td>
<td>Specifies the port to attach to the policy map, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Table Maps (CLI)

Table maps are a form of marking, and also enable the mapping and conversion of one field to another using a table. For example, a table map can be used to map and convert a Layer 2 CoS setting to a precedence value in Layer 3.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# interface</code> &lt;br&gt;<code>gigabitethernet 1/0/3</code></td>
<td>Valid interfaces include physical ports.</td>
</tr>
<tr>
<td><strong>Step 12</strong>  &lt;br&gt;<code>service-policy input policy-map-name</code> &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Switch(config-if)# service-policy input policy_vlan100</code></td>
<td>Specifies the policy-map name, and applies it to an ingress port. Only one policy map per ingress port is supported.</td>
</tr>
<tr>
<td><strong>Step 13</strong>  &lt;br&gt;<code>end</code> &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Switch(config-if)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 14</strong>  &lt;br&gt;<code>show policy-map [policy-map-name [class class-map-name]]</code> &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Switch# show policy-map</code></td>
<td>(Optional) Verifies your entries.</td>
</tr>
<tr>
<td><strong>Step 15</strong>  &lt;br&gt;<code>copy running-config startup-config</code> &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Switch# copy-running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Policy Map on VLANs, on page 609
- Examples: Policer VLAN Configuration, on page 704

**Note**

A table map can be referenced in multiple policies or multiple times in the same policy.
### Configuring Table Maps (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`table-map name {default {default value</td>
<td>copy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>table-map table01</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-tablemap)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>map from value to value</code></td>
<td>In this step, packets with DSCP values 0 are marked to the CoS value 2, DSCP value 1 to the CoS value 4, DSCP value 24 to the CoS value 3, DSCP value 40 to the CoS value 6 and all others to the CoS value 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-tablemap)# <code>map from 0 to 2</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-tablemap)# <code>map from 1 to 4</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-tablemap)# <code>map from 24 to 3</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-tablemap)# <code>map from 40 to 6</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-tablemap)# <code>default 0</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-tablemap)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>exit</code></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-tablemap)# <code>exit</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>exit</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config) <code>exit</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
---|---
Switch# |  

**Step 6**  
**show table-map**  
Example:  
Switch# **show table-map**  
Table Map table01  
from 0 to 2  
from 1 to 4  
from 24 to 3  
from 40 to 6  
default 0  
Displays the table map configuration.

**Step 7**  
**configure terminal**  
Example:  
Switch# **configure terminal**  
Switch(config)#  
Enters global configuration mode.

**Step 8**  
**policy-map**  
Example:  
Switch(config)# **policy-map table-policy**  
Switch(config-pmap)#  
Configures the policy map for the table map.

**Step 9**  
**class class-default**  
Example:  
Switch(config-pmap)# **class class-default**  
Switch(config-pmap-c)#  
Matches the class to the system default.

**Step 10**  
**set cos dscp table table map name**  
Example:  
Switch(config-pmap-c)# **set cos dscp table table01**  
Switch(config-pmap-c)#  
If this policy is applied on input port, that port will have trust DSCP enabled on that port and marking will take place depending upon the specified table map.

**Step 11**  
**end**  
Example:  
Switch(config-pmap-c)# **end**  
Switch#  
Returns to privileged EXEC mode.
What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the `service-policy` command.

Related Topics
- Table Map Marking, on page 612
- Examples: Table Map Marking Configuration, on page 706

Configuring Trust

Configuring Trust Behavior for Wireless Traffic (CLI)

The Cisco IOS XE 3.2 Release supported different trust defaults for wired and wireless ports. The trust default for wired ports was the same as for this software release. For wireless ports, the default system behavior was non-trust, which meant that when the switch came up, all markings for the wireless ports were defaulted to zero and no traffic received priority treatment. For compatibility with an existing wired switch, all traffic went to the best-effort queue by default. The access point performed priority queuing by default. In the downstream direction, the access point maintained voice, video, best-effort, and background queues for queuing. The access selected the queuing strategy based on the 11e tag information. By default, the access point treated all wireless packets as best effort.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | Configures the behavior of the switch to untrust wireless traffic. To configure the switch to trust wireless traffic by default, use the `no` form of the command. |
| `qos wireless-default-untrust` | |
| **Example:** | |
| Switch (config)# `qos wireless-default-untrust` | |

| **Step 3** | Returns to privileged EXEC mode. Alternatively, you can also press `Ctrl-Z` to exit global configuration mode. |
| `end` | |
| **Example:** | |
| Switch(config)# `end` | |

Related Topics
- Trust Behavior for Wired and Wireless Ports, on page 621

Configuring QoS Features and Functionality

Configuring Call Admission Control (CLI)

This task explains how to configure class-based, unconditional packet marking features on your switch for Call Admission Control (CAC).
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> class-map class name</td>
<td>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# class-map voice Switch(config-cmap)#</td>
<td>• word — Class map name.</td>
</tr>
<tr>
<td></td>
<td>• class-default — System default class matching any otherwise unclassified packets.</td>
</tr>
<tr>
<td><strong>Step 3</strong> match dscp dscp value</td>
<td>(Optional) Matches the DSCP values in IPv4 and IPv6 packets.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-cmap)# match dscp 46</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-cmap)# exit Switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> class-map class name</td>
<td>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# class-map video Switch(config-cmap)#</td>
<td>• word — Class map name.</td>
</tr>
<tr>
<td></td>
<td>• class-default — System default class matching any otherwise unclassified packets.</td>
</tr>
<tr>
<td><strong>Step 6</strong> match dscp dscp value</td>
<td>(Optional) Matches the DSCP values in IPv4 and IPv6 packets.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-cmap)# match dscp 34</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Call Admission Control (CLI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 7** | **exit**  
Example:  
Switch(config-cmap)# exit  
Switch(config)# | Returns to global configuration mode. |
| **Step 8** | **table-map name**  
Example:  
Switch(config)# table-map dscp2dscp  
Switch(config-tablemap)# | Creates a table map and enters the table map configuration mode. |
| **Step 9** | **default copy**  
Example:  
Switch(config-tablemap)# default copy | Sets the default behavior for value not found in the table map to copy.  
**Note**: This is the default option. You can also do a mapping of values for DSCP to DSCP. |
| **Step 10** | **exit**  
Example:  
Switch(config-tablemap)# exit  
Switch(config)# | Returns to global configuration mode. |
| **Step 11** | **table-map name**  
Example:  
Switch(config)# table-map dscp2up  
Switch(config-tablemap)# | Creates a new table map and enters the table map configuration mode. |
| **Step 12** | **default copy**  
Example:  
Switch(config-tablemap)# default copy | Sets the default behavior for value not found in the table map to copy.  
**Note**: This is the default option. You can also do a mapping of values for DSCP to UP. |
| **Step 13** | **exit**  
Example:  
Switch(config-tablemap)# exit  
Switch(config)# | Returns to global configuration mode. |
<p>| <strong>Step 14</strong> | <strong>policy-map policy name</strong> | Enters policy map configuration mode. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)#</td>
<td></td>
</tr>
<tr>
<td>policy-map</td>
<td>Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.</td>
</tr>
<tr>
<td>ssid_child_cac</td>
<td></td>
</tr>
<tr>
<td>Switch(config-pmap)#</td>
<td></td>
</tr>
</tbody>
</table>

**Step 15**

<table>
<thead>
<tr>
<th>class class-map-name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Switch(config-pmap)#</td>
</tr>
</tbody>
</table>

**Step 16**

<table>
<thead>
<tr>
<th>priority level level_value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Switch(config-pmap-c)#</td>
</tr>
</tbody>
</table>

**Step 17**

<table>
<thead>
<tr>
<th>police [target_bit_rate</th>
<th>cir</th>
<th>rate ]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-pmap-c)#</td>
<td>police cir 10m</td>
<td></td>
</tr>
</tbody>
</table>

(Optional) Configures the policer:
- **target_bit_rate**—Specifies the bit rate per second. Enter a value between 8000 and 10000000000.
- **cir**—Committed Information Rate.
- **rate**—Specifies the police rate, PCR for hierarchical policies, or SCR for single-level ATM 4.0 policer policies.

**Step 18**

<table>
<thead>
<tr>
<th>admit cac wmm-tspec</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Switch(config-pmap-c)# admit cac wmm-tspec</td>
</tr>
</tbody>
</table>

Configures call admission control for the policy map.

**Note** This command only configures CAC for wireless QoS.

**Step 19**

<table>
<thead>
<tr>
<th>rate value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Switch(config-pmap-admit-cac-wmm)# rate 5000</td>
</tr>
</tbody>
</table>

Configures the target bit rate (Kilo Bits per second). Enter a value from 8 to 10000000.

**Step 20**

<table>
<thead>
<tr>
<th>wlan-up value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Configures the WLAN UP value. Enter a value from 0 to 7.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config-pmap-admit-cac-wmm)# wlan-up 6 7</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 21</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Returns to policy map class configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-pmap-admit-cac-wmm)# exit</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-pmap-c)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 22</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Returns to policy map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-pmap-c)# exit</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-pmap)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 23</strong></td>
<td></td>
</tr>
<tr>
<td><code>class class name</code></td>
<td>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-pmap)# class video</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-pmap-c)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 24</strong></td>
<td></td>
</tr>
<tr>
<td><code>priority level level_value</code></td>
<td>The <code>priority</code> command assigns a strict scheduling priority for the class.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-pmap-c)# priority level 2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Priority level 1 is more important than priority level 2. Priority level 1 reserves bandwidth that is processed first for QoS, so its latency is very low. Both priority level 1 and 2 reserve bandwidth.</td>
</tr>
<tr>
<td><strong>Step 25</strong></td>
<td></td>
</tr>
<tr>
<td>`police [target_bit_rate</td>
<td>cir</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-pmap-c)# police cir 20m</code></td>
<td></td>
</tr>
<tr>
<td><code>• target_bit_rate—Specifies the bit rate per second. Enter a value between 8000 and 10000000000.</code></td>
<td></td>
</tr>
<tr>
<td><code>• cir—Committed Information Rate.</code></td>
<td></td>
</tr>
<tr>
<td><code>• rate—Specifies the police rate, PCR for hierarchical policies, or SCR for single-level ATM 4.0 policer policies.</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 26</strong> admit cac wmm-tspec</td>
<td>Configures call admission control for the policy map.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>[Switch(config-pmap-c)# admit cac wmm-tspec]</td>
<td></td>
</tr>
<tr>
<td>[Switch(config-pmap-admit-cac-wmm)#]</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This command only configures CAC for wireless QoS.</td>
</tr>
<tr>
<td><strong>Step 27</strong> rate value</td>
<td>Configures the target bit rate (Kilo Bits per second). Enter a value from 8 to 1000000.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>[Switch(config-pmap-admit-cac-wmm)# rate 5000]</td>
<td></td>
</tr>
<tr>
<td><strong>Step 28</strong> wlan-up value</td>
<td>Configures the WLAN UP value. Enter a value from 0 to 7.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>[Switch(config-pmap-admit-cac-wmm)# wlan-up 4 5]</td>
<td></td>
</tr>
<tr>
<td><strong>Step 29</strong> exit</td>
<td>Returns to policy map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>[Switch(config-pmap-cac-wmm)# exit]</td>
<td></td>
</tr>
<tr>
<td>[Switch(config-pmap)#]</td>
<td></td>
</tr>
<tr>
<td><strong>Step 30</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>[Switch(config-pmap)# exit]</td>
<td></td>
</tr>
<tr>
<td>[Switch(config)#]</td>
<td></td>
</tr>
<tr>
<td><strong>Step 31</strong> policy-map policy name</td>
<td>Enters policy map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>[Switch(config)# policy-map ssid_cac]</td>
<td></td>
</tr>
<tr>
<td>[Switch(config-pmap)#]</td>
<td></td>
</tr>
<tr>
<td>Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 32</strong> class class-map-name</td>
<td>Defines an interface-level traffic classification, and enters policy-map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>[Switch(config-pmap)# class default]</td>
<td></td>
</tr>
<tr>
<td>In this example, the class map is set to default.</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
</tr>
<tr>
<td>33</td>
<td><code>set dscp dscp table table_map_name</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-pmap-c)# set dscp dscp table dscp2dscp</code></td>
</tr>
<tr>
<td>34</td>
<td><code>set wlan user-priority dscp table table_map_name</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-pmap-c)# set wlan user-priority dscp table dscp2up</code></td>
</tr>
<tr>
<td>35</td>
<td>`shape average {target bit rate</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-pmap-c)# shape average 100000000</code></td>
</tr>
<tr>
<td>36</td>
<td><code>queue-buffers {ratio ratio value}</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-pmap-c)# queue-buffers ratio 0</code></td>
</tr>
<tr>
<td>37</td>
<td><code>service-policy policy_map_name</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-pmap-c)# service-policy ssid_child_cac</code></td>
</tr>
</tbody>
</table>
## Configuring Bandwidth (CLI)

This procedure explains how to configure bandwidth on your switch.

### Before you begin

You should have created a class map for bandwidth before beginning this procedure.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>policy-map policy name</td>
<td>Enters policy map configuration mode. Creates or modifies a policy map</td>
</tr>
<tr>
<td>Example:</td>
<td>that can be attached to one or more interfaces to specify a service</td>
</tr>
<tr>
<td>Switch(config)# policy-map</td>
<td>policy.</td>
</tr>
<tr>
<td>policy_bandwidth01</td>
<td></td>
</tr>
<tr>
<td>Switch(config-pmap)#</td>
<td></td>
</tr>
</tbody>
</table>

---

### What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the `service-policy` command.

For additional information about CAC, refer to the System Management Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches).

For additional information about CAC, refer to the System Management Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series).
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>class class name</code></td>
<td>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-pmap)# class class_bandwidth01</code></td>
<td>• <code>word</code>—Class map name.</td>
</tr>
<tr>
<td><code>Switch(config-pmap-c)#</code></td>
<td>• <code>class-default</code>—System default class matching any otherwise unclassified packets.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>`bandwidth {Kb/s</td>
<td>percent percentage</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-pmap-c)# bandwidth 200000</code></td>
<td>• <code>Kb/s</code>—Configures a specific value in kilobits per second (from 20000 to 10000000).</td>
</tr>
<tr>
<td><code>Switch(config-pmap-c)#</code></td>
<td>• <code>percent</code>—Allocates minimum bandwidth to a particular class based on a percentage. The queue can oversubscribe bandwidth in case other queues do not utilize the entire port bandwidth. The total sum cannot exceed 100 percent, and in case it is less than 100 percent, the rest of the bandwidth is equally divided along all bandwidth queues.</td>
</tr>
<tr>
<td></td>
<td>• <code>remaining</code>—Allocates minimum bandwidth to a particular class. The queue can oversubscribe bandwidth in case other queues do not utilize entire port bandwidth. The total sum cannot exceed 100 percent. It is preferred to use this command when the <code>priority</code> command is used for certain queues in the policy. You can also assign ratios rather than percentages to each queue; the queues will be assigned certain weights which are inline with these ratios. Ratios can range from 0 to 100. Total bandwidth ratio allocation for the policy in this case can exceed 100.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You cannot mix bandwidth types on a policy map. For example, you cannot configure bandwidth in a single policy map using both a bandwidth percent and in kilobits per second.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

**Step 5**  
End  
Example:  
Switch(config-pmap-c)# end  
Switch#

**Purpose**

Saves configuration changes.

**Step 6**

Show policy-map  
Example:  
Switch# show policy-map

(Optional) Displays policy configuration information for all classes configured for all service policies.

### What to do next

Configure any additional policy maps for QoS for your network. After creating the policy maps, attach the traffic policy or polices to an interface using the `service-policy` command.

### Related Topics

- Bandwidth, on page 617

### Configuring Police (CLI)

This procedure explains how to configure policing on your switch.

### Before you begin

You should have created a class map for policing before beginning this procedure.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**        | configure terminal  
Example:  
Switch# configure terminal | Enters global configuration mode. |
| **Step 2**        | policy-map policy name  
Example:  
Switch(config)# policy-map policy_police01  
Switch(config-pmap)# | Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **Step 3**        | class class name  
Example: | Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options |
### Command or Action

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Switch(config-pmap)# **class class_police01**  
Switch(config-pmap-c)# | for policy class map configuration mode include the following:  
- **word**—Class map name.  
- **class-default**—System default class matching any otherwise unclassified packets. |

#### Step 4

| **police** {**target_bit_rate** [**burst bytes** | **bc** | **conform-action** | **pir** ] | **cir** {**target_bit_rate** | **percent** percentage} | **rate** {**target_bit_rate** | **percent** percentage} | **conform-action transmit exceed-action** {**drop** [**violate action**] | **set-cos-transmit** | **set-dscp-transmit** | **set-prec-transmit** | **transmit** [**violate action**] } | The following **police** subcommand options are available:  
- **target_bit_rate**—Bits per second (from 8000 to 10000000000).  
  - **burst bytes**—Enter a value from 1000 to 512000000.  
  - **bc**—Conform burst.  
  - **conform-action**—Action taken when rate is less than conform burst.  
  - **pir**—Peak Information Rate.  
- **cir**—Committed Information Rate.  
  - **target_bit_rate**—Target bit rate (8000 to 10000000000).  
  - **percent**—Percentage of interface bandwidth for CIR.  
- **rate**— Specifies the police rate, PCR for hierarchical policies, or SCR for single-level ATM 4.0 policer policies.  
  - **target_bit_rate**—Target Bit Rate (8000 to 10000000000).  
  - **percent**—Percentage of interface bandwidth for rate.  

**Example:**

Switch(config-pmap-c)# **police 8000 conform-action transmit exceed-action drop**  
Switch(config-pmap-c)# | **transmit** [**violate action**] } |

The following **police conform-action transmit exceed-action** subcommand options are available:  
- **drop**—Drops the packet.  
- **set-cos-transmit**—Sets the CoS value and sends it.  
- **set-dscp-transmit**—Sets the DSCP value and sends it. |
**Purpose**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• set-prec-transmit</td>
<td>Rewrites the packet precedence and sends it.</td>
</tr>
<tr>
<td>• transmit</td>
<td>Transmits the packet.</td>
</tr>
</tbody>
</table>

**Note**

Policer-based markdown actions are only supported using table maps. Only one markdown table map is allowed for each marking field in the switch.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>end</th>
<th>Saves configuration changes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config-pmap-c)# end Switch#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>show policy-map</th>
<th>(Optional) Displays policy configuration information for all classes configured for all service policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch# show policy-map</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the `service-policy` command.

**Related Topics**

- Single-Rate Two-Color Policing, on page 614
- Examples: Single-Rate Two-Color Policing Configuration, on page 705
- Dual-Rate Three-Color Policing, on page 615
- Examples: Dual-Rate Three-Color Policing Configuration, on page 705
- Policing, on page 610
- Token-Bucket Algorithm, on page 611
- Examples: Policing Action Configuration, on page 703
- Examples: Policing Units, on page 704

**Configuring Priority (CLI)**

This procedure explains how to configure priority on your switch.

The switch supports giving priority to specified queues. There are two priority levels available (1 and 2).

**Note**

Queues supporting voice and video should be assigned a priority level of 1.
Before you begin

You should have created a class map for priority before beginning this procedure.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> policy-map policy_name</td>
<td>Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# policy-map policy_priority01</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> class class_name</td>
<td>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-pmap)# class class_priority01</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Switch(config-pmap-c)# priority level 1</td>
<td>(Optional) The priority command assigns a strict scheduling priority for the class. The command options include:</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-pmap-c)# priority level 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- *Kb/s*—Specifies the kilobits per second (from 1 to 2000000).
- *burst_in_bytes*—Specifies the burst in bytes (from 32 to 2000000).
- *level level_value*—Specifies the multilevel (1-2) priority queue.
- *Kb/s*—Specifies the kilobits per second (from 1 to 2000000).
- *burst_in_bytes*—Specifies the burst in bytes (from 32 to 2000000).
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>percent</strong>—Percentage of the total bandwidth.</td>
</tr>
<tr>
<td></td>
<td>• <strong>burst_in_bytes</strong>—Specifies the burst in bytes (from 32 to 2000000).</td>
</tr>
<tr>
<td></td>
<td>• <strong>percent</strong>—Percentage of the total bandwidth.</td>
</tr>
<tr>
<td></td>
<td>• <strong>burst_in_bytes</strong>—Specifies the burst in bytes (32 to 2000000).</td>
</tr>
</tbody>
</table>

**Note**  
Priority level 1 is more important than priority level 2. Priority level 1 reserves bandwidth that is processed first for QoS, so its latency is very low. Both priority level 1 and 2 reserve bandwidth.

**Step 5**  
**Example:**

```
Switch(config-pmap-c)# end
Switch#
```

Saves configuration changes.

**Step 6**  
**Example:**

```
Switch# show policy-map
```

(Optional) Displays policy configuration information for all classes configured for all service policies.

**What to do next**  
Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the `service-policy` command.

**Related Topics**  
[Priority Queues](#), on page 619

---

**Configuring Queues and Shaping**

**Configuring Egress Queue Characteristics**

Depending on the complexity of your network and your QoS solution, you may need to perform all of the procedures in this section. You need to make decisions about these characteristics:

- Which packets are mapped by DSCP, CoS, or QoS group value to each queue and threshold ID?
• What drop percentage thresholds apply to the queues, and how much reserved and maximum memory is needed for the traffic type?
• How much of the fixed buffer space is allocated to the queues?
• Does the bandwidth of the port need to be rate limited?
• How often should the egress queues be serviced and which technique (shaped, shared, or both) should be used?

Note You can only configure the egress queues on the switch.

Configuring Queue Buffers (CLI)
The switch allows you to allocate buffers to queues. If there is no allocation made to buffers, then they are divided equally for all queues. You can use the queue-buffer ratio to divide it in a particular ratio. Since by default DTS (Dynamic Threshold and Scaling) is active on all queues, these are soft buffers.

Note The queue-buffer ratio is supported on both wired and wireless ports, but the queue-buffer ratio cannot be configured with a queue-limit.

Before you begin
The following are prerequisites for this procedure:
• You should have created a class map for the queue buffer before beginning this procedure.
• You must have configured either bandwidth, shape, or priority on the policy map prior to configuring the queue buffers.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Example:
  Switch# configure terminal | |
| **Step 2** policy-map policy name | Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| Example:
  Switch(config)# policy-map policy_queuebuffer01
  Switch(config-pmap)# | |
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td><code>class class name</code></td>
<td>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-pmap)# class class_queuebuffer01 Switch(config-pmap-c)#</code></td>
<td><em>word</em>—Class map name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>class-default</em>—System default class matching any otherwise unclassified packets.</td>
</tr>
<tr>
<td>Step 4</td>
<td>`bandwidth {Kb/s</td>
<td>percent percentage</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-pmap-c)# bandwidth percent 80 Switch(config-pmap-c)#</code></td>
<td><em>Kb/s</em>—Use this command to configure a specific value. The range is 20000 to 10000000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>percent</em>—Allocates a minimum bandwidth to a particular class using a percentage. The queue can oversubscribe bandwidth in case other queues do not utilize the entire port bandwidth. The total sum cannot exceed 100 percent, and in case it is less than 100 percent, the rest of the bandwidth is equally divided along all bandwidth queues.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>remaining</em>—Allocates a minimum bandwidth to a particular class. The queue can oversubscribe bandwidth in case other queues do not utilize entire port bandwidth. The total sum cannot exceed 100 percent. It is preferred to use this command when the <code>priority</code> command is used for certain queues in the policy. You can also assign ratios rather than a percentage to each queue; the queues will be assigned certain weights that are inline with these ratios. Ratios can range from 0 to 100. Total bandwidth ratio allocation for the policy in this case can exceed 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note You cannot mix bandwidth types on a policy map.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>queue-buffers {ratio ratio value}</code></td>
<td>Configures the relative buffer size for the queue.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Queue Limits (CLI)

You use queue limits to configure Weighted Tail Drop (WTD). WTD ensures the configuration of more than one threshold per queue. Each class of service is dropped at a different threshold value to provide for QoS differentiation. With the switch, each queue has 3 explicit programmable threshold classes—0, 1, 2. Therefore, the enqueue/drop decision of each packet per queue is determined by the packet’s threshold class assignment, which is determined by the DSCP, CoS, or QoS group field of the frame header.

WTD also uses a soft limit, and therefore you are allowed to configure the queue limit to up to 400 percent (maximum four times the reserved buffer from common pool). This soft limit prevents overrunning the common pool without impacting other features.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config-pmap-c)# queue-buffers ratio 10</code></td>
<td>Note: The sum of all configured buffers in a policy must be less than or equal to 100 percent. Unallocated buffers are evenly distributed to all the remaining queues. Ensure sufficient buffers are allocated to all queues including the priority queues.</td>
</tr>
<tr>
<td><code>Switch(config-pmap-c)#</code></td>
<td>Note: Protocol Data Units (PDUs) for network control protocols such as spanning-tree and LACP utilize the priority queue or queue 0 (when a priority queue is not configured). Ensure sufficient buffers are allocated to these queues for the protocols to function.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td><code>Switch(config-pmap-c)# end</code></td>
<td><code>Switch#</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>show policy-map</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>(Optional) Displays policy configuration information for all classes configured for all service policies.</td>
</tr>
<tr>
<td><code>Switch# show policy-map</code></td>
<td></td>
</tr>
</tbody>
</table>

### What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the `service-policy` command.

**Related Topics**

- Queue Buffer Allocation, on page 620
- Examples: Queue Buffers Configuration, on page 703
You can only configure queue limits on the switch egress queues on wired ports.

### Before you begin

The following are prerequisites for this procedure:

- You should have created a class map for the queue limits before beginning this procedure.
- You must have configured either bandwidth, shape, or priority on the policy map prior to configuring the queue limits.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>policy-map policy name</td>
<td>Enters policy map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# policy-map policy_queuelimit01</td>
<td>Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>class class name</td>
<td>Enters policy class map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-pmap)# class class_queuelimit01</td>
<td>Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-pmap-c)#</td>
<td>- word—Class map name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- class-default—System default class matching any otherwise unclassified packets.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>bandwidth {Kb/s</td>
<td>percent percentage</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-pmap-c)# bandwidth 500000</td>
<td>The parameters include:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-pmap-c)#</td>
<td>- Kb/s—Use this command to configure a specific value. The range is 20000 to 10000000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- percent—Allocates a minimum bandwidth to a particular class. The queue can oversubscribe bandwidth in case other</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>queues do not utilize the entire port bandwidth. The total sum cannot exceed 100 percent, and in case it is less than 100 percent, the rest of the bandwidth is equally divided along all bandwidth queues.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• remaining — Allocates a minimum bandwidth to a particular class. The queue can oversubscribe bandwidth in case other queues do not utilize entire port bandwidth. The total sum cannot exceed 100 percent. It is preferred to use this command when the priority command is used for certain queues in the policy. You can also assign ratios rather than a percentage to each queue; the queues will be assigned certain weights that are inline with these ratios. Ratios can range from 0 to 100. Total bandwidth ratio allocation for the policy in this case can exceed 100.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>You cannot mix bandwidth types on a policy map.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 5

```plaintext
queue-limit {packets packets | cos {cos value {maximum threshold value | percent percentage } | values {cos value | percent percentage } } | dscp {dscp value {maximum threshold value | percent percentage } | match packet {maximum threshold value | percent percentage } | default {maximum threshold value | percent percentage } | ef {maximum threshold value | percent percentage } | dscp values dscp value} | percent percentage }
```

**Example:**

| Switch (config-pmap-c)# queue-limit dscp 3 percent 20 |
| Switch (config-pmap-c)# queue-limit dscp 4 percent 30 |
| Switch (config-pmap-c)# queue-limit dscp 5 percent 40 |

Sets the queue limit threshold percentage values. With every queue, there are three thresholds (0, 1, 2), and there are default values for each of these thresholds. Use this command to change the default or any other queue limit threshold setting. For example, if DSCP 3, 4, and 5 packets are being sent into a specific queue in a configuration, then you can use this command to set the threshold percentages for these three DSCP values. For additional information about queue limit threshold values, see Weighted Tail Drop, on page 618.

**Note** The switch does not support absolute queue-limit percentages. The switch only supports DSCP or CoS queue-limit percentages.

### Step 6

```plaintext
end
```

**Example:**

| Switch (config-pmap-c)# end |

Saves configuration changes.
Configuring Shaping (CLI)

You use the `shape` command to configure shaping (maximum bandwidth) for a particular class. The queue's bandwidth is restricted to this value even though the port has additional bandwidth left. You can configure shaping as an average percent, as well as a shape average value in bits per second.

Before you begin

You should have created a class map for shaping before beginning this procedure.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>policy-map policy name</code></td>
<td>Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# <code>policy-map policy_shaping01</code> Switch(config-pmap)#</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>class class name</code></td>
<td>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-pmap)# <code>class class_shaping01</code> Switch(config-pmap-c)#</td>
<td><code>\* word</code>—Class map name.</td>
</tr>
</tbody>
</table>
Configuring Precious Metal Policies (CLI)

You can configure precious metal QoS policies on a per-WLAN basis.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global command mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>shape average</strong> <em>target bit rate</em></td>
<td>Configures the average shape rate. You can configure the average shape rate by target bit rates (bits per second) or by percentage of interface bandwidth for the Committed Information Rate (CIR).</td>
</tr>
</tbody>
</table>

**Note** For the egress class-default SSID policy, you must configure the queue buffer ratio as 0 after you configure the average shape rate.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>end</strong></td>
<td>Saves configuration changes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show policy-map</strong></td>
<td>(Optional) Displays policy configuration information for all classes configured for all service policies.</td>
</tr>
</tbody>
</table>

### Related Topics

- Average Rate Shaping, on page 616
- Examples: Average Rate Shaping Configuration, on page 701
- Hierarchical Shaping, on page 616
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>wlan wlan-name</code></td>
<td>Enters the WLAN configuration submode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# wlan test4</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`service-policy {input</td>
<td>output} policy-name`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-wlan)# service-policy output platinum</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-wlan)# service-policy input platinum-up</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Upstream policies differ from downstream policies. The upstream policies have a suffix of <code>-up</code>.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>`show wlan {wlan-id</td>
<td>wlan-name}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show wlan name qos-wlan</code></td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

*Precious Metal Policies for Wireless QoS*, on page 624

## Configuring QoS Policies for Multicast Traffic (CLI)

### Before you begin

The following are the prerequisites for configuring a QoS policy for multicast traffic:

- You must have a multicast service policy configured.
- You must enable multicast-multicast mode before applying the policy.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>ap capwap multicast service-policy output service-policy-name</code></td>
<td>Applies the configured multicast policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)#ap capwap multicast service-policy output service-policy-mcast</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- [Wireless QoS Multicast](#), on page 610
- Examples: [Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic](#), on page 696

### Configuring Port Policies (GUI)

**Procedure**

- **Step 1** Choose **Configuration > Wireless**
- **Step 2** Expand the QoS node by clicking on left pane and choose **QOS-Policy**.
  The QOS-Policy page is displayed.
- **Step 3** Click **Add New** to create a new QoS policy.
  The **Create QoS Policy** page is displayed.
- **Step 4** Select **Port** from the **Policy Type** drop-down menu.
- **Step 5** Enter the policy name in the **Policy Name** text field.
- **Step 6** Specify a description for the policy you want to create in the **Description** field.
- **Step 7** Configure the voice or video priorities for the port policies by enabling the Enable Voice and Enable Video parameters.

**Note** You must attach the port policy to an interface. Default values are recommended.
Step 8
Click Add to add the policy.

What to do next
Proceed to assign the port policy on an interface.

Related Topics
- Port Policies, on page 596
- Port Policy Format, on page 596
- Restrictions for QoS on Wireless Targets, on page 632
- Supported QoS Features on Wireless Targets, on page 594
- Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696

Applying or Changing Port Policies (GUI)

Procedure

Step 1
Choose Configuration > Controller > System > Interfaces > Port Summary.
The Port Configuration page is displayed.

Step 2
Select the interface on which you want to configure the port policy from the Interface Name column.

Step 3
Apply or change the QoS Port Policy by selecting the policy from the Assign Policy drop-down list.
The Existing Policy field displays the current policy assigned.

Note All interfaces in a channel group must be assigned to the same port policy.

Step 4
Click Apply.

Related Topics
- Port Policies, on page 596
- Port Policy Format, on page 596
- Restrictions for QoS on Wireless Targets, on page 632
- Supported QoS Features on Wireless Targets, on page 594
- Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696

Applying a QoS Policy on a WLAN (GUI)

Procedure

Step 1
Choose Configuration > Wireless.

Step 2
Expand the WLAN node by clicking on the left pane and choose WLANs.
The WLANs page is displayed.
Step 3  Select the WLAN for which you want to configure the QoS policies by clicking on the WLAN Profile.

Step 4  Click the QoS tab to configure the QoS policies on the WLAN.

You can also configure precious metal policies for the WLAN.

The following options are available:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>QoS SSID Policy</strong></td>
<td></td>
</tr>
<tr>
<td>Egress Policy</td>
<td>QoS downstream policy configuration.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Existing Policy</strong> column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the <strong>Assign Policy</strong> column.</td>
</tr>
<tr>
<td></td>
<td>If a policy is not selected, NONE is displayed.</td>
</tr>
<tr>
<td>Ingress Policy</td>
<td>QoS upstream policy configuration.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Existing Policy</strong> column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the <strong>Assign Policy</strong> column.</td>
</tr>
<tr>
<td></td>
<td>If a policy is not selected, NONE is displayed.</td>
</tr>
<tr>
<td><strong>QoS Client Policy</strong></td>
<td></td>
</tr>
<tr>
<td>Egress Policy</td>
<td>QoS downstream policy configuration.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Existing Policy</strong> column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the <strong>Assign Policy</strong> column.</td>
</tr>
<tr>
<td></td>
<td>If a policy is not selected, NONE is displayed.</td>
</tr>
<tr>
<td>Ingress Policy</td>
<td>QoS upstream policy configuration.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Existing Policy</strong> column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the <strong>Assign Policy</strong> column.</td>
</tr>
<tr>
<td></td>
<td>If a policy is not selected, NONE is displayed.</td>
</tr>
<tr>
<td><strong>WMM</strong></td>
<td></td>
</tr>
<tr>
<td>WMM Policy</td>
<td>WMM Policy. This parameter has the following values:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—Disables this WMM policy.</td>
</tr>
<tr>
<td></td>
<td>• Allowed—Allows the clients to communicate with the WLAN.</td>
</tr>
<tr>
<td></td>
<td>• Require—Ensures that it is mandatory for the clients to have WMM features enabled on them to communicate with the WLAN.</td>
</tr>
</tbody>
</table>

Step 5  Click **Apply**.

Related Topics

- Port Policies, on page 596
- Port Policy Format, on page 596
- Restrictions for QoS on Wireless Targets, on page 632
Monitoring QoS

The following commands can be used to monitor QoS on the switch.

### Table 46: Monitoring QoS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show class-map [class_map_name]</code></td>
<td>Displays a list of all class maps configured.</td>
</tr>
<tr>
<td>`show class-map type control subscriber {all</td>
<td>name }`</td>
</tr>
</tbody>
</table>
| `show class-map type control subscriber detail` | - all—Displays information for all class maps.  
- name—Displays configured class maps. |
| `show policy-map [policy_map_name]` | Displays a list of all policy maps configured. Command parameters include: |
| | - policy map name  
- interface  
- session |
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show policy-map interface { Auto-template</td>
<td>Capwap</td>
</tr>
<tr>
<td>• <code>Auto-template</code>—Auto-Template interface</td>
<td></td>
</tr>
<tr>
<td>• <code>Capwap</code>—CAPWAP tunnel interface</td>
<td></td>
</tr>
<tr>
<td>• <code>GigabitEthernet</code>—Gigabit Ethernet IEEE.802.3z</td>
<td></td>
</tr>
<tr>
<td>• <code>GroupVI</code>—Group virtual interface</td>
<td></td>
</tr>
<tr>
<td>• <code>InternalInterface</code>—Internal interface</td>
<td></td>
</tr>
<tr>
<td>• <code>Loopback</code>—Loopback interface</td>
<td></td>
</tr>
<tr>
<td>• <code>Null</code>—Null interface</td>
<td></td>
</tr>
<tr>
<td>• <code>Lspvif</code>—LSP virtual interface</td>
<td></td>
</tr>
<tr>
<td>• <code>Port-channel</code>—Ethernet channel of interfaces</td>
<td></td>
</tr>
<tr>
<td>• <code>TenGigabitEthernet</code>—10-Gigabit Ethernet</td>
<td></td>
</tr>
<tr>
<td>• <code>Tunnel</code>—Tunnel interface</td>
<td></td>
</tr>
<tr>
<td>• <code>Vlan</code>—Catalyst VLANs</td>
<td></td>
</tr>
<tr>
<td>• <code>brief</code>—Brief description of policy maps</td>
<td></td>
</tr>
<tr>
<td>• <code>class</code>—Statistics for individual class</td>
<td></td>
</tr>
<tr>
<td>• <code>input</code>—Input policy</td>
<td></td>
</tr>
<tr>
<td>• <code>output</code>—Output policy</td>
<td></td>
</tr>
<tr>
<td>• <code>wireless</code>—wireless</td>
<td></td>
</tr>
<tr>
<td><code>show policy-map interface wireless ap [access point]</code></td>
<td>Displays the runtime representation and statistics for all the wireless APs on the switch.</td>
</tr>
<tr>
<td><code>show policy-map interface wireless ssid [ssid]</code></td>
<td>Displays the runtime representation and statistics for all the SSID targets on the switch.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show policy-map interface wireless client mac [mac_address]</code></td>
<td>Displays the runtime representation and statistics for all the client targets on the switch.</td>
</tr>
<tr>
<td>`show policy-map session [ input</td>
<td>output</td>
</tr>
<tr>
<td>`show policy-map type control subscriber { all</td>
<td>name }`</td>
</tr>
<tr>
<td><code>show table-map</code></td>
<td>Displays all the table maps and their configurations.</td>
</tr>
<tr>
<td>`show platform qos wireless [afd { client</td>
<td>ssid }</td>
</tr>
<tr>
<td>`show policy-map interface wireless ssid name ssid-name [radio type {24ghz</td>
<td>5ghz} ap name ap-name</td>
</tr>
<tr>
<td>`show wireless client mac-address mac_address service-policy {input</td>
<td>output}`</td>
</tr>
<tr>
<td><code>show wlan qos service-policies</code></td>
<td>Displays the SSID policies configured on all WLANs.</td>
</tr>
<tr>
<td><code>show ap name ap_name service-policy</code></td>
<td>Displays all the policies configured on the AP.</td>
</tr>
</tbody>
</table>

### Monitoring SSID and Client Policies Statistics (GUI)

Statistics are supported only for ingress policies with a maximum of five classes on wireless targets. For very large policies, statistics for ingress policies are not visible at the switch. The frequency of the statistics depends on the number of clients associated with the access point.
<table>
<thead>
<tr>
<th>Type of Statistics</th>
<th>Method</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID Policies</td>
<td>Choose <strong>Monitor &gt; Controller &gt; Statistics &gt; QoS</strong>.</td>
<td>The QoS page is displayed with a list of SSID policies, Radio Type, and AP. Choose an SSID policy, radio, and access point from the drop-down lists and click <strong>Apply</strong> to view the statistics of the chosen SSID policy. You can view details such as match criteria, confirmed bytes, conformed rate, and exceeded rate.</td>
</tr>
<tr>
<td>Client Policies</td>
<td>Choose <strong>Monitor &gt; Clients &gt; Client Details</strong>.</td>
<td>The Clients page is displayed with a list of client MAC addresses, AP, and other details. Click the MAC address of a client and click the <strong>QoS Statistics</strong> tab. You can view details such as match criteria, confirmed bytes, conformed rate, and exceeded rate.</td>
</tr>
</tbody>
</table>

**Configuration Examples for QoS**

**Examples: Classification by Access Control Lists**

This example shows how to classify packets for QoS by using access control lists (ACLs):

```
Switch# configure terminal
Switch(config)# access-list 101 permit ip host 12.4.1.1 host 15.2.1.1
Switch(config)# class-map acl-101
Switch(config-cmap)# description match on access-list 101
Switch(config-cmap)# match access-group 101
Switch(config-cmap)#
```

After creating a class map by using an ACL, you then create a policy map for the class, and apply the policy map to an interface for QoS.

**Related Topics**

- Creating a Traffic Class (CLI), on page 635
- Class Maps, on page 608

**Examples: Class of Service Layer 2 Classification**

This example shows how to classify packets for QoS using a class of service Layer 2 classification:
Switch# configure terminal
Switch(config)# class-map cos
Switch(config-cmap)# match cos ?
<0-7>  Enter up to 4 class-of-service values separated by white-spaces
Switch(config-cmap)# match cos 3 4 5
Switch(config-cmap)#

After creating a class map by using a CoS Layer 2 classification, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: Class of Service DSCP Classification

This example shows how to classify packets for QoS using a class of service DSCP classification:

Switch# configure terminal
Switch(config)# class-map dscp
Switch(config-cmap)# match dscp af21 af22 af23
Switch(config-cmap)#

After creating a class map by using a DSCP classification, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: VLAN ID Layer 2 Classification

This example shows how to classify for QoS using a VLAN ID Layer 2 classification:

Switch# configure terminal
Switch(config)# class-map vlan-120
Switch(config-cmap)# match vlan ?
<1-4095>  VLAN id
Switch(config-cmap)# match vlan 120
Switch(config-cmap)#

After creating a class map by using a VLAN Layer 2 classification, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: Classification by DSCP or Precedence Values

This example shows how to classify packets by using DSCP or precedence values:

Switch# configure terminal
Switch(config)# class-map prec2
Switch(config-cmap)# description matching precedence 2 packets
Switch(config-cmap)# match ip precedence 2
Switch(config-cmap)# exit
Switch(config)# class-map ef
Switch(config-cmap)# description EF traffic
Switch(config-cmap)# match ip dscp ef
Switch(config-cmap)#
After creating a class map by using a DSCP or precedence values, you then create a policy map for the class, and apply the policy map to an interface for QoS.

**Examples: Hierarchical Classification**

The following is an example of a hierarchical classification, where a class named parent is created, which matches another class named child. The class named child matches based on the IP precedence being set to 2.

```
Switch# configure terminal
Switch(config)# class-map child
Switch(config-cmap)# match ip precedence 2
Switch(config-cmap)# exit
Switch(config)# class-map parent
Switch(config-cmap)# match class child
Switch(config-cmap)#
```

After creating the parent class map, you then create a policy map for the class, and apply the policy map to an interface for QoS.

**Related Topics**

- Hierarchical QoS, on page 600

**Examples: Hierarchical Policy Configuration**

The following is an example of a configuration using hierarchical polices:

```
Switch# configure terminal
Switch(config)# class-map c1
Switch(config-cmap)# match dscp 30
Switch(config-cmap)# exit
Switch(config)# class-map c2
Switch(config-cmap)# match precedence 4
Switch(config-cmap)# exit
Switch(config)# class-map c3
Switch(config-cmap)# exit
Switch(config)# policy-map child
Switch(config-pmap)# class c1
Switch(config-pmap-c)# priority level 1
Switch(config-pmap-c)# policy rate percent 20 conform-action transmit exceed action drop
Switch(config-pmap-c-policy)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# class c2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# class class-default
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config)# policy-map parent
Switch(config-pmap)# class class-default
```
The following example shows a hierarchical policy using table maps:

```
Switch(config)# table-map dscp2dscp
  Switch(config-tablemap)# default copy
Switch(config)# table-map dscp2up
  Switch(config-tablemap)# map from 46 to 6
  Switch(config-tablemap)# map from 34 to 5
Switch(config)# policy-map ssid_child_policy
  Switch(config-pmap)# class voice
    Switch(config-pmap-c)# priority level 1
  Switch(config-pmap)# class video
    Switch(config-pmap-c)# priority level 2
  Switch(config-pmap)# class class-default
    Switch(config-pmap-c)# shape average 3000000
    Switch(config-pmap-c)# queue-buffer ratio 0
    Switch(config-pmap-c)# set dscp dscp table dscp2dscp
    Switch(config-pmap-c)# service-policy ssid_child_policy
```

Related Topics

Hierarchical QoS, on page 600

Examples: Classification for Voice and Video

This example describes how to classify packet streams for voice and video using switch specific information.

In this example, voice and video are coming in from end-point A into GigabitEthernet1/0/1 on the switch and have precedence values of 5 and 6, respectively. Additionally, voice and video are also coming from end-point B into GigabitEthernet1/0/2 on the switch with DSCP values of EF and AF11, respectively.

Assume that all the packets from the both the interfaces are sent on the uplink interface, and there is a requirement to police voice to 100 Mbps and video to 150 Mbps.

To classify per the above requirements, a class to match voice packets coming in on GigabitEthernet1/0/1 is created, named voice-interface-1, which matches precedence 5. Similarly another class for voice is created, named voice-interface-2, which will match voice packets in GigabitEthernet1/0/2. These classes are associated to two separate policies named input-interface-1, which is attached to GigabitEthernet1/0/1, and input-interface-2, which is attached to GigabitEthernet1/0/2. The action for this class is to mark the qos-group to 10. To match packets with QoS-group 10 on the output interface, a class named voice is created which matches on QoS-group 10. This is then associated to another policy named output-interface, which is associated to the uplink interface. Video is handled in the same way, but matches on QoS-group 20.

The following example shows how classify using the above switch specific information:

```
Switch(config)#
Switch(config)# class-map voice-interface-1
Switch(config-cmap)# match ip precedence 5
Switch(config-cmap)# exit

Switch(config)# class-map video-interface-1
Switch(config-cmap)# match ip precedence 6
```
Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic

The following example provides a template for creating a port child policy for managing quality of service for voice and video traffic.

```
Policy-map port_child_policy
    Class voice (match dscp ef)
        Priority level 1
        Police Multicast Policer
    Class video (match dscp af41)
        Priority level 2
        Police Multicast Policer
    Class mcast-data (match non-client-nrt)
```
Multicast Policer in the example above is not a keyword. It refers to the policing policy configured.

Two class maps with name voice and video are configured with DSCP assignments of 46 and 34. The voice traffic is assigned the priority of 1 and the video traffic is assigned the priority level 2 and is processed using Q0 and Q1. If your network receives multicast voice and video traffic, you can configure multicast policers. The non-client NRT data and NRT data are processed using the Q2 and Q3 queues.

**Related Topics**
- Configuring Port Policies (GUI), on page 686
- Applying or Changing Port Policies (GUI), on page 687
- Applying a QoS Policy on a WLAN (GUI), on page 687
- Port Policies, on page 596
- Port Policy Format, on page 596
- Configuring QoS Policies for Multicast Traffic (CLI), on page 685
- Wireless QoS Multicast, on page 610

### Examples: Configuring Downstream SSID Policy

To configure a downstream BSSID policy, you must first configure a port child policy with priority level queuing.

<table>
<thead>
<tr>
<th>Type of Policy</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-defined port child policy</td>
<td>policy-map port_child_policy&lt;br&gt; class voice&lt;br&gt; priority level 1 20000&lt;br&gt; class video&lt;br&gt; priority level 2 10000&lt;br&gt; class non-client-nrt-class&lt;br&gt; bandwidth remaining ratio 10&lt;br&gt; class class-default&lt;br&gt; bandwidth remaining ratio 15</td>
</tr>
<tr>
<td>Egress BSSID policy</td>
<td>policy-map bssid-policer&lt;br&gt; queue-buffer ratio 0&lt;br&gt; class class-default&lt;br&gt; shape average 30000000&lt;br&gt; set dscp dscp table dscp2dscp&lt;br&gt; set wlan user-priority dscp table dscp2up&lt;br&gt; service-policy ssid_child_qos</td>
</tr>
</tbody>
</table>
### Examples: Ingress SSID Policies

The following examples show ingress SSID hierarchical policies:

<table>
<thead>
<tr>
<th>Type of ingress SSID policies</th>
<th>Example</th>
</tr>
</thead>
</table>
| Ingress SSID hierarchical policies | policy-map ssid-child-policy  
class voice  //match dscp 46  
police 3m  
class video  //match dscp 34  
police 4m  
policy-map ssid-in-policy  
class class-default  
set dscp wlan user-priority table up2dscp  
service-policy ssid-child-policy  

| | policy-map ssid_in_policy  
class dscp=40  
set cos 1  
police 10m  
class up-l  
set dscp 34  
police 12m  
class dscp=10  
set dscp 20  
police 15m  
class class-default  
set dscp wlan user-priority table up2dscp  
police 50m |
## Examples: Client Policies

<table>
<thead>
<tr>
<th>Type of Client Policy</th>
<th>Example/Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default egress client policy</td>
<td>Any incoming traffic contains the user-priority as 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The default client policy is enabled only on WMM clients that are ACM-enabled.</td>
</tr>
<tr>
<td></td>
<td>You can verify if ACM is enabled by using the <code>show ap dot11 5ghz network</code> command. To enable ACM, use the <code>ap dot11 5ghz cac voice acm</code> command.</td>
</tr>
<tr>
<td></td>
<td>Policy-map client-def-down</td>
</tr>
<tr>
<td></td>
<td>class class-default</td>
</tr>
<tr>
<td></td>
<td>set wlan user-priority 0</td>
</tr>
<tr>
<td>Default ingress client policy</td>
<td>Any traffic that is sent to the wired network from wireless network will result in the DSCP value being set to 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The default client policy is enabled only on WMM clients that are ACM-enabled.</td>
</tr>
<tr>
<td></td>
<td>Policy-map client-def-up</td>
</tr>
<tr>
<td></td>
<td>class class-default</td>
</tr>
<tr>
<td></td>
<td>set dscp 0</td>
</tr>
<tr>
<td>Client policies generated automatically and applied to the WMM client when the client authenticates to a profile in AAA with a configured QoS-level attribute.</td>
<td>Policy Map platinum-WMM</td>
</tr>
<tr>
<td></td>
<td>Class voice-plat</td>
</tr>
<tr>
<td></td>
<td>set wlan user-priority 6</td>
</tr>
<tr>
<td></td>
<td>Class video-plat</td>
</tr>
<tr>
<td></td>
<td>set wlan user-priority 4</td>
</tr>
<tr>
<td></td>
<td>Class class-default</td>
</tr>
<tr>
<td></td>
<td>set wlan user-priority 0</td>
</tr>
<tr>
<td></td>
<td>Policy Map gold-WMM</td>
</tr>
<tr>
<td></td>
<td>Class voice-gold</td>
</tr>
<tr>
<td></td>
<td>set wlan user-priority 4</td>
</tr>
<tr>
<td></td>
<td>Class video-gold</td>
</tr>
<tr>
<td></td>
<td>set wlan user-priority 4</td>
</tr>
<tr>
<td></td>
<td>Class class-default</td>
</tr>
<tr>
<td></td>
<td>set wlan user-priority 0</td>
</tr>
<tr>
<td>Non-WMM client precious metal policies</td>
<td>Policy Map platinum</td>
</tr>
<tr>
<td></td>
<td>set wlan user-priority 6</td>
</tr>
<tr>
<td>Type of Client Policy</td>
<td>Example/Details</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
| Egress client policy where any traffic matching class voice1, the user priority is set to a pre-defined value. | The class can be set to assign a DSCP or ACL. | Policy Map client1-down  
Class voice1    //match dscp, cos  
    set wlan user-priority <>  
Class voice2    //match acl  
    set wlan user-priority <>  
Class voice3    
    set wlan user-priority <>  
Class class-default  
    set wlan user-priority 0 |
| Client policy based on AAA and TCLAS | | Policy Map client2-down[ AAA+ TCLAS pol example]  
Class    voice1\match dscp  
    police <>  
    set <>  
Class class-default  
    set <>  
Class voice1|| voice2 [match acl]  
    police <>  
    class voice1  
    set <>  
    class voice2  
    set <> |
| Client policy for voice and video for traffic in the egress direction | | Policy Map client3-down  
class voice \match dscp, cos  
    police X  
class video  
    police Y  
class class-default  
    police Z |
| Client policy for voice and video for traffic in the ingress direction using policing | | Policy Map client1-up  
class voice \match dscp, up, cos  
    police X  
class video  
    police Y  
class class-default  
    police Z |
| Client policy for voice and video based on DSCP | | Policy Map client2-up  
class voice \match dscp, up, cos  
    set dscp <>  
class video  
    set dscp <>  
class class-default  
    set dscp <> |
<table>
<thead>
<tr>
<th>Type of Client Policy</th>
<th>Example/Details</th>
</tr>
</thead>
</table>
| Client ingress policy with marking and policing     | policy-map client_in_policy  
  class dscp-48 //match dscp 48  
  set cos 3  
  police 2m  
  class up-4  //match wlan user-priority 4  
  set dscp 10  
  police 3m  
  class acl  //match acl  
  set cos 2  
  police 5m  
  class class-default  
  set dscp 20  
  police 15m |
| Hierarchical client ingress policy                  | policy-map client-child-policy  
  class voice  //match dscp 46  
  set dscp 40  
  police 5m  
  class video  //match dscp 34  
  set dscp 30  
  police 7m  
  policy-map client-in-policy  
  class class-default  
  police 15m  
  service-policy client-child-policy |

**Related Topics**
- Configuring Client Policies (CLI)
- Configuring Client Policies (GUI), on page 642
- Applying a QoS Policy on a WLAN (GUI), on page 687
- Client Policies, on page 599

**Examples: Average Rate Shaping Configuration**

The following example shows how to configure average rate shaping:

```
Switch# configure terminal
Switch(config)# class-map precl
Switch(config-cmap)# description matching precedence 1 packets
Switch(config-cmap)# match ip precedence 1
Switch(config-cmap)# end

Switch# configure terminal
Switch(config)# class-map precl
Switch(config-cmap)# description matching precedence 2 packets
Switch(config-cmap)# match ip precedence 2
Switch(config-cmap)# exit

Switch(config)# policy-map shaper
Switch(config-pmap)# class precl
Switch(config-pmap-c)# shape average 512000
Switch(config-pmap-c)# exit
```
After configuring the class maps, policy map, and shape averages for your configuration, proceed to then apply the policy map to the interface for QoS.

**Related Topics**

- Configuring Shaping (CLI), on page 683
- Average Rate Shaping, on page 616

**Examples: Queue-limit Configuration**

The following example shows how to configure a queue-limit policy based upon DSCP values and percentages:

Switch# configure terminal
Switch#(config)# policy-map port-queue
Switch#(config-pmap)# class dscp-1-2-3
Switch#(config-pmap-c)# bandwidth percent 20
Switch#(config-pmap-c)# queue-limit dscp 1 percent 80
Switch#(config-pmap-c)# queue-limit dscp 2 percent 90
Switch#(config-pmap-c)# queue-limit dscp 3 percent 100
Switch#(config-pmap-c)# exit

Switch#(config-pmap)# class dscp-4-5-6
Switch#(config-pmap-c)# bandwidth percent 20
Switch#(config-pmap-c)# queue-limit dscp 4 percent 20
Switch#(config-pmap-c)# queue-limit dscp 5 percent 30
Switch#(config-pmap-c)# queue-limit dscp 6 percent 20
Switch#(config-pmap-c)# exit

Switch#(config-pmap)# class dscp-7-8-9
Switch#(config-pmap-c)# bandwidth percent 20
Switch#(config-pmap-c)# queue-limit dscp 7 percent 20
Switch#(config-pmap-c)# queue-limit dscp 8 percent 30
Switch#(config-pmap-c)# queue-limit dscp 9 percent 20
Switch#(config-pmap-c)# exit

Switch#(config-pmap)# class dscp-10-11-12
Switch#(config-pmap-c)# bandwidth percent 20
Switch#(config-pmap-c)# queue-limit dscp 10 percent 20
Switch#(config-pmap-c)# queue-limit dscp 11 percent 30
Switch#(config-pmap-c)# queue-limit dscp 12 percent 20
Switch#(config-pmap-c)# exit

Switch#(config-pmap)# class dscp-13-14-15
Switch#(config-pmap-c)# bandwidth percent 10
Switch#(config-pmap-c)# queue-limit dscp 13 percent 20
Switch#(config-pmap-c)# queue-limit dscp 14 percent 30
Switch#(config-pmap-c)# queue-limit dscp 15 percent 20
Switch#(config-pmap-c)# end
Switch#
After finishing with the above policy map queue-limit configuration, you can then proceed to apply the policy map to an interface for QoS.

**Related Topics**
- Configuring Queue Limits (CLI), on page 680
- Weighted Tail Drop, on page 618

**Examples: Queue Buffers Configuration**

The following example shows how configure a queue buffer policy and then apply it to an interface for QoS:

Switch# configure terminal
Switch(config)# policy-map policy1001
Switch(config-pmap)# class class1001
Switch(config-pmap-c)# bandwidth remaining ratio 10
Switch(config-pmap-c)# queue-buffer ratio ?
<0-100> Queue-buffers ratio limit
Switch(config-pmap-c)# queue-buffer ratio 20
Switch(config-pmap-c)# end

Switch# configure terminal
Switch(config)# interface gigabitEthernet2/0/3
Switch(config-if)# service-policy output policy1001
Switch(config-if)# end

**Related Topics**
- Configuring Queue Buffers (CLI), on page 678
- Queue Buffer Allocation, on page 620

**Examples: Policing Action Configuration**

The following example displays the various policing actions that can be associated to the policer. These actions are accomplished using the conforming, exceeding, or violating packet configurations. You have the flexibility to drop, mark and transmit, or transmit packets that have exceeded or violated a traffic profile.

For example, a common deployment scenario is one where the enterprise customer polices traffic exiting the network towards the service provider and marks the conforming, exceeding and violating packets with different DSCP values. The service provider could then choose to drop the packets marked with the exceeded and violated DSCP values under cases of congestion, but may choose to transmit them when bandwidth is available.

**Note**

The Layer 2 fields can be marked to include the CoS fields, and the Layer 3 fields can be marked to include the precedence and the DSCP fields.

One useful feature is the ability to associate multiple actions with an event. For example, you could set the precedence bit and the CoS for all conforming packets. A submode for an action configuration could then be provided by the policing feature.

This is an example of a policing action configuration:

Switch# configure terminal
Switch(config)# policy-map police
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police cir 1000000 pir 2000000
Switch(config-pmap-c-policy)# conform-action transmit
Switch(config-pmap-c-policy)# exceed-action set-dscp-transmit dscp table exceed-markdown-table
Switch(config-pmap-c-policy)# violate-action set-dscp-transmit dscp table violate-markdown-table
Switch(config-pmap-c-policy)# end

In this example, the exceed-markdown-table and violate-markdown-table are table maps.

Note
Policer-based markdown actions are only supported using table maps. Only one markdown table map is allowed for each marking field in the switch.

Related Topics
Configuring Police (CLI), on page 673
Policing, on page 610
Token-Bucket Algorithm, on page 611

Examples: Policer VLAN Configuration

The following example displays a VLAN policer configuration. At the end of this configuration, the VLAN policy map is applied to an interface for QoS.

Switch# configure terminal
Switch(config)# class-map vlan100
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# exit
Switch(config)# policy-map vlan100
Switch(config-pmap)# policy-map class vlan100
Switch(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Switch(config-pmap-c-policy)# end
Switch# configure terminal
Switch(config)# interface gigabitEthernet1/0/5
Switch(config-if)# service-policy input vlan100

Related Topics
Classifying, Policing, and Marking Traffic on SVIs by Using Policy Maps (CLI), on page 658
Policy Map on VLANs, on page 609

Examples: Policing Units

The following examples display the various units of policing that are supported for QoS. The policing unit is the basis on which the token bucket works.

The following units of policing are supported:

- CIR and PIR are specified in bits per second. The burst parameters are specified in bytes. This is the default mode; it is the unit that is assumed when no units are specified. The CIR and PIR can also be configured in percent, in which case the burst parameters have to be configured in milliseconds.
• CIR and PIR are specified in packets per second. In this case, the burst parameters are configured in packets as well.

The following is an example of a policer configuration in bits per second:

Switch(config)# policy-map bps-policer
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police rate 256000 bps burst 1000 bytes
conform-action transmit exceed-action drop

The following is an example of a policer configuration in packets per second. In this configuration, a dual-rate three-color policer is configured where the units of measurement is packet. The burst and peak burst are all specified in packets.

Switch(config)# policy-map pps-policer
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police rate 5000 pps burst 100 packets
peak-rate 10000 pps peak-burst 200 packets conform-action transmit
exceed-action drop violate-action drop

Related Topics
   Configuring Police (CLI), on page 673
   Token-Bucket Algorithm, on page 611

Examples: Single-Rate Two-Color Policing Configuration

The following example shows how to configure a single-rate two-color policer:

Switch(config)# class-map match-any prec1
Switch(config-cmap)# match ip precedence 1
Switch(config-cmap)# exit
Switch(config)# policy-map policer
Switch(config-pmap)# class prec1
Switch(config-pmap-c)# police cir 256000 conform-action transmit exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap-c)#

Related Topics
   Configuring Police (CLI), on page 673
   Single-Rate Two-Color Policing, on page 614

Examples: Dual-Rate Three-Color Policing Configuration

The following example shows how to configure a dual-rate three-color policer:

Switch# configure terminal
Switch(config)# policy-Map dual-rate-3color-policer
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police cir 64000 bc 2000 pir 128000 be 2000
Switch(config-pmap-c)# conform-action transmit
Switch(config-pmap-c-policer)# exceed-action set-dscp-transmit dscp table exceed-markdown-table
Switch(config-pmap-c-policer)# violate-action set-dscp-transmit dscp table
Examples: Table Map Marking Configuration

The following steps and examples show how to use table map marking for your QoS configuration:

1. Define the table map.

   Define the table-map using the `table-map` command and indicate the mapping of the values. This table does not know of the policies or classes within which it will be used. The default command in the table map indicates the value to be copied into the 'to' field when there is no matching 'from' field. In the example, a table map named `table-map1` is created. The mapping defined is to convert the value from 0 to 1 and from 2 to 3, while setting the default value to 4.

   Switch(config)# table-map table-map1
   Switch(config-tablemap)# map from 0 to 1
   Switch(config-tablemap)# map from 2 to 3
   Switch(config-tablemap)# default 4
   Switch(config-tablemap)# exit

2. Define the policy map where the table map will be used.

   In the example, the incoming CoS is mapped to the DSCP based on the mapping specified in the table `table-map1`. For this example, if the incoming packet has a DSCP of 0, the CoS in the packet is set 1. If no table map name is specified the command assumes a default behavior where the value is copied as is from the 'from' field (DSCP in this case) to the 'to' field (CoS in this case). Note however, that while the CoS is a 3-bit field, the DSCP is a 6-bit field, which implies that the CoS is copied to the first three bits in the DSCP.

   Switch(config)# policy map policy1
   Switch(config-pmap)# class class-default
   Switch(config-pmap-c)# set cos dscp table table-map1
   Switch(config-pmap-c)# exit

3. Associate the policy to an interface.

   Switch(config)# interface GigabitEthernet1/0/1
   Switch(config-if)# service-policy output policy1

Note: Policier based markdown actions are only supported using table maps. Only one markdown table map is allowed for each marking field in the switch.

Related Topics

- Configuring Police (CLI), on page 673
- Dual-Rate Three-Color Policing, on page 615
Switch(config-if)# exit

Related Topics
Configuring Table Maps (CLI), on page 661
Table Map Marking, on page 612

Example: Table Map Configuration to Retain CoS Markings

The following example shows how to use table maps to retain CoS markings on an interface for your QoS configuration.

The cos-trust-policy policy (configured in the example) is enabled in the ingress direction to retain the CoS marking coming into the interface. If the policy is not enabled, only the DSCP is trusted by default. If a pure Layer 2 packet arrives at the interface, then the CoS value will be rewritten to 0 when there is no such policy in the ingress port for CoS.

Switch# configure terminal
Switch(config)# table-map cos2cos
Switch(config-tablemap)# default copy
Switch(config-tablemap)# exit

Switch(config)# policy-map cos-trust-policy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos cos table cos2cos
Switch(config-pmap-c)# exit

Switch(config)# interface GigabitEthernet1/0/2
Switch(config-if)# service-policy input cos-trust-policy
Switch(config-if)# exit

Related Topics
Trust Behavior for Wired and Wireless Ports, on page 621

Additional References for QoS

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>For complete syntax and usage information for the commands used in this chapter.</td>
<td>QoS Command Reference (Catalyst 3850 Switches)QoS Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS Quality of Service Solutions Command Reference</td>
</tr>
<tr>
<td>Related Topic</td>
<td>Document Title</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Call Admission Control (CAC)</td>
<td>System Management Configuration Guide (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>System Management Configuration Guide (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td></td>
<td>System Management Command Reference (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>System Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Multicast Shaping and Policing Rate</td>
<td>IP Multicast Routing Configuration Guide (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>Routing Configuration Guide (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Application Visibility and Control</td>
<td>System Management Configuration Guide (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>System Management Configuration Guide (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td></td>
<td>System Management Command Reference (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>System Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Application Visibility and Control</td>
<td>System Management Configuration Guide (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>System Management Configuration Guide (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td></td>
<td>System Management Command Reference (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>System Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

**Error Message Decoder**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
<tr>
<td>the Error Message Decoder tool.</td>
<td></td>
</tr>
</tbody>
</table>

**Standards and RFCs**

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<p>| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Link                                                                                                                                                                                                 |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | <a href="http://www.cisco.com/support">http://www.cisco.com/support</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |</p>
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>Support for IPv6 wireless clients. The Cisco IOS XE 3.2 software release did not support IPv6 for wireless clients. This is now supported. Client policies can now have IPv4 and IPv6 filters.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>Support for 3 radios and 11ac.</td>
</tr>
</tbody>
</table>
| Cisco IOS XE 3.3SE | New classification counters available in the `show policy-map` command.
|                   | **Note** This feature is only available on wired targets.                   |
| Cisco IOS XE 3.6E | Marking and policing actions for ingress SSID policies. Client policies are applied at the access point. |
| Cisco IOS XE 3.6E | New classification counters for wireless targets available in the `show policy-map` command. |
| Cisco IOS XE 3.6E | Statistics are supported only for ingress policies.                         |
PART X

Radio Resource Management

- Radio Resource Management, on page 713
Radio Resource Management

- Finding Feature Information, on page 713
- Prerequisites for Configuring Radio Resource Management, on page 713
- Restrictions for Radio Resource Management, on page 714
- Information About Radio Resource Management, on page 714
- How to Configure RRM, on page 722
- Monitoring RRM Parameters and RF Group Status, on page 743
- Examples: RF Group Configuration, on page 745
- Information About ED-RRM, on page 745
- Additional References for Radio Resource Management, on page 747
- Feature History and Information For Performing Radio Resource Management Configuration, on page 747

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Radio Resource Management

The switch should be configured as a mobility controller and not a mobility anchor to configure Radio Resource Management. It may require dynamic channel assignment functionality for the home APs to be supported.

The new mobility architecture that involves mobility controller and mobility agent must be configured on the switch or controllers for RRM to work.

Note

Refer Mobility Configuration Guide for configuring mobility controller and mobility agent.
Restrictions for Radio Resource Management

The number of APs in a RF-group is limited to 2000.
The number of APs in a RF-group is limited to 500.
If an AP tries to join the RF-group that already holds the maximum number of APs it can support, the device rejects the application and throws an error.
To enable Airtime Fairness mode for APs, you should disable enforce-policy mode and reapply it again. This will change the airtime fairness configuration for all the APs. You can also use the `ap name <ap-name> dot11 24ghz airtime-fairness mode enforce-policy` command to change airtime fairness mode for individual APs.

Information About Radio Resource Management

The Radio Resource Management (RRM) software that is embedded in the switch acts as a built-in Radio Frequency (RF) engineer to consistently provide real-time RF management of your wireless network. RRM enables switches to continually monitor their associated lightweight access points for the following information:

- Traffic load—The total bandwidth used for transmitting and receiving traffic. It enables wireless LAN managers to track and plan network growth ahead of client demand.
- Interference—The amount of traffic coming from other 802.11 sources.
- Noise—The amount of non-802.11 traffic that is interfering with the currently assigned channel.
- Coverage—The Received Signal Strength (RSSI) and signal-to-noise ratio (SNR) for all connected clients.
- Other —The number of nearby access points.

RRM performs these functions:

- Radio resource monitoring
- Power control transmission
- Dynamic channel assignment
- Coverage hole detection and correction
- RF grouping

Note

RRM grouping does not occur when an AP operates in a static channel that is not in the DCA channel list. The Neighbor Discovery Protocol (NDP) is sent only on DCA channels; therefore, when a radio operates on a non-DCA channel, it does not receive NDP on the channel.
Radio Resource Monitoring

RRM automatically detects and configures new switches and lightweight access points as they are added to the network. It then automatically adjusts the associated and nearby lightweight access points to optimize coverage and capacity.

Lightweight access points can scan all the valid 2.4 GHz and 5 GHz channels for the country of operation as well as for channels available in other locations. The access points in local mode go off channel for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

In the presence of voice traffic or other critical traffic (in the last 100 ms), access points can defer off-channel measurements. The access points also defer off-channel measurements based on the WLAN scan priority configurations.

Each access point spends only 0.2 percent of its time off channel. This activity is distributed across all the access points so that adjacent access points are not scanning at the same time, which could adversely affect wireless LAN performance.

RRM supports new mobility architecture for RF grouping that involves Mobility Controller (MC) and Mobility Agent (MA).

- Mobility Controller (MC)—The Cisco WLC 5700 Series Controllers, Cisco Catalyst 3850 Switch, or Cisco Unified Wireless Networking Solution controller can act as MC. The MC has MC functionality and MA functionality that is running internally into it.
- Mobility Agent (MA)—The Mobility Agent is the component that maintains client mobility state machine for a mobile client.

Information About RF Groups

An RF group is a logical collection of Cisco WLCs that coordinate to perform RRM in a globally optimized manner to perform network calculations on a per-radio basis. An RF group exists for each 802.11 network type. Clustering Cisco WLCs into a single RF group enables the RRM algorithms to scale beyond the capabilities of a single Cisco WLC.

An RF group is created based on the following parameters:

- User-configured RF network name.
- Neighbor discovery performed at the radio level.
- Country list configured on MC.

RF grouping runs between MCs.

Lightweight access points periodically send out neighbor messages over the air. Access points using the same RF group name validate messages from each other.

When access points on different Cisco WLCs hear validated neighbor messages at a signal strength of ~80 dBm or stronger, the Cisco WLCs dynamically form an RF neighborhood in auto mode. In static mode, the leader is manually selected and the members are added to the RF Group.
RF groups and mobility groups are similar, in that, they both define clusters of Cisco WLCs, but they are different in terms of their use. An RF group facilitates scalable, system-wide dynamic RF management, while a mobility group facilitates scalable, system-wide mobility and Cisco WLC redundancy.

RF Group Leader

Starting in the 7.0.116.0 release, the RF Group Leader can be configured in two ways as follows:

- **Auto Mode**—In this mode, the members of an RF group elect an RF group leader to maintain a *master* power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or RF group members experience major changes).

- **Static Mode**—In this mode, a user selects a Cisco WLC as an RF group leader manually. In this mode, the leader and the members are manually configured and fixed. If the members are unable to join the RF group, the reason is indicated. The leader tries to establish a connection with a member every minute if the member has not joined in the previous attempt.

The RF group leader analyzes real-time radio data collected by the system, calculates the power and channel assignments, and sends them to each of the Cisco WLCs in the RF group. The RRM algorithms ensure system-wide stability, and restrain channel and power scheme changes to the appropriate local RF neighborhoods.

In Cisco WLC software releases prior to 6.0, the dynamic channel assignment (DCA) search algorithm attempts to find a good channel plan for the radios associated to Cisco WLCs in the RF group, but it does not adopt a new channel plan unless it is considerably better than the current plan. The channel metric of the worst radio in both plans determines which plan is adopted. Using the worst-performing radio as the single criterion for adopting a new channel plan can result in pinning or cascading problems.

Pinning occurs when the algorithm could find a better channel plan for some of the radios in an RF group, but is prevented from pursuing such a channel plan change because the worst radio in the network does not have any better channel options. The worst radio in the RF group could potentially prevent other radios in the group from seeking better channel plans. The larger the network, the more likely pinning becomes.

Cascading occurs when one radio’s channel change results in successive channel changes to optimize the remaining radios in the RF neighborhood. Optimizing these radios could lead to their neighbors and their neighbors’ neighbors having a suboptimal channel plan and triggering their channel optimization. This effect could propagate across multiple floors or even multiple buildings if all the access point radios belong to the same RF group. This change results in considerable client confusion and network instability.

The main cause of both pinning and cascading is the way in which the search for a new channel plan is performed and that any potential channel plan changes are controlled by the RF circumstances of a single radio. In Cisco WLC software release 6.0, the DCA algorithm has been redesigned to prevent both pinning and cascading. The following changes have been implemented:

- **Multiple local searches**—The DCA search algorithm performs multiple local searches initiated by different radios in the same DCA run rather than performing a single global search that is driven by a single radio. This change addresses both pinning and cascading, while maintaining the desired flexibility and adaptability of DCA and without jeopardizing stability.
- **Multiple Channel Plan Change Initiators (CPCIs)**—Previously, the single worst radio was the sole initiator of a channel plan change. Now each radio in an RF group is evaluated and prioritized as a potential initiator. Intelligent randomization of the resulting list ensures that every radio is eventually evaluated, which eliminates the potential for pinning.

- **Limiting the propagation of channel plan changes (Localization)**—For each CPCI radio, the DCA algorithm performs a local search for a better channel plan, but only the CPCI radio itself and its one-hop neighboring access points are actually allowed to change their current transmit channels. The impact of an access point triggering a channel plan change is felt only to within two RF hops from that access point, and the actual channel plan changes are confined to within a one-hop RF neighborhood. Because this limitation applies across all CPCIs, cascading cannot occur.

- **Non-RSSI-based cumulative cost metric**—A cumulative cost metric measures how well an entire region, neighborhood, or network performs with respect to a given channel plan. The individual cost metrics of all the access points in that area are considered in order to provide an overall understanding of the channel plan’s quality. These metrics ensure that the improvement or deterioration of each single radio is factored into any channel plan change. The objective is to prevent channel plan changes in which a single radio improves, but at the expense of multiple other radios experiencing a considerable performance decline.

The RRM algorithms run at a specified updated interval, which is 600 seconds by default. Between update intervals, the RF group leader sends keepalive messages to each of the RF group members and collects real-time RF data.

---

**Note**

Several monitoring intervals are also available. See the Configuring RRM section for details.

---

**RF Group Name**

A Cisco WLC is configured in an RF group name, which is sent to all the access points joined to the Cisco WLC and used by the access points as the shared secret for generating the hashed MIC in the neighbor messages. To create an RF group, you configure all of the Cisco WLCs to be included in the group with the same RF group name.

If there is any possibility that an access point joined to a Cisco WLC might hear RF transmissions from an access point on a different Cisco WLC, you should configure the Cisco WLCs with the same RF group name. If RF transmissions between access points can be heard, then system-wide RRM is recommended to avoid 802.11 interference and contention as much as possible.

**Mobility Controller**

An MC can either be a group leader or a group member. One of the MCs can act as a RF group leader based on RF grouping and RF group election with other MCs. The order of priority to elect the RF leader is based on the maximum number of APs the controller or switch can support. The highest priority being 1 and the least being 5.

1. WiSM 2 Controllers
2. Cisco WLC 5700 Series Controllers
3. WiSM 1 Controllers
4. Catalyst 3850 Series Switches
5. Catalyst 3650 Series Switches
When one of the MCs becomes the RRM group leader, the remaining MCs become RRM group members. RRM group members send their RF information to the Group Leader. The group leader determines a channel and Tx power plan for the network and passes the information back to the RF group members. The MCs push the power plan to MA for the radios that belong to MA. These channel and power plans are ultimately pushed down to individual radios.

Note
MC has MA functionality within it.

Mobility Agent

The MA communicates with the MC. The MC includes MAC or IP address of the switch/controller while communicating with the MA.

The MA provides the following information when polled by the MC:
- Interference or noise data.
- Neighbor data.
- Radio capabilities (supported channels, power levels).
- Radio configuration (power, channel, channel width).
- Radar data.

The MC exchanges the following information with the switch/controller (MA). The message includes:
- Configurations (channel/power/channel width) for individual radios.
- Polling requests for current configurations and RF measurements for individual radios
- Group Leader Update

In turn, the MA communicates the following messages with the MC:
- RF measurements from radios (e.g. load, noise and neighbor information)
- RF capabilities and configurations of individual radios

The MA sets channel, power, and channel width on the radios when directed by the MC. The DFS, coverage hole detection/mitigation, static channel/power configurations are performed by the MA.

Rogue Access Point Detection in RF Groups

After you have created an RF group of Cisco WLCs, you need to configure the access points connected to the Cisco WLCs to detect rogue access points. The access points will then select the beacon or probe-response frames in neighboring access point messages to see if they contain an authentication information element (IE) that matches that of the RF group. If the selection is successful, the frames are authenticated. Otherwise, the authorized access point reports the neighboring access point as a rogue, records its BSSID in a rogue table, and sends the table to the Cisco WLC.

The AP has a RRM CAPWAP subsystem that exchanges messages with the mobility agent.

RRM components on the AP perform the following functions:
• AP measurements, such as interference (Wi-Fi), noise, coverage, and load, and client measurements.
• Radio neighbor discovery.
• Radar detection.
• Set various RF parameters (channel, channel width, transmit power control, and so on)

## Transmit Power Control

The switch dynamically controls access point transmit power based on the real-time wireless LAN conditions. The Transmit Power Control (TPC) algorithm increases and decreases an access point’s power in response to changes in the RF environment. In most instances, TPC seeks to lower an access point's power to reduce interference, but in the case of a sudden change in the RF coverage, for example, if an access point fails or becomes disabled, TPC can also increase power on the surrounding access points. This feature is different from coverage hole detection, which is primarily concerned with clients. TPC provides enough RF power to achieve the required coverage levels while avoiding channel interference between access points.

## Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings

The TPC algorithm balances RF power in many diverse RF environments. However, it is possible that automatic power control will not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions, for example, when all the access points must be mounted in a central hallway, placing the access points close together, but requiring coverage to the edge of the building.

In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings apply to all the access points through RF profiles in a RF network.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment, enter the maximum and minimum transmit power used by RRM in the fields in the Tx Power Control window. The range for these parameters is -10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

If you configure a maximum transmit power, RRM does not allow any access point attached to the switch to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, no access point will transmit above 11 dBm, unless the access point is configured manually.

## Dynamic Channel Assignment

Two adjacent access points on the same channel can cause either signal contention or signal collision. In a collision, data is not received by the access point. This functionality can become a problem, for example, when someone reading an e-mail in a café affects the performance of the access point in a neighboring business. Even though these are separate networks, someone sending traffic to the café on channel 1 can disrupt communication in an enterprise using the same channel. Switches can dynamically allocate access point channel assignments to avoid conflict and increase capacity and performance. Channels are reused to avoid
wasting scarce RF resources. In other words, channel 1 is allocated to a different access point far from the café, which is more effective than not using channel 1 altogether.

The switch’s Dynamic Channel Assignment (DCA) capabilities are also useful in minimizing adjacent channel interference between access points. For example, two overlapping channels in the 802.11b/g band, such as 1 and 2, cannot simultaneously use 11 or 54 Mbps. By effectively reassigning channels, the switch keeps adjacent channels that are separated.

---

**Note**
We recommend that you use only nonoverlapping channels (1, 6, 11, and so on).

**Note**
Channel change does not require you to shut down the radio.

The switch examines a variety of real-time RF characteristics to efficiently handle channel assignments as follows:

- **Access point received energy**—The received signal strength measured between each access point and its nearby neighboring access points. Channels are optimized for the highest network capacity.

- **Noise**—Noise can limit signal quality at the client and access point. An increase in noise reduces the effective cell size and degrades user experience. By optimizing channels to avoid noise sources, the switch can optimize coverage while maintaining system capacity. If a channel is unusable due to excessive noise, that channel can be avoided.

- **802.11 interference**—Interference is any 802.11 traffic that is not a part of your wireless LAN, including rogue access points and neighboring wireless networks. Lightweight access points constantly scan all the channels looking for sources of interference. If the amount of 802.11 interference exceeds a predefined configurable threshold (the default is 10 percent), the access point sends an alert to the switch. Using the RRM algorithms, the switch may then dynamically rearrange channel assignments to increase system performance in the presence of the interference. Such an adjustment could result in adjacent lightweight access points being on the same channel, but this setup is preferable to having the access points remain on a channel that is unusable due to an interfering foreign access point.

In addition, if other wireless networks are present, the switch shifts the usage of channels to complement the other networks. For example, if one network is on channel 6, an adjacent wireless LAN is assigned to channel 1 or 11. This arrangement increases the capacity of the network by limiting the sharing of frequencies. If a channel has virtually no capacity remaining, the switch may choose to avoid this channel. In huge deployments in which all nonoverlapping channels are occupied, the switch does its best, but you must consider RF density when setting expectations.

- **Load and utilization**—When utilization monitoring is enabled, capacity calculations can consider that some access points are deployed in ways that carry more traffic than other access points, for example, a lobby versus an engineering area. The switch can then assign channels to improve the access point that has performed the worst. The load is taken into account when changing the channel structure to minimize the impact on the clients that are currently in the wireless LAN. This metric keeps track of every access point’s transmitted and received packet counts to determine how busy the access points are. New clients avoid an overloaded access point and associate to a new access point. This Load and utilization parameter is disabled by default.

The switch combines this RF characteristic information with RRM algorithms to make system-wide decisions. Conflicting demands are resolved using soft-decision metrics that guarantee the best choice for minimizing
network interference. The end result is optimal channel configuration in a three-dimensional space, where access points on the floor above and below play a major factor in an overall wireless LAN configuration.

Note
Radios using 40-MHz channels in the 2.4-GHz band or 80MHz channels are not supported by DCA.

The RRM startup mode is invoked in the following conditions:

• In a single-switch environment, the RRM startup mode is invoked after the switch is upgraded and rebooted.

• In a multiple-switch environment, the RRM startup mode is invoked after an RF Group leader is elected.

You can trigger the RRM startup mode from the CLI.

The RRM startup mode runs for 100 minutes (10 iterations at 10-minute intervals). The duration of the RRM startup mode is independent of the DCA interval, sensitivity, and network size. The startup mode consists of 10 DCA runs with high sensitivity (making channel changes easy and sensitive to the environment) to converge to a steady-state channel plan. After the startup mode is finished, DCA continues to run at the specified interval and sensitivity.

Note
DCA algorithm interval is set to 1 hour, but DCA algorithm always runs in default interval of 10 min, channel allocation occurs at 10-min intervals for the first 10 cycles, and channel changes occur as per the DCA algorithm every 10 min. After that the DCA algorithm goes back to the configured time interval. This is common for both DCA interval and anchor time because it follows the steady state.

Note
If Dynamic Channel Assignment (DCA)/Transmit Power Control (TPC) is turned off on the RF group member, and auto is set on RF group leader, the channel or TX power on a member gets changed as per the algorithm that is run on the RF group leader.

Coverage Hole Detection and Correction

The RRM coverage hole detection algorithm can detect areas of radio coverage in a wireless LAN that are below the level needed for robust radio performance. This feature can alert you to the need for an additional (or relocated) lightweight access point.

If clients on a lightweight access point are detected at threshold levels (RSSI, failed client count, percentage of failed packets, and number of failed packets) lower than those specified in the RRM configuration, the access point sends a “coverage hole” alert to the switch. The alert indicates the existence of an area where clients are continually experiencing poor signal coverage, without having a viable access point to which to roam. The switch discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the switch mitigates the coverage hole by increasing the transmit power level for that specific access point. The switch does not mitigate coverage holes caused by clients that are unable to increase their transmit power or are statically set to a power level because increasing their downstream transmit power might increase interference in the network.
# How to Configure RRM

## Configuring Advanced RRM CCX Parameters (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap dot11 24ghz</td>
<td>5ghz rrm ccx location-measurement interval</td>
</tr>
<tr>
<td>Example: Switch(config)# ap dot11 24ghz rrm ccx location-measurement 15</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring Neighbor Discovery Type (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap dot11 24ghz</td>
<td>5ghz rrm ndp-type {protected</td>
</tr>
<tr>
<td>Example: Switch(config)#ap dot11 24ghz rrm ndp-type protected Switch(config)#ap dot11 24ghz rrm ndp-type transparent</td>
<td>• <strong>protected</strong>—Sets the neighbor discover type to protected. Packets are encrypted. • <strong>transparent</strong>—Sets the neighbor discover type to transparent. Packets are sent as is.</td>
</tr>
</tbody>
</table>
Configuring RRM Profile Thresholds, Monitoring Channels, and Monitoring Intervals (GUI)

Procedure

Step 1  Choose Configuration > Wireless > 802.11a/n/ac > RRM > General or Configuration > Wireless > 802.11b/g/n > RRM > General to open RRM General page.

Step 2  Configure profile thresholds used for alarming as follows:

Note  The profile thresholds have no bearing on the functionality of the RRM algorithms. Switches send an SNMP trap (or an alert) to the Cisco Prime Infrastructure or another trap receiver when individual APs values set for these threshold parameters are exceeded.

a)  In the Interference text box, enter the percentage of interference (802.11 traffic from sources outside of your wireless network) on a single access point. The valid range is 0 to 100%, and the default value is 10%.

b)  In the Clients text box, enter the number of clients on a single access point. The valid range is 1 to 75, and the default value is 12.

c)  In the Noise text box, enter the level of noise (non-802.11 traffic) on a single access point. The valid range is –127 to 0 dBm, and the default value is –70 dBm.

d)  In the Utilization text box, enter the percentage of RF bandwidth being used by a single access point. The valid range is 0 to 100%, and the default value is 80%.

e)  In the Throughput text box, enter the level of Throughput being used by a single access point. The valid range is 1000 to 1000000, and the default value is 1000000.

Step 3  From the Channel List drop-down list, choose one of the following options to specify the set of channels that the access point uses for RRM scanning:

•  All Channels—RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation.

•  Country Channels—RRM channel scanning occurs only on the data channels in the country of operation. This is the default value.

•  DCA Channels—RRM channel scanning occurs only on the channel set used by the DCA algorithm, which by default includes all of the non-overlapping channels allowed in the country of operation. However, you can specify the channel set to be used by DCA if desired. To do so, follow instructions in the Dynamic Channel Assignment.

Step 4  Configure monitor intervals as follows:

1.  In the Channel Scan Interval text box, enter (in seconds) the sum of the time between scans for each channel within a radio band. The entire scanning process takes 50 ms per channel, per radio and runs at
the interval configured here. The time spent listening on each channel is determined by the non-configurable
50-ms scan time and the number of channels to be scanned. For example, in the U.S. all 11 802.11b/g
channels are scanned for 50 ms each within the default 180-second interval. So every 16 seconds, 50 ms
is spent listening on each scanned channel (180/11 = ~16 seconds). The Channel Scan Interval parameter
determines the interval at which the scanning occurs. The valid range is 60 to 3600 seconds, and the
default value for 802.11a/n/ac and 802.11b/g/n radios is 180 seconds.

2. In the Neighbor Packet Frequency text box, enter (in seconds) how frequently neighbor packets (messages)
are sent, which eventually builds the neighbor list. The valid range is 60 to 3600 seconds, and the default
value is 60 seconds.

   Note If the access point radio does not receive a neighbor packet from an existing neighbor within
   60 minutes, the Cisco WLC deletes that neighbor from the neighbor list.

   Step 5 Click Apply.
   Step 6 Click Save Configuration.

   Note Click Set to Factory Default if you want to return all of the Cisco WLC’s RRM parameters to their
   factory-default values.

Configuring RF Groups

This section describes how to configure RF groups through either the GUI or the CLI.

   Note The RF group name is generally set at deployment time through the Startup Wizard. However, you can change
   it as necessary.

   Note When the multiple-country feature is being used, all Cisco WLCs intended to join the same RF group must
   be configured with the same set of countries, configured in the same order.

   Note You can also configure RF groups using the Cisco Prime Infrastructure.

Configuring the RF Group Mode (GUI)

   Procedure

   Step 1 Choose Configuration > Wireless > 802.11a/n/ac > RRM > RF Grouping or Configuration > Wireless >
   802.11b/g/n > RRM > RF Grouping to open the RF Grouping page.
   Step 2 From the Group Mode drop-down list, choose the mode that you want to configure for this Cisco WLC.
You can configure RF grouping in the following modes:

- **auto**—Sets the RF group selection to automatic update mode.
  
  **Note** A configured static leader cannot become a member of another RF group until its mode is set to “auto”.

- **leader**—Sets the RF group selection to static mode, and sets this Cisco WLC as the group leader.

- **off**—Sets the RF group selection off. Every Cisco WLC optimizes its own access point parameters.
  
  **Note** A Cisco WLC with a lower priority cannot assume the role of a group leader if a Cisco WLC with a higher priority is available. Here, priority is related to the processing power of the Cisco WLC.

**Note** We recommend that Cisco WLCs participate in automatic RF grouping. You can override RRM settings without disabling automatic RF group participation.

### Configuring RF Group Selection Mode (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures RF group selection mode for 802.11 bands.</td>
</tr>
<tr>
<td>`ap dot11 24ghz</td>
<td>5ghz rrm group-mode {auto</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)#ap dot11 24ghz rrm group-mode leader</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 3** Click **Apply** to save the configuration and click **Restart** to restart the RRM RF Grouping algorithm.

**Step 4** If you configured RF Grouping mode for this Cisco WLC as a static leader, you can add group members from the Group Members section as follows:

1. In the switch Name text box, enter the Cisco WLC that you want to add as a member to this group.
2. In the IP Address text box, enter the IP address of the Cisco WLC.
3. Click **Add** to add the member to this group.
   
   **Note** If the member has not joined the static leader, the reason of the failure is shown in parentheses.

**Step 5** Click **Apply**.

**Step 6** Click **Save Configuration**.
### Configuring an RF Group Name (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>wireless rf-network name</td>
<td>Creates an RF group. The group name should be ASCII String up to 19 characters and is case sensitive.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch (config)# wireless rf-network test1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>show network profile profile_number</td>
<td>Displays the RF group.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You can view the network profile number from 1 to 4294967295.</td>
</tr>
</tbody>
</table>

### Configuring an RF Group Name (GUI)

**Procedure**

- **Step 1**: Choose **Configuration > Controller > General** to open the General page.
- **Step 2**: Enter a name for the RF group in the RF Group Name text box. The name can contain up to 19 ASCII characters and is case sensitive.
- **Step 3**: Click **Apply** to commit your changes.
- **Step 4**: Click **Save Configuration** to save your changes.
Step 5  Repeat this procedure for each controller that you want to include in the RF group.

Configuring Members in a 802.11 Static RF Group (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap dot11 24ghz</td>
<td>5ghz rrm group-member group_name ip_addr</td>
</tr>
<tr>
<td>Example: Switch(config)#ap dot11 24ghz rrm group-member Grpmem01 10.1.1.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Transmit Power Control

### Configuring the Tx-Power Control Threshold (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap dot11 24ghz</td>
<td>5ghz rrm tpc-threshold threshold_value</td>
</tr>
<tr>
<td>Example: Switch(config)#ap dot11 24ghz rrm tpc-threshold –60</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring the Tx-Power Level (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **configure terminal**
| **Example:** | Switch# configure terminal |
| **Step 2** | **ap dot11 24ghz | 5ghz rrm txpower {trans_power_level | auto | max | min | once}**
| **Example:** | Switch(config)# ap dot11 24ghz rrm txpower auto |
| **Step 3** | **end**
| **Example:** | Switch(config)# end |

**Step 1**
Enters global configuration mode.

**Step 2**
Configures the 802.11 tx-power level
- **trans_power_level**—Sets the transmit power level.
- **auto**—Enables auto-RF.
- **max**—Configures the maximum auto-RF tx-power.
- **min**—Configures the minimum auto-RF tx-power.
- **once**—Enables one-time auto-RF.

**Step 3**
Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring Transmit Power Control (GUI)

### Procedure

**Step 1**
Choose Configuration > Wireless > 802.11a/n/ac > RRM > TPC or Configuration > Wireless > 802.11b > RRM > TPC to open RRM Tx Power Control (TPC) page.

**Step 2**
Choose the Transmit Power Control.
Coverage Optimal Mode (TPCv1)—Offers strong signal coverage and stability. In this mode, power can be kept low to gain extra capacity and reduce interference.

**Step 3**
Choose one of the following options from the Power Level Assignment Method list to specify the Cisco WLC’s dynamic power assignment mode:
- **Automatic**—Causes the Cisco WLC to periodically evaluate and, if necessary, update the transmit power for all joined access points. This is the default value.
- **On Demand**—Causes the Cisco WLC to periodically evaluate the transmit power for all joined access points. However, the Cisco WLC updates the power, if necessary, only when you click **Apply** after choosing **On Demand**.
The Cisco WLC does not evaluate and update the transmit power immediately when you click Apply after choosing On Demand. It waits for the next 600-second interval. This value is not configurable.

- **Fixed**—Prevents the Cisco WLC from evaluating and, if necessary, updating the transmit power for joined access points. The power level is set to the fixed value chosen from the drop-down list. The corresponding option for Fixed when you try to configure from CLI is once.

Note: The transmit power level is assigned an integer value instead of a value in mW or dBm. The integer corresponds to a power level that varies depending on the regulatory domain, channel, and antennas in which the access points are deployed.

Note: For optimal performance, we recommend that you use the Automatic setting.

**Step 4** Enter the maximum and minimum power level assignment values in the Maximum Power Level Assignment and Minimum Power Level Assignment text boxes.

The range for the Maximum Power Level Assignment is –10 to 30 dBm.

The range for the Minimum Power Level Assignment is –10 to 30 dBm.

**Step 5** In the Power Threshold text box, enter the cutoff signal level used by RRM when determining whether to reduce an access point’s power. The default value for this parameter is –70 dBm for TPCv1, but can be changed when access points are transmitting at higher (or lower) than desired power levels.

The range for this parameter is –80 to –50 dBm. Increasing this value (between –65 and –50 dBm) causes the access points to operate at a higher transmit power. Decreasing the value has the opposite effect.

In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.

This page also shows the following nonconfigurable transmit power level parameter settings:

- Power Neighbor Count—The minimum number of neighbors an access point must have for the transmit power control algorithm to run.

- Power Assignment Leader—The MAC address of the RF group leader, which is responsible for power level assignment.

- Last Power Level Assignment—The last time RRM evaluated the current transmit power level assignments.

**Step 6** Click Apply.

**Step 7** Click Save Configuration.
# Configuring 802.11 RRM Parameters

## Configuring Advanced 802.11 Channel Assignment Parameters (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ap dot11 {24ghz</td>
<td>5ghz} rrm channel cleanair-event sensitivity {high</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ap dot11 {24ghz</td>
<td>5ghz} rrm channel dca {channel number</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)#ap dot11 24ghz rrm channel dca interval 2</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Advanced 802.11 Channel Assignment Parameters (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• sensitivity – Configures the DCA sensitivity level to changes in the environment.</td>
<td></td>
</tr>
<tr>
<td>• high – Specifies the most sensitivity.</td>
<td></td>
</tr>
<tr>
<td>• low – Specifies the least sensitivity.</td>
<td></td>
</tr>
<tr>
<td>• medium – Specifies medium sensitivity.</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 4

- `ap dot11 5ghz rrm channel dca chan-width {20 | 40 | 80}`

  **Example:**

  ```
  Switch(config)#ap dot11 5ghz rrm channel dca chan-width best maximum 20
  ```

  Configures the DCA channel bandwidth for all 802.11 radios in the 5-GHz band. Sets the channel bandwidth to 20 MHz, 40 MHz, or 80 MHz. 20 MHz is the default value for channel bandwidth. 80 MHz is the default value for best. Set the channel bandwidth to best before configuring the constraints.

#### Step 5

- `ap dot11 {24ghz | 5ghz} rrm channel dca {add | remove} channel_number | anchor-time | global {auto | once} | interval | min-metric | sensitivity {high | low | medium}}`

  **Example:**

  ```
  Switch(config)#ap dot11 24ghz rrm channel dca interval 2
  ```

  Configures dynamic channel assignment (DCA) algorithm parameters for the 802.11 band.

  - **add channel_number** – Enter a channel number to be added to the DCA list. The channel_number ranges from 1 to 14.

  - **anchor-time** – Configures the anchor time for the DCA. The range is between 0 and 23 hours.

  - **global** – Configures the DCA mode for all 802.11 Cisco APs.
    - **auto** – Runs auto-RF.
    - **once** – Runs auto-RF only once.

  - **interval** – Configures the DCA interval value. The values are 1, 2, 3, 4, 6, 8, 12 and 24 hours and the default value 0 denotes 10 minutes.

  - **min-metric** – Configures the DCA minimum RSSI energy metric. The range is between -100 and -60.

  - **sensitivity** – Configures the DCA sensitivity level to changes in the environment.
    - **high** – Specifies the most sensitivity.
    - **low** – Specifies the least sensitivity.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• medium—Specifies medium sensitivity.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 6**

**ap dot11 \{24ghz | 5ghz\} rrm channel device**

**Example:**

```
Switch(config)#ap dot11 24ghz rrm channel device
```

Configures the persistent non-Wi-Fi device avoidance in the 802.11 channel assignment.

**Step 7**

**ap dot11 \{24ghz | 5ghz\} rrm channel foreign**

**Example:**

```
Switch(config)#ap dot11 24ghz rrm channel foreign
```

Configures the foreign AP 802.11 interference avoidance in the channel assignment.

**Step 8**

**ap dot11 \{24ghz | 5ghz\} rrm channel load**

**Example:**

```
Switch(config)#ap dot11 24ghz rrm channel load
```

Configures the Cisco AP 802.11 load avoidance in the channel assignment.

**Step 9**

**ap dot11 \{24ghz | 5ghz\} rrm channel noise**

**Example:**

```
Switch(config)#ap dot11 24ghz rrm channel noise
```

Configures the 802.11 noise avoidance in the channel assignment.

**Step 10**

**end**

**Example:**

```
Switch(config)#end
```

Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

---

**Configuring Dynamic Channel Assignment (GUI)**

You can specify the channels that the Dynamic Channel Assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning by using the Cisco WLC GUI.

**Note**

This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

**Procedure**

**Step 1**

Disable the 802.11a/n/ac or 802.11b/g/n network as follows:

a) Choose Configuration > Wireless > 802.11a/n/ac > Network or Configuration > Wireless > 802.11b/g/n > Network to open the Global Parameters page.
b) Unselect the 802.11a/n/ac (or 802.11b/g/n) Network Status check box.
c) Click Apply.

**Step 2** Choose Configuration > Wireless > 802.11a/n/ac > RRM > DCA or Configuration > Wireless > 802.11b/g/n > RRM > DCA to open the Dynamic Channel Assignment (DCA) page.

**Step 3** Choose one of the following options from the Channel Assignment Method drop-down list to specify the Cisco WLC’s DCA mode:

- **Automatic**—Causes the Cisco WLC to periodically evaluate and, if necessary, update the channel assignment for all joined access points. This is the default value.

- **Freeze**—Causes the Cisco WLC to evaluate and update the channel assignment for all joined access points, if necessary, only when you click **Apply** after selecting the **Freeze** option.

  **Note** The Cisco WLC does not evaluate and update the channel assignment immediately when you click **Apply** after selecting the **Freeze** option. It waits for the next interval to elapse.

- **OFF**—Turns off DCA and sets all access point radios to the first channel of the band. If you choose this option, you must manually assign channels on all radios.

  **Note** For optimal performance, we recommend that you use the Automatic setting.

**Step 4** From the Interval drop-down list, choose one of the following options to specify how often the DCA algorithm is allowed to run: 10 minutes, 1 hour, 2 hours, 3 hours, 4 hours, 6 hours, 8 hours, 12 hours, or 24 hours. The default value is 10 minutes.

**Step 5** From the Anchor Time drop-down list, choose a number to specify the time of day when the DCA algorithm is to start. The options are numbers between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.

**Step 6** Check the **Avoid Foreign AP Interference** check box to cause the Cisco WLC’s RRM algorithms to consider 802.11 traffic from foreign access points (those not included in your wireless network) when assigning channels to lightweight access points, or unselect it to disable this feature. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign access points. The default value is selected.

**Step 7** Select the **Avoid Cisco AP Load** check box to cause the Cisco WLC’s RRM algorithms to consider 802.11 traffic from Cisco lightweight access points in your wireless network when assigning channels, or unselect it to disable this feature. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load. The default value is unselected.

**Step 8** Select the **Avoid Non-802.11a (802.11b) Noise** check box to cause the Cisco WLC’s RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight access points, or unselect it to disable this feature. For example, RRM may have access points avoid channels with significant interference from nonaccess point sources, such as microwave ovens. The default value is selected.

**Step 9** Select the **Avoid Persistent Non-WiFi Interference** check box to enable the Cisco WLC to ignore persistent non-Wi-Fi interference.

**Step 10** From the DCA Channel Sensitivity drop-down list, choose one of the following options to specify how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channels:

- **Low**—The DCA algorithm is not particularly sensitive to environmental changes.

- **Medium**—The DCA algorithm is moderately sensitive to environmental changes.

- **High**—The DCA algorithm is highly sensitive to environmental changes.
The default value is Medium. The DCA sensitivity thresholds vary by radio band, as noted in the following table:

**Table 47: DCA Sensitivity Thresholds**

<table>
<thead>
<tr>
<th>Option</th>
<th>2.4-GHz DCA Sensitivity Threshold</th>
<th>5-GHz DCA Sensitivity Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>5 dB</td>
<td>5 dB</td>
</tr>
<tr>
<td>Medium</td>
<td>10 dB</td>
<td>15 dB</td>
</tr>
<tr>
<td>Low</td>
<td>20 dB</td>
<td>20 dB</td>
</tr>
</tbody>
</table>

**Step 11**

For 802.11a/n/ac networks only, choose one of the following channel width options to specify the channel bandwidth supported for all 802.11n radios in the 5-GHz band:

- **20 MHz** — The 20-MHz channel bandwidth (default)

- **40 MHz** — The 40-MHz channel bandwidth

  **Note** If you choose 40 MHz, be sure to choose at least two adjacent channels from the DCA Channel List in **Step 13** (for example, a primary channel of 36 and an extension channel of 40). If you choose only one channel, that channel is not used for 40-MHz channel width.

  **Note** If you choose 40 MHz, you can also configure the primary and extension channels used by individual access points.

  **Note** To override the globally configured DCA channel width setting, you can statically configure an access point’s radio for 20- or 40-MHz mode in the 802.11a/n Cisco APs > Configure page. If you then change the static RF channel assignment method to WLC Controlled on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

  **Note** If you choose 40 MHz on the A radio, you cannot pair channels 116, 140, and 165 with any other channels.

- **80 MHz** — The 80-MHz bandwidth for the 802.11ac radios.

  **Note** If you choose 80 MHz, be sure to choose four adjacent channels from the DCA Channel List in **Step 13** (for example, a primary channel of 36 and an extension channel of 40). If you choose only one channel, that channel is not used for 40-MHz channel width.

  **Note** If you choose 80 MHz, you can also configure the primary and extension channels used by individual access points.

  **Note** To override the globally configured DCA channel width setting, you can statically configure an access point’s radio for 20-, 40-, or 80-MHz mode on the 802.11a/n Cisco APs > Configure page. If you then change the static RF channel assignment method to WLC Controlled on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.
Note  If you choose 40 MHz on the A radio, you cannot pair channels 116, 140, and 165 with any other channels.

This page also shows the following nonconfigurable channel parameter settings:

- **Channel Assignment Leader**—The MAC address of the RF group leader, which is responsible for channel assignment.

- **Last Auto Channel Assignment**—The last time RRM evaluated the current channel assignments. This is used only for RF leader and not for the RF member.

**Step 12**  In the DCA Channel List area, the DCA Channels text box shows the channels that are currently selected. To choose a channel, select its check box in the Select column. To exclude a channel, unselect its check box.

The ranges are as follows:

- **802.11a**—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165 (depending on countries).

- **802.11b/g**—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 (depending on countries).

The defaults are as follows:

- **802.11a**—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161

- **802.11b/g**—1, 6, 11

**Step 13**  Click **Apply**.

**Step 14**  Reenable the 802.11 networks as follows:

1. Choose **Configuration > Wireless > 802.11a/n/ac > Network** or **Configuration > Wireless > 802.11b/g/n > Network** to open the Global Parameters page.

2. Select the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box.

3. Click **Apply**.

**Step 15**  Click **Save Configuration**.

---

### Configuring 802.11 Coverage Hole Detection (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch# configure terminal
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures the 802.11 coverage hole detection for data packets.</td>
</tr>
<tr>
<td>`ap dot11 24ghz</td>
<td>5ghz rrm coverage data {fail-percentage</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)#ap dot11 24ghz rrm coverage data fail-percentage 60</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the 802.11 Cisco AP coverage exception level as a percentage that ranges from 0 to 100%.</td>
</tr>
<tr>
<td>`ap dot11 24ghz</td>
<td>5ghz rrm coverage exception global exception level`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)#ap dot11 24ghz rrm coverage exception global 50</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the 802.11 Cisco AP client minimum exception level that ranges from 1 to 75 clients.</td>
</tr>
<tr>
<td>`ap dot11 24ghz</td>
<td>5ghz rrm coverage level global cli_min exception level`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)#ap dot11 24ghz rrm coverage level global 10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures the 802.11 coverage hole detection for voice packets.</td>
</tr>
<tr>
<td>`ap dot11 24ghz</td>
<td>5ghz rrm coverage voice {fail-percentage</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)#ap dot11 24ghz rrm coverage voice packet-count 10</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Coverage Hole Detection (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

#### Step 1
Disable the 802.11 network as follows:

a) Choose **Configuration > Wireless > 802.11a/n/ac** or **Configuration > Wireless > 802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Global Parameters page.

b) Unselect the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box.

c) Click **Apply**.

#### Step 2
Choose **Configuration > Wireless > 802.11a/n/ac > RRM > Coverage Thresholds** or **Configuration > Wireless > 802.11b/g/n > RRM > Coverage Thresholds** to open coverage page.

#### Step 3
Select the **Enable Coverage Hole Detection** check box to enable coverage hole detection, or unselect it to disable this feature. If you enable coverage hole detection, the Cisco WLC automatically determines, based on data received from the access points, if any access points have clients that are potentially located in areas with poor coverage. The default value is selected.

#### Step 4
In the **Data RSSI** text box, enter the minimum Receive Signal Strength Indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is −90 to −60 dBm, and the default value is −80 dBm. The access point takes data RSSI measurements every 5 seconds and reports them to the Cisco WLC in 90-second intervals.

#### Step 5
In the **Voice RSSI** text box, enter the minimum Receive Signal Strength Indication (RSSI) value for voice packets received by the access point. The value that you enter is used to identify coverage holes within your network. If the access point receives a packet in the voice queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is −90 to −60 dBm, and the default value is −80 dBm. The access point takes voice RSSI measurements every 5 seconds and reports them to the Cisco WLC in 90-second intervals.

#### Step 6
In the **Min Failed Client Count per AP** text box, enter the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold. The valid range is 1 to 75, and the default value is 3.

#### Step 7
In the **Coverage Exception Level per AP** text box, enter the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. The valid range is 0 to 100%, and the default value is 25%.
If both the number and percentage of failed packets exceed the values configured for Failed Packet Count and Failed Packet Percentage (configurable through the Cisco WLC CLI) for a 5-second period, the client is considered to be in a pre-alarm condition. The Cisco WLC uses this information to distinguish between real and false coverage holes. False positives are generally due to the poor roaming logic implemented on most clients. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the Min Failed Client Count per AP and Coverage Exception Level per AP text boxes over two 90-second periods (a total of 180 seconds). The Cisco WLC determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

**Note**

Step 8  Click **Apply**.

Step 9  Reenable the 802.11 network as follows:

a) Choose **Configuration > Wireless > 802.11a/n/ac > Network** or **Configuration > Wireless > 802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b) Select the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box.

c) Click **Apply**.

Step 10  Click **Save Configuration**.

---

### Configuring 802.11 Event Logging (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

| **Step 2** | **ap dot11 24ghz | 5ghz rrm logging|channel | coverage | foreign | load | noise | performance | txpower|
|-------------|------------------|
|              | Example:         |
|              | Switch(config)#ap dot11 24ghz rrm logging  |
|              | channel          |
|              | Switch(config)#ap dot11 24ghz rrm logging  |
|              | coverage         |
|              | Switch(config)#ap dot11 24ghz rrm logging  |
|              | foreign          |
|              | Switch(config)#ap dot11 24ghz rrm logging  |
|              | load             |
|              | Switch(config)#ap dot11 24ghz rrm logging  |
|              | noise            |
|              | Switch(config)#ap dot11 24ghz rrm logging  |
|              | performance      |

- **channel**—Configures the 802.11 channel change logging mode.
- **coverage**—Configures the 802.11 coverage profile logging mode.
- **foreign**—Configures the 802.11 foreign interference profile logging mode.
- **load**—Configures the 802.11 load profile logging mode.
- **noise**—Configures the 802.11 noise profile logging mode.
- **performance**—Configures the 802.11 performance profile logging mode.
- **txpower**—Configures the 802.11 transmit power change logging mode.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)#ap dot11 24ghz rrm logging txpower</td>
<td></td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

### Configuring 802.11 Statistics Monitoring (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap dot11 24ghz</td>
<td>5ghz rrm monitor channel-list {all</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)#ap dot11 24ghz rrm monitor channel-list all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ap dot11 24ghz</td>
<td>5ghz rrm monitor coverage interval</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)#ap dot11 24ghz rrm monitor coverage 600</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ap dot11 24ghz</td>
<td>5ghz rrm monitor load interval</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)#ap dot11 24ghz rrm monitor load 180</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ap dot11 24ghz</td>
<td>5ghz rrm monitor noise interval</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)#ap dot11 24ghz rrm monitor noise 360</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the 802.11 Performance Profile (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> ap dot11 24ghz</td>
<td>5ghz rrm profile clients cli_threshold_value</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ap dot11 24ghz rrm profile clients 20</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> ap dot11 24ghz</td>
<td>5ghz rrm profile foreign int_threshold_value</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ap dot11 24ghz rrm profile foreign 50</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> ap dot11 24ghz</td>
<td>5ghz rrm profile noise for_noise_threshold_value</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ap dot11 24ghz rrm profile noise -65</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> ap dot11 24ghz</td>
<td>5ghz rrm profile throughput throughput_threshold_value</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Rogue Access Point Detection in RF Groups

Configuring Rogue Access Point Detection in RF Groups (CLI)

**Before you begin**

Ensure that each Cisco WLC in the RF group has been configured with the same RF group name.

**Note**

The name is used to verify the authentication IE in all beacon frames. If the Cisco WLCs have different names, false alarms will occur.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> ap name <em>Cisco_AP</em> mode {local</td>
<td>monitor}</td>
</tr>
<tr>
<td>Example: Switch# ap name ap1 mode local</td>
<td></td>
</tr>
<tr>
<td><strong>Configures a particular access point for local (normal) mode or monitor (listen-only) mode. Perform this step for every access point connected to the Cisco WLC.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> end</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Enters global configuration mode.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> wireless wps ap-authentication</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Enables rogue access point detection.</strong></td>
<td></td>
</tr>
</tbody>
</table>
## Enabling Rogue Access Point Detection in RF Groups (GUI)

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch (config)# wireless wps ap-authentication</td>
<td>Specifies when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.</td>
</tr>
</tbody>
</table>

### Step 5

**wireless wps ap-authentication threshold value**

**Example:**

Switch (config)# wireless wps ap-authentication threshold 50

### Enabling Rogue Access Point Detection in RF Groups (GUI)

### Procedure

**Step 1**

Make sure that each Cisco WLC in the RF group has been configured with the same RF group name.

**Note**

The name is used to verify the authentication IE in all beacon frames. If the Cisco WLCs have different names, false alarms will occur.

**Step 2**

Choose Configuration > Wireless > Access Points > All APs to open the All APs page.

**Step 3**

Click the name of an access point to open the All APs > Edit page.

**Step 4**

Choose either local or monitor from the AP Mode drop-down list and click Apply to commit your changes.

**Step 5**

Click Save Configuration to save your changes.

**Step 6**

Repeat Step 2 through Step 5 for every access point connected to the Cisco WLC.

**Step 7**


The name of the RF group to which this Cisco WLC belongs appears at the top of the page.

**Step 8**

Choose AP Authentication from the Protection Type drop-down list to enable rogue access point detection.

**Step 9**

Enter a number in the Alarm Trigger Threshold edit box to specify when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.
The valid threshold range is from 1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.

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

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

**Step 12** Repeat this procedure on every Cisco WLC in the RF group.

**Note**  If rogue access point detection is not enabled on every Cisco WLC in the RF group, the access points on the Cisco WLCs with this feature disabled are reported as rogues.

---

**Monitoring RRM Parameters and RF Group Status**

**Monitoring RRM Parameters**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap dot11 24ghz ccx</td>
<td>Displays the 802.11b CCX information for all Cisco APs.</td>
</tr>
<tr>
<td>show ap dot11 24ghz channel</td>
<td>Displays the configuration and statistics of the 802.11b channel assignment.</td>
</tr>
<tr>
<td>show ap dot11 24ghz coverage</td>
<td>Displays the configuration and statistics of the 802.11b coverage.</td>
</tr>
<tr>
<td>show ap dot11 24ghz group</td>
<td>Displays the configuration and statistics of the 802.11b grouping.</td>
</tr>
<tr>
<td>show ap dot11 24ghz l2roam</td>
<td>Displays 802.11b l2roam information.</td>
</tr>
<tr>
<td>show ap dot11 24ghz logging</td>
<td>Displays the configuration and statistics of the 802.11b event logging.</td>
</tr>
<tr>
<td>show ap dot11 24ghz monitor</td>
<td>Displays the configuration and statistics of the 802.11b monitoring.</td>
</tr>
<tr>
<td>show ap dot11 24ghz profile</td>
<td>Displays 802.11b profiling information for all Cisco APs.</td>
</tr>
<tr>
<td>show ap dot11 24ghz receiver</td>
<td>Displays the configuration and statistics of the 802.11b receiver.</td>
</tr>
<tr>
<td>show ap dot11 24ghz summary</td>
<td>Displays the configuration and statistics of the 802.11b Cisco APs.</td>
</tr>
<tr>
<td>show ap dot11 24ghz txpower</td>
<td>Displays the configuration and statistics of the 802.11b transmit power control.</td>
</tr>
<tr>
<td>show ap dot11 5ghz ccx</td>
<td>Displays 802.11a CCX information for all Cisco APs.</td>
</tr>
<tr>
<td>show ap dot11 5ghz channel</td>
<td>Displays the configuration and statistics of the 802.11a channel assignment.</td>
</tr>
<tr>
<td>show ap dot11 5ghz coverage</td>
<td>Displays the configuration and statistics of the 802.11a coverage.</td>
</tr>
<tr>
<td>show ap dot11 5ghz group</td>
<td>Displays the configuration and statistics of the 802.11a grouping.</td>
</tr>
<tr>
<td>Commands</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show ap dot11 5ghz l2roam</td>
<td>Displays 802.11a l2roam information.</td>
</tr>
<tr>
<td>show ap dot11 5ghz logging</td>
<td>Displays the configuration and statistics of the 802.11a event logging.</td>
</tr>
<tr>
<td>show ap dot11 5ghz monitor</td>
<td>Displays the configuration and statistics of the 802.11a monitoring.</td>
</tr>
<tr>
<td>show ap dot11 5ghz profile</td>
<td>Displays 802.11a profiling information for all Cisco APs.</td>
</tr>
<tr>
<td>show ap dot11 5ghz receiver</td>
<td>Displays the configuration and statistics of the 802.11a receiver.</td>
</tr>
<tr>
<td>show ap dot11 5ghz summary</td>
<td>Displays the configuration and statistics of the 802.11a Cisco APs.</td>
</tr>
<tr>
<td>show ap dot11 5ghz txpower</td>
<td>Displays the configuration and statistics of the 802.11a transmit power control.</td>
</tr>
</tbody>
</table>

### Monitoring RF Group Status (CLI)

This section describes the new commands for RF group status.

The following commands can be used to monitor RF group status on the switch.

**Table 49: Monitoring Aggressive Load Balancing Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap dot11 5ghz group</td>
<td>Displays the Cisco WLC name which is the RF group leader for the 802.11a RF network.</td>
</tr>
<tr>
<td>show ap dot11 24ghz group</td>
<td>Displays the Cisco WLC name which is the RF group leader for the 802.11b/g RF network.</td>
</tr>
</tbody>
</table>

### Monitoring RF Group Status (GUI)

**Procedure**

**Step 1**

Choose **Configuration > Wireless > 802.11a/n/ac > or 802.11b/g/n > RRM > RF Grouping** to open the RF Grouping Algorithm page.

This page shows the details of the RF group, displaying the configurable parameter **Group mode**, the **Group role** of this Cisco WLC, the **Group Update Interval** and the Cisco WLC name and IP address of the **Group Leader** to this Cisco WLC.

**Note**

RF grouping mode can be set using the **Group Mode** drop-down list.

**Tip** Once a Cisco WLC has joined as a static member and you want to change the grouping mode, we recommend that you remove the member from the configured static-leader and also make sure that a member Cisco WLC has not been configured to be a member on multiple static leaders. This is to avoid repeated join attempts from one or more RF static leaders.
Step 2  (Optional) Repeat this procedure for the network type that you did not select (802.11a/n/ac or 802.11b/g/n).

Examples: RF Group Configuration

This example shows how to configure RF group name:

```
Switch# configure terminal
Switch(config)# wireless rf-network test1
Switch(config)# ap dot11 24ghz shutdown
Switch(config)# end
Switch # show network profile 5
```

This example shows how to configure rogue access point detection in RF groups:

```
Switch# ap name ap1 mode local
Switch# end
Switch# configure terminal
Switch(config)# wireless wps ap-authentication
Switch(config)# wireless wps ap-authentication threshold 50
Switch(config)# end
```

Information About ED-RRM

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a threshold for air quality (AQ) that, if exceeded, triggers an immediate channel change for the affected access point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active. Cisco CleanAir also identifies and locates the source of interference so that more permanent mitigation of the device can be performed at a later time.

Configuring ED-RRM on the Cisco Wireless LAN Controller (CLI)

Procedure

Step 1  Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference by entering these commands:

- `ap dot11 {24ghz | 5ghz} rrm channel cleanair-event` — Configures CleanAir driven RRM parameters for the 802.11 Cisco lightweight access points.
- `ap dot11 {24ghz | 5ghz} rrm channel cleanair-event sensitivity {low | medium | high | custom}` — Configures CleanAir driven RRM sensitivity for the 802.11 Cisco lightweight access points. Default selection is Medium.
**Configuring ED-RRM (GUI)**

**Procedure**

**Step 1** Choose **Configure > Radio Configurations > 2.4 GHZ or 5 GHZ > RRM > DCA** to open the ED-RRM page.

**Note** Before enabling ED-RRM, you have to disable Network Status from **Configure > Radio Configurations > 2.4 GHZ or 5 GHZ > Network > General** page, and then re-enable the network after configuring ED-RRM.

**Step 2** In the Event Driven RRM section, select the **EDRRM** check box to reveal ED-RRM parameters.

**Step 3** From the Sensitivity Threshold drop-down, select the value.

Options are: Low, Medium, or High. Default selection is Medium.

**Note** In the Show running configuration, the Sensitivity Threshold value selected by default is not visible.

**Step 4** Select the **Rogue Contribution** check box to reveal Rogue Duty-Cycle parameters.

**Step 5** Enter the **Rogue Duty Cycle** value in the text box.

The valid range is from 1 to 99, with 80 as the default.

**Step 6** Click **Apply**.

**Step 7** Click **Save Configuration**.
Additional References for Radio Resource Management

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RRM commands and their details</td>
<td>RRM Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td></td>
<td>RRM Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information For Performing Radio Resource Management Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
PART XI

Security

• Preventing Unauthorized Access, on page 751
• Controlling Switch Access with Passwords and Privilege Levels, on page 753
• Configuring TACACS+, on page 769
• Configuring RADIUS, on page 785
• Configuring Kerberos, on page 831
• Configuring Local Authentication and Authorization, on page 837
• Configuring Secure Shell (SSH), on page 841
• Configuring Secure Socket Layer HTTP, on page 851
• IPv4 ACLs, on page 865
• IPv6 ACLs, on page 919
• Configuring DHCP, on page 929
• Configuring IP Source Guard, on page 951
• Configuring Dynamic ARP Inspection, on page 959
• Configuring IEEE 802.1x Port-Based Authentication, on page 975
• Configuring MACsec Encryption, on page 1061
• Web-Based Authentication, on page 1083
• Configuring Cisco TrustSec, on page 1117
• Configuring Wireless Guest Access, on page 1119
• Managing Rogue Devices, on page 1145
• Classifying Rogue Access Points, on page 1157
• Configuring wIPS, on page 1171
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Preventing Unauthorized Access

You can prevent unauthorized users from reconfiguring your switch and viewing configuration information. Typically, you want network administrators to have access to your switch while you restrict access to users who dial from outside the network through an asynchronous port, connect from outside the network through a serial port, or connect through a terminal or workstation from within the local network.

To prevent unauthorized access into your switch, you should configure one or more of these security features:

- At a minimum, you should configure passwords and privileges at each switch port. These passwords are locally stored on the switch. When users attempt to access the switch through a port or line, they must enter the password specified for the port or line before they can access the switch.

- For an additional layer of security, you can also configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. 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.

- If you want to use username and password pairs, but you want to store them centrally on a server instead of locally, you can store them in a database on a security server. Multiple networking devices can then use the same database to obtain user authentication (and, if necessary, authorization) information.
- You can also enable the login enhancements feature, which logs both failed and unsuccessful login attempts. Login enhancements can also be configured to block future login attempts after a set number of unsuccessful attempts are made. For more information, see the Cisco IOS Login Enhancements documentation.

**Related Topics**

- Configuring Username and Password Pairs, on page 762
- TACACS+ and Switch Access, on page 771
- Setting a Telnet Password for a Terminal Line, on page 760
CHAPTER 41

Controlling Switch Access with Passwords and Privilege Levels

• Finding Feature Information, on page 753
• Restrictions for Controlling Switch Access with Passwords and Privileges, on page 753
• Information About Passwords and Privilege Levels, on page 754
• How to Control Switch Access with Passwords and Privilege Levels, on page 756
• Monitoring Switch Access, on page 766
• Configuration Examples for Setting Passwords and Privilege Levels, on page 767
• Additional References, on page 768

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Controlling Switch Access with Passwords and Privileges

The following are the restrictions for controlling switch access with passwords and privileges:

• Disabling password recovery will not work if you have set the switch to boot up manually by using the boot manual global configuration command. This command produces the boot loader prompt (switch:) after the switch is power cycled.

Related Topics

Disabling Password Recovery, on page 759
Password Recovery, on page 754
Information About Passwords and Privilege Levels

Default Password and Privilege Level Configuration

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 enter after they have logged into a network device.

This table shows the default password and privilege level configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable password and privilege level</td>
<td>No password is defined. The default is level 15 (privileged EXEC level). The password is not encrypted in the configuration file.</td>
</tr>
<tr>
<td>Enable secret password and privilege level</td>
<td>No password is defined. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.</td>
</tr>
<tr>
<td>Line password</td>
<td>No password is defined.</td>
</tr>
</tbody>
</table>

Additional Password Security

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, 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.

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.

Related Topics
- Protecting Enable and Enable Secret Passwords with Encryption, on page 757
- Example: Protecting Enable and Enable Secret Passwords with Encryption, on page 767

Password Recovery

By default, any end user with physical access to the switch can recover from a lost password by interrupting the boot process while the switch is powering on and then by entering a new password.

The password-recovery disable feature protects access to the switch password by disabling part of this functionality. When this feature is enabled, the end user can interrupt the boot process only by agreeing to set
the system back to the default configuration. With password recovery disabled, you can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted.

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol.

To re-enable password recovery, use the `service password-recovery` global configuration command.

**Related Topics**
- Disabling Password Recovery, on page 759
- Restrictions for Controlling Switch Access with Passwords and Privileges, on page 753

### Terminal Line Telnet Configuration

When you power-up your switch for the first time, an automatic setup program runs to assign IP information and to create a default configuration for continued use. The setup program also prompts you to configure your switch for Telnet access through a password. If you did not configure this password during the setup program, you can configure it when you set a Telnet password for a terminal line.

**Related Topics**
- Setting a Telnet Password for a Terminal Line, on page 760
- Example: Setting a Telnet Password for a Terminal Line, on page 767

### Username and Password Pairs

You can configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. 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.

**Related Topics**
- Configuring Username and Password Pairs, on page 762

### Privilege Levels

Cisco devices use privilege levels to provide password security for different levels of switch operation. By default, the Cisco IOS software operates in two modes (privilege levels) of password security: user EXEC (Level 1) and privileged EXEC (Level 15). 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.

**Privilege Levels on Lines**

Users can override the privilege level you set using the `privilege level` line configuration command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the `disable` command. If users know the password to a higher privilege level, they can use that password to enable the
higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

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.

**Command Privilege Levels**

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 traffic` 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.

**Related Topics**
- Setting the Privilege Level for a Command, on page 763
- Example: Setting the Privilege Level for a Command, on page 767
- Changing the Default Privilege Level for Lines, on page 765
- Logging into and Exiting a Privilege Level, on page 766

---

### How to Control Switch Access with Passwords and Privilege Levels

#### Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode. Follow these steps to set or change a static enable password:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>enable password password</code></td>
<td>Defines a new password or changes an existing password for access to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>By default, no password is defined.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# enable password secret321</code></td>
<td></td>
</tr>
</tbody>
</table>
For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password abc?123, do this:

1. Enter abc.
2. Enter Ctrl-v.
3. Enter ?123.

When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abc?123 at the password prompt.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

Example: Setting or Changing a Static Enable Password, on page 767

**Protecting Enable and Enable Secret Passwords with Encryption**

Follow these steps to establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify:
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>Switch&gt;</code> <code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Use one of the following:</td>
</tr>
<tr>
<td>• <code>enable password [level level] [password encryption-type encrypted-password]</code></td>
<td>• Defines a new password or changes an existing password for access to privileged EXEC mode.</td>
</tr>
<tr>
<td>• <code>enable secret [level level] [password encryption-type encrypted-password]</code></td>
<td>• Defines a secret password, which is saved using a nonreversible encryption method.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• (Optional) For <code>level</code>, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges).</td>
</tr>
<tr>
<td><code>Switch(config)# enable password example102</code></td>
<td>• For <code>password</code>, specify a string from 1 to 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.</td>
</tr>
<tr>
<td>or</td>
<td>• (Optional) For <code>encryption-type</code>, only type 5, a Cisco proprietary encryption algorithm, is available. If you specify an encryption type, you must provide an encrypted password—an encrypted password that you copy from another switch configuration.</td>
</tr>
<tr>
<td><code>Switch(config)# enable secret level 1 password secret123sample</code></td>
<td><strong>Note</strong> If you specify an encryption type and then enter a clear text password, you cannot re-enter privileged EXEC mode. You cannot recover a lost encrypted password by any method.</td>
</tr>
</tbody>
</table>

---

**Note**

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

Follow these steps to disable password recovery to protect the security of your switch:

**Before you begin**

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4 service password-encryption</td>
<td>(Optional) Encrypts the password when the password is defined or when the configuration is written. Encryption prevents the password from being readable in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# service password-encryption</td>
<td></td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 6 show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 7 copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Additional Password Security, on page 754
- Example: Protecting Enable and Enable Secret Passwords with Encryption, on page 767
### Setting a Telnet Password for a Terminal Line

Beginning in user EXEC mode, follow these steps to set a Telnet password for the connected terminal line:

#### Before you begin

- Attach a PC or workstation with emulation software to the switch console port, or attach a PC to the Ethernet management port.
- The default data characteristics of the console port are 9600, 8, 1, no parity. You might need to press the Return key several times to see the command-line prompt.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Note: If a password is required for access to privileged EXEC mode, you will be prompted for it.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> line vty 0 15</td>
<td>Configures the number of Telnet sessions (lines), and enters line configuration mode. There are 16 possible sessions on a command-capable Switch. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# line vty 0 15</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> password password</td>
<td>Sets a Telnet password for the line or lines. For password, specify a string from 1 to 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.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-line)# password abcxyz543</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-line)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- Preventing Unauthorized Access, on page 751
Configuring Username and Password Pairs

Follow these steps to configure username and password pairs:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the username, privilege level, and password for each user.</td>
</tr>
<tr>
<td><code>username name [privilege level] {password encryption-type password}</code></td>
<td>• For <code>name</code>, specify the user ID as one word or the MAC address. Spaces and quotation marks are not allowed.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• You can configure a maximum of 12000 clients each, for both username and MAC filter.</td>
</tr>
<tr>
<td>Switch(config)# <code>username adamsample privilege 1 password secret456</code></td>
<td>• (Optional) For <code>level</code>, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 1 gives user EXEC mode access.</td>
</tr>
<tr>
<td>Switch(config)# <code>username 111111111111 mac attribute</code></td>
<td>• For <code>encryption-type</code>, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow.</td>
</tr>
<tr>
<td></td>
<td>• For <code>password</code>, specify the password the user must enter to gain access to the Switch. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the <code>username</code> command.</td>
</tr>
</tbody>
</table>
### Setting the Privilege Level for a Command

Follow these steps to set the privilege level for a command:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong>&lt;br&gt;Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Setting the Privilege Level for a Command

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

configure terminal

**Example:**

Switch# configure terminal

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>privilege mode level level command</td>
<td>Sets the privilege level for a command.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# privilege exec level 14 configure</td>
<td>• For <em>mode</em>, enter <em>configure</em> for global configuration mode, <em>exec</em> for EXEC mode, <em>interface</em> for interface configuration mode, or <em>line</em> for line configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• For <em>level</em>, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the <em>enable</em> password.</td>
</tr>
<tr>
<td></td>
<td>• For <em>command</em>, specify the command to which you want to restrict access.</td>
</tr>
</tbody>
</table>

**Step 4**

enable password level level password

**Example:**

Switch(config)# enable password level 14 SecretPswd14

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>privilege mode level level command</td>
<td>Sets the privilege level for a command.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# privilege exec level 14 configure</td>
<td>• For <em>mode</em>, enter <em>configure</em> for global configuration mode, <em>exec</em> for EXEC mode, <em>interface</em> for interface configuration mode, or <em>line</em> for line configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• For <em>level</em>, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges.</td>
</tr>
<tr>
<td></td>
<td>• For <em>password</em>, specify a string from 1 to 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.</td>
</tr>
</tbody>
</table>

**Step 5**

end

**Example:**

Switch(config)# end

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>privilege mode level level command</td>
<td>Sets the privilege level for a command.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# privilege exec level 14 configure</td>
<td>• For <em>mode</em>, enter <em>configure</em> for global configuration mode, <em>exec</em> for EXEC mode, <em>interface</em> for interface configuration mode, or <em>line</em> for line configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• For <em>level</em>, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges.</td>
</tr>
<tr>
<td></td>
<td>• For <em>password</em>, specify a string from 1 to 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.</td>
</tr>
</tbody>
</table>

**Step 6**

copy running-config startup-config

**Example:**

Switch# copy running-config

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>privilege mode level level command</td>
<td>Sets the privilege level for a command.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# privilege exec level 14 configure</td>
<td>• For <em>mode</em>, enter <em>configure</em> for global configuration mode, <em>exec</em> for EXEC mode, <em>interface</em> for interface configuration mode, or <em>line</em> for line configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• For <em>level</em>, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges.</td>
</tr>
<tr>
<td></td>
<td>• For <em>password</em>, specify a string from 1 to 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.</td>
</tr>
</tbody>
</table>

(Optional) Saves your entries in the configuration file.

---

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
### Changing the Default Privilege Level for Lines

Follow these steps to change the default privilege level for the specified line:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>· Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> line vty line</td>
<td>Selects the virtual terminal line on which to restrict access.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# line vty 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> privilege level level</td>
<td>Changes the default privilege level for the line.</td>
</tr>
<tr>
<td>Example:</td>
<td>For level, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the enable password.</td>
</tr>
<tr>
<td>Switch(config)# privilege level 15</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Logging into andExiting a Privilege Level

Beginning in user EXEC mode, follow these steps to log into a specified privilege level and exit a specified privilege level.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable level</td>
<td>Logs in to a specified privilege level. Following the example, Level 15 is privileged EXEC mode. For <em>level</em>, the range is 0 to 15.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable 15</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>disable level</td>
<td>Exits to a specified privilege level. Following the example, Level 1 is user EXEC mode. For <em>level</em>, the range is 0 to 15.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# disable 1</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

Privilege Levels, on page 755

Monitoring Switch Access

Table 51: Commands for Displaying DHCP Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show privilege</td>
<td>Displays the privilege level configuration.</td>
</tr>
</tbody>
</table>
Configuration Examples for Setting Passwords and Privilege Levels

Example: Setting or Changing a Static Enable Password

This example shows how to change the enable password to 1lu2c3k4y5. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
Switch(config)# enable password 1lu2c3k4y5
```

Related Topics

- Setting or Changing a Static Enable Password, on page 756

Example: Protecting Enable and Enable Secret Passwords with Encryption

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

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

Related Topics

- Protecting Enable and Enable Secret Passwords with Encryption, on page 757
- Additional Password Security, on page 754

Example: Setting a Telnet Password for a Terminal Line

This example shows how to set the Telnet password to let45me67in89:

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
```

Related Topics

- Setting a Telnet Password for a Terminal Line, on page 760
- Terminal Line Telnet Configuration, on page 755

Example: Setting the Privilege Level for a 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:

```
Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14
```
Additional References

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring TACACS+

- Finding Feature Information, on page 769
- Prerequisites for TACACS+, on page 769
- Information About TACACS+, on page 771
- How to Configure Switch Access with TACACS+, on page 774
- Monitoring TACACS+, on page 782
- Additional References for Configuring Secure Shell, on page 782
- Feature Information for TACACS+, on page 783

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for TACACS+

The following are the prerequisites for set up and configuration of switch access with TACACS+ (must be performed in the order presented):

1. Configure the switches with the TACACS+ server addresses.
2. Set an authentication key.
3. Configure the key from Step 2 on the TACACS+ servers.
4. Enable authentication, authorization, and accounting (AAA).
5. Create a login authentication method list.
6. Apply the list to the terminal lines.
7. Create an authorization and accounting method list.
The following are the prerequisites for controlling switch access with TACACS+:

- You must have access to a configured TACACS+ server to configure TACACS+ features on your switch. Also, you must have access to TACACS+ services maintained in a database on a TACACS+ daemon typically running on a LINUX or Windows workstation.

- We recommend a redundant connection between a switch stack and the TACACS+ server. This is to help ensure that the TACACS+ server remains accessible in case one of the connected stack members is removed from the switch stack.

- You need a system running the TACACS+ daemon software to use TACACS+ on your switch.

- To use TACACS+, it must be enabled.

- Authorization must be enabled on the switch to be used.

- Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

- To use any of the AAA commands listed in this section or elsewhere, you must first enable AAA with the `aaa new-model` command.

- At a minimum, 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.

- The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific port before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named `default`). The default method list is automatically applied to all ports except those that have a named method list explicitly defined. A defined method list overrides the default method list.

- 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+.

**Related Topics**

- [TACACS+ Overview](#), on page 771
- [TACACS+ Operation](#), on page 772
- [How to Configure Switch Access with TACACS+](#), on page 774
- [Method List](#), on page 773
- [Configuring TACACS+ Login Authentication](#), on page 776
- [TACACS+ Login Authentication](#), on page 773
- [Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services](#), on page 779
- [TACACS+ Authorization for Privileged EXEC Access and Network Services](#), on page 774
Information About TACACS+

TACACS+ and Switch Access

This section describes TACACS+. TACACS+ provides detailed accounting information and flexible administrative control over the authentication and authorization processes. It is facilitated through authentication, authorization, accounting (AAA) and can be enabled only through AAA commands.

Related Topics

- Preventing Unauthorized Access, on page 751
- Configuring the Switch for Local Authentication and Authorization, on page 837
- SSH Servers, Integrated Clients, and Supported Versions, on page 843

TACACS+ Overview

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your switch.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—indpendently. 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.

The goal of TACACS+ is to provide a method for managing multiple network access points from a single management service. Your switch can be a network access server along with other Cisco routers and access servers.

Figure 41: Typical TACACS+ Network Configuration

TACACS+, administered through the AAA security services, can provide these services:
• Authentication—Provides complete control of authentication through login and password dialog, challenge and response, and messaging support.

The authentication facility can conduct a dialog with the user (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 user screens. For example, a message could notify users that their passwords must be changed because of the company’s password aging policy.

• Authorization—Provides fine-grained control over user capabilities for the duration of the user’s session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on what commands a user 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 user activity for a security audit or to provide information for user billing. Accounting records include user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the switch and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between the switch and the TACACS+ daemon are encrypted.

Related Topics

Prerequisites for TACACS+, on page 769

TACACS+ Operation

When a user attempts a simple ASCII login by authenticating to a switch using TACACS+, this process occurs:

1. When the connection is established, the switch contacts the TACACS+ daemon to obtain a username prompt to show to the user. The user enters a username, and the switch then contacts the TACACS+ daemon to obtain a password prompt. The switch displays the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ daemon.

TACACS+ allows a dialog between the daemon and the user until the daemon receives enough information to authenticate the user. The daemon prompts for a username and password combination, but can include other items, such as the user’s mother’s maiden name.

2. The switch eventually receives one of these responses from the TACACS+ daemon:
   • ACCEPT—The user is authenticated and service can begin. If the switch is configured to require authorization, authorization begins at this time.
   • REJECT—The user is not authenticated. The user 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 switch. If an ERROR response is received, the switch typically tries to use an alternative method for authenticating the user.
   • CONTINUE—The user is prompted for additional authentication information.
After authentication, the user undergoes an additional authorization phase if authorization has been enabled on the switch. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. 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 user and the services that the user can access:
   • Telnet, Secure Shell (SSH), rlogin, or privileged EXEC services
   • Connection parameters, including the host or client IP address, access list, and user timeouts

Related Topics
   Prerequisites for TACACS+, on page 769

Method List

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 backup 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.

Related Topics
   How to Configure Switch Access with TACACS+, on page 774
   Prerequisites for TACACS+, on page 769

TACACS+ Configuration Options

You can configure the switch 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.

Related Topics
   Identifying the TACACS+ Server Host and Setting the Authentication Key, on page 775

TACACS+ Login Authentication

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 backup 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.
TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user’s profile, which is located either 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.

TACACS+ 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 switch reports user 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.

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 users accessing the switch through the CLI.

Note

Although TACACS+ configuration is performed through the CLI, the TACACS+ server authenticates HTTP connections that have been configured with a privilege level of 15.

How to Configure Switch Access with TACACS+

This section describes how to configure your switch to support TACACS+.
## Identifying the TACACS+ Server Host and Setting the Authentication Key

Follow these steps to identify the TACACS+ server host and set the authentication key:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable<br>Example: Switch> enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| Step 2 | configure terminal<br>Example: Switch# configure terminal | Enters global configuration mode. |
| Step 3 | tacacs server server-name<br>Example: Switch(config)# tacacs server yourserver | Identifies 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 in which you specify them.  
For server-name, specify the server name. |
| Step 4 | address {ipv4 | ipv6} ip address<br>Example: Switch(config-server-tacacs)# address ipv4 10.0.1.12 | Configures the IP address for the TACACS server. |
| Step 5 | exit<br>Example: Switch(config-server-tacacs)# exit | Exits the TACACS server mode and enters the global configuration mode. |
| Step 6 | aaa new-model<br>Example: Switch(config)# aaa new-model | Enables AAA. |
| Step 7 | aaa group server tacacs+ group-name<br>Example: Switch(config)# aaa group server tacacs+ | (Optional) Defines the AAA server-group with a group name.  
This command puts the Switch in a server group subconfiguration mode. |
### Configuring TACACS+ Login Authentication

Follow these steps to configure TACACS+ login authentication:

#### Before you begin

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports.

---

**Note**

To secure the switch for HTTP access by using AAA methods, you must configure the switch with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

For more information about the `ip http authentication` command, see the *Cisco IOS Security Command Reference, Release 12.4*.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>your_server_group</td>
<td>(Optional) Associates 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 3.</td>
</tr>
</tbody>
</table>

**Step 8**

```
server ip-address
Example:
Switch(config)# server 10.1.2.3
```

**Step 9**

```
end
Example:
Switch(config)# end
```

**Step 10**

```
show running-config
Example:
Switch# show running-config
```

**Step 11**

```
copy running-config startup-config
Example:
Switch# copy running-config startup-config
```

Related Topics

[TACACS+ Configuration Options](#), on page 773

---

Follow these steps to configure TACACS+ login authentication:

#### Before you begin

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports.

---

**Note**

To secure the switch for HTTP access by using AAA methods, you must configure the switch with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

For more information about the `ip http authentication` command, see the *Cisco IOS Security Command Reference, Release 12.4*.
# Configuring TACACS+ Login Authentication

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
**Example:**  
`Switch> enable` |
| Step 2 | `configure terminal` | Enters global configuration mode.  
**Example:**  
`Switch# configure terminal` |
| Step 3 | `aaa new-model` | Enables AAA.  
**Example:**  
`Switch(config)# aaa new-model` |
| Step 4 | `aaa authentication login \{default | list-name\} method1 [method2...]` | Creates a login authentication method list.  
**Example:**  
`Switch(config)# aaa authentication login default tacacs+ local`  
- 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 ports.  
  - 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.  
Select one of these methods:  
- `enable`—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the `enable password` global configuration command.  
- `group tacacs+`—Uses TACACS+ authentication. Before you can use this authentication method, you must configure the TACACS+ server. |
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• line — Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the <code>password</code> command.</td>
<td></td>
</tr>
<tr>
<td>• local — Use the local username database for authentication. You must enter username information in the database. Use the <code>username password</code> global configuration command.</td>
<td></td>
</tr>
<tr>
<td>• local-case — Use a case-sensitive local username database for authentication. You must enter username information in the database by using the <code>username name password</code> global configuration command.</td>
<td></td>
</tr>
<tr>
<td>• none — Do not use any authentication for login.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 5

| Step 5 | line [console | tty | vty] line-number [ending-line-number] |
|--------|----------------------------------------|
| Example: | Switch(config)# line 2 4 |

Enters line configuration mode, and configures the lines to which you want to apply the authentication list.

### Step 6

| Step 6 | login authentication {default | list-name} |
|--------|------------------------------------------|
| Example: | Switch(config-line)# login authentication default |

Applies 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.

### Step 7

<table>
<thead>
<tr>
<th>Step 7</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config-line)# end</td>
</tr>
</tbody>
</table>

Returns to privileged EXEC mode.

### Step 8

<table>
<thead>
<tr>
<th>Step 8</th>
<th>show running-config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch# show running-config</td>
</tr>
</tbody>
</table>

Verifies your entries.
Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

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

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

Follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt;</code> <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa authorization network</td>
<td>Configures the switch for user TACACS+</td>
</tr>
<tr>
<td>tacacs+</td>
<td>authorization for all network-related service requests.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# aaa authorization network tacacs+</code></td>
<td></td>
</tr>
</tbody>
</table>
Starting TACACS+ Accounting

Follow these steps to start TACACS+ Accounting:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

---

Related Topics
TACACS+ Authorization for Privileged EXEC Access and Network Services, on page 774
Prerequisites for TACACS+, on page 769
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 aaa accounting network start-stop tacacs+</td>
<td>Enables TACACS+ accounting for all network-related service requests.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa accounting network start-stop tacacs+</td>
<td></td>
</tr>
<tr>
<td>Step 4 aaa accounting exec start-stop tacacs+</td>
<td>Enables TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa accounting exec start-stop tacacs+</td>
<td></td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 6 show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 7 copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### What to do next

To establish a session with a router if the AAA server is unreachable, use the `aaa accounting system guarantee-first` command. It guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the `no aaa accounting system guarantee-first` command.

### Related Topics

- [TACACS+ Accounting](#), on page 774
Establishing a Session with a Router if the AAA Server is Unreachable

To establishing a session with a router if the AAA server is unreachable, use the `aaa accounting system guarantee-first` command. It guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the `no aaa accounting system guarantee-first` command.

Monitoring TACACS+

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show tacacs</code></td>
<td>Displays TACACS+ server statistics.</td>
</tr>
</tbody>
</table>

Additional References for Configuring Secure Shell

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Identity Control policies and Identity Service templates for Session Aware networking.</td>
<td>Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.</td>
<td>Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature Information for TACACS+

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS 12.2(54)SG</td>
<td>The Per VRF for TACACS+ Servers feature allows per virtual route forwarding (per VRF) to be configured for authentication, authorization, and accounting (AAA) on TACACS+ servers. The following commands were introduced or modified: <code>ip tacacs source-interface</code>, <code>ip vrf forwarding (server-group)</code>, <code>server-private</code> (TACACS+).</td>
</tr>
</tbody>
</table>
Feature Information for TACACS+
Configuring RADIUS

- Finding Feature Information, on page 785
- Prerequisites for Configuring RADIUS, on page 785
- Restrictions for Configuring RADIUS, on page 786
- Information about RADIUS, on page 787
- How to Configure RADIUS, on page 810
- Monitoring CoA Functionality, on page 826
- Configuration Examples for Controlling Switch Access with RADIUS, on page 827
- Additional References for Configuring Secure Shell, on page 828
- Feature Information for RADIUS, on page 829

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring RADIUS

This section lists the prerequisites for controlling Switch access with RADIUS.

General:

- RADIUS and Authentication, Authorization, and Accounting (AAA) must be enabled to use any of the configuration commands in this chapter.

- RADIUS is facilitated through AAA and can be enabled only through AAA commands.

- Use the `aaa new-model` global configuration command to enable AAA.

- Use the `aaa authentication` global configuration command to define method lists for RADIUS authentication.
• Use **line** and **interface** commands to enable the defined method lists to be used.

• 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.

• You should have access to and should configure a RADIUS server before configuring RADIUS features on your Switch.

• The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server Version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, see the RADIUS server documentation.

• To use the Change-of-Authorization (CoA) interface, a session must already exist on the switch. CoA can be used to identify a session and enforce a disconnect request. The update affects only the specified session.

• A redundant connection between a switch stack and the RADIUS server is recommended. This is to help ensure that the RADIUS server remains accessible in case one of the connected stack members is removed from the switch stack.

For RADIUS operation:

• Users must first successfully complete RADIUS authentication before proceeding to RADIUS authorization, if it is enabled.

**Related Topics**

- **RADIUS and Switch Access**, on page 787
- **RADIUS Operation**, on page 788

## Restrictions for Configuring RADIUS

This topic covers restrictions for controlling Switch access with RADIUS.

**General:**

• To prevent a lapse in security, you cannot configure RADIUS through a network management application.

RADIUS is not suitable in the following network security situations:

• Multiprotocol access environments. RADIUS does not support AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetWare Asynchronous Services Interface (NASI), or X.25 PAD connections.

• Switch-to-switch or router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires authentication.

• Networks using a variety of services. RADIUS generally binds a user to one service model.

**Related Topics**

- **RADIUS Overview**, on page 787
Information about RADIUS

RADIUS and Switch Access

This section describes how to enable and configure RADIUS. RADIUS provides detailed accounting information and flexible administrative control over the authentication and authorization processes.

Related Topics

- Prerequisites for Configuring RADIUS, on page 785
- Configuring the Switch for Local Authentication and Authorization, on page 837
- SSH Servers, Integrated Clients, and Supported Versions, on page 843

RADIUS Overview

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco routers and switches. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

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 has been customized to work with the Kerberos security system.

- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a smart card access control system. In one case, RADIUS has been used with Enigma’s security cards to validate users and to grant access to network resources.

- Networks already using RADIUS. You can add a Cisco Switch containing a RADIUS client to the network. This might be the first step when you make a transition to a TACACS+ server. See Figure 2: Transitioning from RADIUS to TACACS+ Services below.

- Network in which the user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to the network through a protocol such as IEEE 802.1x. For more information about this protocol, see Chapter 11, “Configuring IEEE 802.1x Port-Based Authentication.”

- 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 might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.
RADIUS Operation

When a user attempts to log in and authenticate to a Switch that is access controlled by a RADIUS server, these events occur:

1. The user is prompted to enter a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of the following responses from the RADIUS server:
   • ACCEPT—The user is authenticated.
   • REJECT—The user is either not authenticated and is prompted to re-enter the username and password, or access is denied.
   • CHALLENGE—A challenge requires additional data from the user.
   • CHALLENGE PASSWORD—A response requests the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for privileged EXEC or network authorization. The additional data included with the ACCEPT or REJECT packets includes these items:

• Telnet, SSH, rlogin, or privileged EXEC services
• Connection parameters, including the host or client IP address, access list, and user timeouts

Related Topics

Prerequisites for Configuring RADIUS, on page 785
RADIUS Change of Authorization

The RADIUS Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. When a policy changes for a user or user group in AAA, administrators can send RADIUS CoA packets from the AAA server such as a Cisco Secure Access Control Server (ACS) to reinitialize authentication and apply the new policy. This section provides an overview of the RADIUS interface including available primitives and how they are used during a CoA.

- Change-of-Authorization Requests
- CoA Request Response Code
- CoA Request Commands
- Session Reauthentication
- Stacking Guidelines for Session Termination

A standard RADIUS interface is typically used in a pulled model where the request originates from a network attached device and the response come from the queried servers. Catalyst switches support the RADIUS CoA extensions defined in RFC 5176 that are typically used in a pushed model and allow for the dynamic reconfiguring of sessions from external AAA or policy servers.

The switch supports these per-session CoA requests:

- Session reauthentication
- Session termination
- Session termination with port shutdown
- Session termination with port bounce

This feature is integrated with Cisco Secure Access Control Server (ACS) 5.1.

The RADIUS interface is enabled by default on Catalyst switches. However, some basic configuration is required for the following attributes:

- Security and Password—refer to the “Preventing Unauthorized Access to Your Switch” section in this guide.
- Accounting—refer to the “Starting RADIUS Accounting” section in the Configuring Switch-Based Authentication chapter in this guide.

Cisco IOS software supports the RADIUS CoA extensions defined in RFC 5176 that are typically used in a push model to allow the dynamic reconfiguring of sessions from external AAA or policy servers. Per-session CoA requests are supported for session identification, session termination, host reauthentication, port shutdown, and port bounce. This model comprises one request (CoA-Request) and two possible response codes:

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA nonacknowledgement (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a AAA or policy server) and directed to the device that acts as a listener.
The table below shows the RADIUS CoA commands and vendor-specific attributes (VSAs) supported by Identity-Based Networking Services. All CoA commands must include the session identifier between the device and the CoA client.

Table 53: RADIUS CoA Commands Supported by Identity-Based Networking Services

<table>
<thead>
<tr>
<th>CoA Command</th>
<th>Cisco VSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate service</td>
<td>Cisco:Avpair=&quot;subscriber:command=activate-service&quot;</td>
</tr>
<tr>
<td></td>
<td>Cisco:Avpair=&quot;subscriber:service-name=&lt;service-name&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td>Cisco:Avpair=&quot;subscriber:precedence=&lt;precedence-number&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td>Cisco:Avpair=&quot;subscriber:activation-mode=replace-all&quot;</td>
</tr>
<tr>
<td>Deactivate service</td>
<td>Cisco:Avpair=&quot;subscriber:command=deactivate-service&quot;</td>
</tr>
<tr>
<td></td>
<td>Cisco:Avpair=&quot;subscriber:service-name=&lt;service-name&gt;&quot;</td>
</tr>
<tr>
<td>Bounce host port</td>
<td>Cisco:Avpair=&quot;subscriber:command=bounce-host-port&quot;</td>
</tr>
<tr>
<td>Disable host port</td>
<td>Cisco:Avpair=&quot;subscriber:command=disable-host-port&quot;</td>
</tr>
<tr>
<td>Session query</td>
<td>Cisco:Avpair=&quot;subscriber:command=session-query&quot;</td>
</tr>
<tr>
<td>Session reauthenticate</td>
<td>Cisco:Avpair=&quot;subscriber:command=reauthenticate&quot;</td>
</tr>
<tr>
<td></td>
<td>Cisco:Avpair=&quot;subscriber:reauthenticate-type=last&quot; or</td>
</tr>
<tr>
<td></td>
<td>Cisco:Avpair=&quot;subscriber:reauthenticate-type=rerun&quot;</td>
</tr>
<tr>
<td>Session terminate</td>
<td>This is a standard disconnect request and does not require a VSA.</td>
</tr>
<tr>
<td>Interface template</td>
<td>Cisco:Avpair=&quot;interface-template-name=&lt;interfacetemplate&gt;&quot;</td>
</tr>
</tbody>
</table>

Change-of-Authorization Requests

Change of Authorization (CoA) requests, as described in RFC 5176, are used in a push model to allow for session identification, host reauthentication, and session termination. The model is comprised of one request (CoA-Request) and two possible response codes:

- CoA acknowledgment (ACK) [CoA-ACK]
- CoA non-acknowledgment (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a RADIUS or policy server) and directed to the switch that acts as a listener.

RFC 5176 Compliance

The Disconnect Request message, which is also referred to as Packet of Disconnect (POD), is supported by the switch for session termination.
This table shows the IETF attributes are supported for this feature.

**Table 54: Supported IETF Attributes**

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>State</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-ID</td>
</tr>
<tr>
<td>44</td>
<td>Acct-Session-ID</td>
</tr>
<tr>
<td>80</td>
<td>Message-Authenticator</td>
</tr>
<tr>
<td>101</td>
<td>Error-Cause</td>
</tr>
</tbody>
</table>

This table shows the possible values for the Error-Cause attribute.

**Table 55: Error-Cause Values**

<table>
<thead>
<tr>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Residual Session Context Removed</td>
</tr>
<tr>
<td>202</td>
<td>Invalid EAP Packet (Ignored)</td>
</tr>
<tr>
<td>401</td>
<td>Unsupported Attribute</td>
</tr>
<tr>
<td>402</td>
<td>Missing Attribute</td>
</tr>
<tr>
<td>403</td>
<td>NAS Identification Mismatch</td>
</tr>
<tr>
<td>404</td>
<td>Invalid Request</td>
</tr>
<tr>
<td>405</td>
<td>Unsupported Service</td>
</tr>
<tr>
<td>406</td>
<td>Unsupported Extension</td>
</tr>
<tr>
<td>407</td>
<td>Invalid Attribute Value</td>
</tr>
<tr>
<td>501</td>
<td>Administratively Prohibited</td>
</tr>
<tr>
<td>502</td>
<td>Request Not Routable (Proxy)</td>
</tr>
<tr>
<td>503</td>
<td>Session Context Not Found</td>
</tr>
<tr>
<td>504</td>
<td>Session Context Not Removable</td>
</tr>
<tr>
<td>505</td>
<td>Other Proxy Processing Error</td>
</tr>
<tr>
<td>506</td>
<td>Resources Unavailable</td>
</tr>
<tr>
<td>507</td>
<td>Request Initiated</td>
</tr>
<tr>
<td>508</td>
<td>Multiple Session Selection Unsupported</td>
</tr>
</tbody>
</table>
Preconditions

To use the CoA interface, a session must already exist on the switch. CoA can be used to identify a session and enforce a disconnect request. The update affects only the specified session.

CoA Request Response Code

The CoA Request response code can be used to convey a command to the switch.

The packet format for a CoA Request Response code as defined in RFC 5176 consists of the following fields: Code, Identifier, Length, Authenticator, and Attributes in the Type:Length:Value (TLV) format. The Attributes field is used to carry Cisco vendor-specific attributes (VSAs).

Related Topics

CoA Request Commands, on page 793

Session Identification

For disconnect and CoA requests targeted at a particular session, the switch locates the session based on one or more of the following attributes:

- Acct-Session-Id (IETF attribute #44)
- Audit-Session-Id (Cisco VSA)
- Calling-Station-Id (IETF attribute #31 which contains the host MAC address)
- IPv6 Attributes, which can be one of the following:
  - Framed-IPv6-Prefix (IETF attribute #97) and Framed-Interface-Id (IETF attribute #96), which together create a full IPv6 address per RFC 3162
  - Framed-IP6-Address
- Plain IP Address (IETF attribute #8)

Unless all session identification attributes included in the CoA message match the session, the switch returns a Disconnect-NAK or CoA-NAK with the “Invalid Attribute Value” error-code attribute.

If more than one session identification attribute is included in the message, all the attributes must match the session or the switch returns a Disconnect-negative acknowledgment (NAK) or CoA-NAK with the error code “Invalid Attribute Value.”

The packet format for a CoA Request code as defined in RFC 5176 consists of the fields: Code, Identifier, Length, Authenticator, and Attributes in Type:Length:Value (TLV) format.
The attributes field is used to carry Cisco vendor-specific attributes (VSAs).

For CoA requests targeted at a particular enforcement policy, the device returns a CoA-NAK with the error code “Invalid Attribute Value” if any of the above session identification attributes are included in the message.

Related Topics

- CoA Disconnect-Request, on page 794
- CoA Request: Disable Host Port, on page 795
- CoA Request: Bounce-Port, on page 795

CoA ACK Response Code

If the authorization state is changed successfully, a positive acknowledgment (ACK) is sent. The attributes returned within CoA ACK will vary based on the CoA Request and are discussed in individual CoA Commands.

CoA NAK Response Code

A negative acknowledgment (NAK) indicates a failure to change the authorization state and can include attributes that indicate the reason for the failure. Use `show` commands to verify a successful CoA.

CoA Request Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Cisco VSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reauthenticate host</td>
<td>Cisco:Avpair=&quot;subscriber:command=reauthenticate&quot;</td>
</tr>
<tr>
<td>Terminate session</td>
<td>This is a standard disconnect request that does not require a VSA.</td>
</tr>
<tr>
<td>Bounce host port</td>
<td>Cisco:Avpair=&quot;subscriber:command=bounce-host-port&quot;</td>
</tr>
<tr>
<td>Disable host port</td>
<td>Cisco:Avpair=&quot;subscriber:command=disable-host-port&quot;</td>
</tr>
</tbody>
</table>

6 All CoA commands must include the session identifier between the switch and the CoA client.

Related Topics

- CoA Request Response Code, on page 792

Session Reauthentication

The AAA server typically generates a session reauthentication request when a host with an unknown identity or posture joins the network and is associated with a restricted access authorization profile (such as a guest VLAN). A reauthentication request allows the host to be placed in the appropriate authorization group when its credentials are known.

To initiate session authentication, the AAA server sends a standard CoA-Request message which contains a Cisco VSA in this form: `Cisco:Avpair="subscriber:command=reauthenticate"` and one or more session identification attributes.

The current session state determines the switch response to the message. If the session is currently authenticated by IEEE 802.1x, the switch responds by sending an EAPoL (Extensible Authentication Protocol over Lan) -RequestId message to the server.
If the session is currently authenticated by MAC authentication bypass (MAB), the switch sends an access-request to the server, passing the same identity attributes used for the initial successful authentication.

If session authentication is in progress when the switch receives the command, the switch terminates the process, and restarts the authentication sequence, starting with the method configured to be attempted first.

If the session is not yet authorized, or is authorized via guest VLAN, or critical VLAN, or similar policies, the reauthentication message restarts the access control methods, beginning with the method configured to be attempted first. The current authorization of the session is maintained until the reauthentication leads to a different authorization result.

### Session Reauthentication in a Switch Stack

When a switch stack receives a session reauthentication message:

- It checkpoints the need for a re-authentication before returning an acknowledgment (ACK).
- It initiates reauthentication for the appropriate session.
- If authentication completes with either success or failure, the signal that triggered the reauthentication is removed from the stack member.
- If the stack master fails before authentication completes, reauthentication is initiated after stack master switch-over based on the original command (which is subsequently removed).
- If the stack master fails before sending an ACK, the new stack master treats the re-transmitted command as a new command.

### Session Termination

There are three types of CoA requests that can trigger session termination. A CoA Disconnect-Request terminates the session, without disabling the host port. This command causes re-initialization of the authenticator state machine for the specified host, but does not restrict that host access to the network.

To restrict a host’s access to the network, use a CoA Request with the Cisco:Avpair="subscriber:command=disable-host-port" VSA. This command is useful when a host is known to be causing problems on the network, and you need to immediately block network access for the host. When you want to restore network access on the port, re-enable it using a non-RADIUS mechanism.

When a device with no supplicant, such as a printer, needs to acquire a new IP address (for example, after a VLAN change), terminate the session on the host port with port-bounce (temporarily disable and then re-enable the port).

### CoA Disconnect-Request

This command is a standard Disconnect-Request. If the session cannot be located, the switch returns a Disconnect-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the switch terminates the session. After the session has been completely removed, the switch returns a Disconnect-ACK.

If the switch fails-over to a standby switch before returning a Disconnect-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the session is not found following re-sending, a Disconnect-ACK is sent with the “Session Context Not Found” error-code attribute.

**Related Topics**

- Session Identification, on page 792
CoA Request: Disable Host Port

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. To restore network access on the port, reenable it using a non-RADIUS mechanism. This command is carried in a standard CoA-Request message that has this new vendor-specific attribute (VSA):

```
Cisco:Avpair="subscriber:command=disable-host-port"
```

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the “Session Identification” section. If the session cannot be located, the switch returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the switch disables the hosting port and returns a CoA-ACK message.

If the switch fails before returning a CoA-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the switch fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is restarted on the new active switch.

---

**Note**

A Disconnect-Request failure following command re-sending could be the result of either a successful session termination before change-over (if the Disconnect-ACK was not sent) or a session termination by other means (for example, a link failure) that occurred after the original command was issued and before the standby switch became active.

Related Topics

- [Session Identification](#), on page 792

CoA Request: Bounce-Port

A RADIUS server CoA bounce port sent from a RADIUS server can cause a link flap on an authentication port, which triggers DHCP renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The CoA bounce port is carried in a standard CoA-Request message that contains the following VSA:

```
Cisco:Avpair="subscriber:command=bounce-host-port"
```

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes. If the session cannot be located, the switch returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the switch disables the hosting port for a period of 10 seconds, re-enables it (port-bounce), and returns a CoA-ACK.

If the switch fails before returning a CoA-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the switch fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is re-started on the new active switch.

Related Topics

- [Session Identification](#), on page 792

Stacking Guidelines for Session Termination

No special handling is required for CoA Disconnect-Request messages in a switch stack.
Stacking Guidelines for CoA-Request Bounce-Port

Because the `bounce-port` command is targeted at a session, not a port, if the session is not found, the command cannot be executed.

When the Auth Manager command handler on the stack master receives a valid `bounce-port` command, it checkpoints the following information before returning a CoA-ACK message:

- the need for a port-bounce
- the port-id (found in the local session context)

The switch initiates a port-bounce (disables the port for 10 seconds, then re-enables it).

If the port-bounce is successful, the signal that triggered the port-bounce is removed from the standby stack master.

If the stack master fails before the port-bounce completes, a port-bounce is initiated after stack master change-over based on the original command (which is subsequently removed).

If the stack master fails before sending a CoA-ACK message, the new stack master treats the re-sent command as a new command.

Stacking Guidelines for CoA-Request Disable-Port

Because the `disable-port` command is targeted at a session, not a port, if the session is not found, the command cannot be executed.

When the Auth Manager command handler on the stack master receives a valid `disable-port` command, it verifies this information before returning a CoA-ACK message:

- the need for a port-disable
- the port-id (found in the local session context)

The switch attempts to disable the port.

If the port-disable operation is successful, the signal that triggered the port-disable is removed from the standby stack master.

If the stack master fails before the port-disable operation completes, the port is disabled after stack master change-over based on the original command (which is subsequently removed).

If the stack master fails before sending a CoA-ACK message, the new stack master treats the re-sent command as a new 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.

When enabled, RADIUS can authenticate users accessing the switch through the CLI.

RADIUS Server Host

Switch-to-RADIUS-server communication involves several components:

- Hostname or IP address
• Authentication destination port
• Accounting destination port
• Key string
• Timeout period
• Retransmission value

You identify RADIUS security servers by their hostname or IP address, hostname 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.

If two different host entries on the same RADIUS server are configured for the same service—for example, 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 %RADIUS-4-RADIUS_DEAD message appears, and then the switch 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 switch 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 switch.

The timeout, retransmission, and encryption key values can be configured globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings.

**Related Topics**
- Identifying the RADIUS Server Host, on page 810
- Defining AAA Server Groups, on page 815
- Configuring Settings for All RADIUS Servers, on page 820
- Configuring RADIUS Login Authentication, on page 813

---

**RADIUS Login Authentication**

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific port 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 ports 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 backup 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.

**Related Topics**
- Configuring RADIUS Login Authentication, on page 813
AAA Server Groups

You can configure the switch 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, which 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), 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 different UDP ports on a server at the same IP address. If you configure two different host entries on the same RADIUS server for the same service, (for example, accounting), the second configured host entry acts as a fail-over backup to the first one. If the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order in which they are configured.)

Related Topics
Defining AAA Server Groups, on page 815

AAA Authorization

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user’s profile, which 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.

Related Topics
Configuring RADIUS Authorization for User Privileged Access and Network Services, on page 817

RADIUS Accounting

The AAA accounting feature tracks the services that users are using and the amount of network resources that they are consuming. When you enable AAA accounting, the switch 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. You can then analyze the data for network management, client billing, or auditing.

Related Topics
Starting RADIUS Accounting, on page 818

Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the switch 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, which 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 attribute-value (AV) pair defined in the Cisco TACACS+ specification, and sep is = for mandatory attributes and is * for optional attributes. The full set of features available for TACACS+ authorization can then be used for RADIUS.

For example, the following AV pair causes Cisco’s “multiple named IP address pools” feature to be activated during IP authorization (during PPP’s Internet Protocol Control Protocol (IPCP) address assignment):

cisco-avpair= “ip:addr-pool=first”

If you insert an “*”, the AV pair “ip:addr-pool=first” becomes optional. Note that any AV pair can be made optional:

cisco-avpair= “ip:addr-pool*first”

The following example shows how to cause a user logging in from a network access server to have immediate access to 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, see RFC 2138, “Remote Authentication Dial-In User Service (RADIUS).”

Attribute 26 contains the following three elements:

• Type
• Length
• String (also known as data)
  • Vendor-Id
  • Vendor-Type
  • Vendor-Length
  • Vendor-Data

The figure below shows the packet format for a VSA encapsulated “behind” attribute 26.

Figure 43: VSA Encapsulated Behind Attribute 26

It is up to the vendor to specify the format of their VSA. The Attribute-Specific field (also known as Vendor-Data) is dependent on the vendor's definition of that attribute.

The table below describes significant fields listed in the Vendor-Specific RADIUS IETF Attributes table (second table below), which lists supported vendor-specific RADIUS attributes (IETF attribute 26).
### Table 57: Vendor-Specific Attributes Table Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>All attributes listed in the following table are extensions of IETF attribute 26.</td>
</tr>
<tr>
<td>Vendor-Specific Command Codes</td>
<td>A defined code used to identify a particular vendor. Code 9 defines Cisco VSAs, 311 defines Microsoft VSAs, and 529 defines Ascend VSAs.</td>
</tr>
<tr>
<td>Sub-Type Number</td>
<td>The attribute ID number. This number is much like the ID numbers of IETF attributes, except it is a “second layer” ID number encapsulated behind attribute 26.</td>
</tr>
<tr>
<td>Attribute</td>
<td>The ASCII string name of the attribute.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the attribute.</td>
</tr>
</tbody>
</table>

### Table 58: Vendor-Specific RADIUS IETF Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>311</td>
<td>1</td>
<td>MSCHAP-Response</td>
<td>Contains the response value provided by a PPP MS-CHAP user in response to the challenge. It is only used in Access-Request packets. This attribute is identical to the PPP CHAP Identifier. (RFC 2548)</td>
</tr>
<tr>
<td>26</td>
<td>311</td>
<td>11</td>
<td>MSCHAP-Challenge</td>
<td>Contains the challenge sent by a network access server to an MS-CHAP user. It can be used in both Access-Request and Access-Challenge packets. (RFC 2548)</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-cm-local-window-size</td>
<td>Specifies the maximum receive window size for L2TP control messages. This value is advertised to the peer during tunnel establishment.</td>
</tr>
<tr>
<td>Number</td>
<td>Vendor-Specific Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------</td>
<td>----------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>12tp-drop-out-of-order</td>
<td>Respects sequence numbers on data packets by dropping those that are received out of order. This does not ensure that sequence numbers will be sent on data packets, just how to handle them if they are received.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>12tp-hello-interval</td>
<td>Specifies the number of seconds for the hello keepalive interval. Hello packets are sent when no data has been sent on a tunnel for the number of seconds configured here.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>12tp-hidden-avp</td>
<td>When enabled, sensitive AVPs in L2TP control messages are scrambled or hidden.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>12tp-nosession-timeout</td>
<td>Specifies the number of seconds that a tunnel will stay active with no sessions before timing out and shutting down.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>tunnel-tos-reflect</td>
<td>Copies the IP ToS field from the IP header of each payload packet to the IP header of the tunnel packet for packets entering the tunnel at the LNS.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>12tp-tunnel-authen</td>
<td>If this attribute is set, it performs L2TP tunnel authentication.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>12tp-tunnel-password</td>
<td>Shared secret used for L2TP tunnel authentication and AVP hiding.</td>
</tr>
</tbody>
</table>
### Vendor-Specific RADIUS Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-udp-checksum</td>
<td>This is an authorization attribute and defines whether L2TP should perform UDP checksums for data packets. Valid values are “yes” and “no.” The default is no.</td>
</tr>
</tbody>
</table>

### Store and Forward Fax Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>3</td>
<td>Fax-Account-Id-Origin</td>
<td>Indicates the account ID origin as defined by system administrator for the <code>mmoip aaa receive-id</code> or the <code>mmoip aaa send-id</code> commands.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>4</td>
<td>Fax-Msg-Id=</td>
<td>Indicates a unique fax message identification number assigned by Store and Forward Fax.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>5</td>
<td>Fax-Pages</td>
<td>Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>6</td>
<td>Fax-Coverpage-Flag</td>
<td>Indicates whether or not a cover page was generated by the off-ramp gateway for this fax session. True indicates that a cover page was generated; false means that a cover page was not generated.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>7</td>
<td>Fax-Modem-Time</td>
<td>Indicates the amount of time in seconds the modem sent fax data (x) and the amount of time in seconds of the total fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds, and the total fax session took 15 seconds.</td>
</tr>
</tbody>
</table>
### Vendor-Specific RADIUS Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>8</td>
<td>Fax-Connect-Speed</td>
<td>Indicates the modem speed at which this fax-mail was initially transmitted or received. Possible values are 1200, 4800, 9600, and 14400.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>9</td>
<td>Fax-Recipient-Count</td>
<td>Indicates the number of recipients for this fax transmission. Until e-mail servers support Session mode, the number should be 1.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>10</td>
<td>Fax-Process-Abort-Flag</td>
<td>Indicates that the fax session was aborted or successful. True means that the session was aborted; false means that the session was successful.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>11</td>
<td>Fax-Dsn-Address</td>
<td>Indicates the address to which DSNs will be sent.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>12</td>
<td>Fax-Dsn-Flag</td>
<td>Indicates whether or not DSN has been enabled. True indicates that DSN has been enabled; false means that DSN has not been enabled.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>13</td>
<td>Fax-Mdn-Address</td>
<td>Indicates the address to which MDNs will be sent.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>14</td>
<td>Fax-Mdn-Flag</td>
<td>Indicates whether or not message delivery notification (MDN) has been enabled. True indicates that MDN had been enabled; false means that MDN had not been enabled.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>15</td>
<td>Fax-Auth-Status</td>
<td>Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown.</td>
</tr>
<tr>
<td>Number</td>
<td>Vendor-Specific Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------</td>
<td>-----------------</td>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>16</td>
<td>Email-Server-Address</td>
<td>Indicates the IP address of the e-mail server handling the on-ramp fax-mail message.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>17</td>
<td>Email-Server-Ack-Flag</td>
<td>Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>18</td>
<td>Gateway-Id</td>
<td>Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>19</td>
<td>Call-Type</td>
<td>Describes the type of fax activity: fax receive or fax send.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>20</td>
<td>Port-Used</td>
<td>Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>21</td>
<td>Abort-Cause</td>
<td>If the fax session aborts, indicates the system component that signaled the abort. Examples of system components that could trigger an abort are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server.</td>
</tr>
</tbody>
</table>

**H323 Attributes**

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>23</td>
<td>Remote-Gateway-ID (h323-remote-address)</td>
<td>Indicates the IP address of the remote gateway.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>24</td>
<td>Connection-ID (h323-conf-id)</td>
<td>Identifies the conference ID.</td>
</tr>
<tr>
<td>Number</td>
<td>Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
<td>-----------------</td>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>25</td>
<td>Setup-Time (h323-setup-time)</td>
<td>Indicates the setup time for this connection in Coordinated Universal Time (UTC) formerly known as Greenwich Mean Time (GMT) and Zulu time.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>26</td>
<td>Call-Origin (h323-call-origin)</td>
<td>Indicates the origin of the call relative to the gateway. Possible values are originating and terminating (answer).</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>27</td>
<td>Call-Type (h323-call-type)</td>
<td>Indicates call leg type. Possible values are telephony and VoIP.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>28</td>
<td>Connect-Time (h323-connect-time)</td>
<td>Indicates the connection time for this call leg in UTC.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>29</td>
<td>Disconnect-Time (h323-disconnect-time)</td>
<td>Indicates the time this call leg was disconnected in UTC.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>30</td>
<td>Disconnect-Cause (h323-disconnect-cause)</td>
<td>Specifies the reason a connection was taken offline per Q.931 specification.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>31</td>
<td>Voice-Quality (h323-voice-quality)</td>
<td>Specifies the impairment factor (ICPIF) affecting voice quality for a call.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>33</td>
<td>Gateway-ID (h323-gw-id)</td>
<td>Indicates the name of the underlying gateway.</td>
</tr>
</tbody>
</table>

Large Scale Dialout Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>callback-dialstring</td>
<td>Defines a dialing string to be used for callback.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>data-service</td>
<td>No description available.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>dial-number</td>
<td>Defines the number to dial.</td>
</tr>
</tbody>
</table>
## Vendor-Specific RADIUS Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>force-56</td>
<td>Determines whether the network access server uses only the 56 K portion of a channel, even when all 64 K appear to be available.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>map-class</td>
<td>Allows the user profile to reference information configured in a map class of the same name on the network access server that dials out.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>send-auth</td>
<td>Defines the protocol to use (PAP or CHAP) for username-password authentication following CLID authentication.</td>
</tr>
<tr>
<td>Number</td>
<td>Vendor-Specific Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------</td>
<td>-----------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>send-name</td>
<td>PPP name authentication. To apply for PAP, do not configure the <code>ppp pap send-name password</code> command on the interface. For PAP, “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication. For CHAP, “preauth:send-name” will be used not only for outbound authentication, but also for inbound authentication. For a CHAP inbound case, the NAS will use the name defined in “preauth:send-name” in the challenge packet to the caller box.</td>
</tr>
</tbody>
</table>

**Note** The send-name attribute has changed over time: Initially, it performed the functions now provided by both the send-name and remote-name attributes. Because the remote-name attribute has been added, the send-name attribute is restricted to its current behavior.
### Vendor-Specific RADIUS Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>send-secret</td>
<td>PPP password authentication. The vendor-specific attributes (VSAs) “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication. For a CHAP outbound case, both “preauth:send-name” and “preauth:send-secret” will be used in the response packet.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>remote-name</td>
<td>Provides the name of the remote host for use in large-scale dial-out. Dialer checks that the large-scale dial-out remote name matches the authenticated name, to protect against accidental user RADIUS misconfiguration. (For example, dialing a valid phone number but connecting to the wrong device.)</td>
</tr>
</tbody>
</table>

**Miscellaneous Attributes**
<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>2</td>
<td>Cisco-NAS-Port</td>
<td>Specifies additional vendor specific attribute (VSA) information for NAS-Port accounting. To specify additional NAS-Port information in the form an Attribute-Value Pair (AVPair) string, use the <code>radius-server vsa send</code> global configuration command. <strong>Note</strong> This VSA is typically used in Accounting, but may also be used in Authentication (Access-Request) packets.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>min-links</td>
<td>Sets the minimum number of links for MLP.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>proxyacl#&lt;n&gt;</td>
<td>Allows users to configure the downloadable user profiles (dynamic ACLs) by using the authentication proxy feature so that users can have the configured authorization to permit traffic going through the configured interfaces.</td>
</tr>
</tbody>
</table>
### Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the switch 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 switch. You specify the RADIUS host and secret text string by using the `radius server` global configuration commands.

#### Related Topics

- [Configuring the Switch for Vendor-Proprietary RADIUS Server Communication](#), on page 822

---

### How to Configure RADIUS

#### Identifying the RADIUS Server Host

To apply these settings globally to all RADIUS servers communicating with the Switch, use the three unique global configuration commands: `radius-server timeout`, `radius-server retransmit`, and `key string`.

You can configure the Switch to use AAA server groups to group existing server hosts for authentication. For more information, see Related Topics below.
You also need to configure some settings on the RADIUS server. These settings include the IP address of the Switch and the key string to be shared by both the server and the Switch. For more information, see the RADIUS server documentation.

Follow these steps to configure per-server RADIUS server communication.

**Before you begin**

If you configure both global and per-server functions (timeout, retransmission, and key commands) on the switch, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these settings on all RADIUS servers, see Related Topics below.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  Example:  
  Switch> enable |
| **Step 2** configure terminal | Enters global configuration mode.  
  Example:  
  Switch# configure terminal |
| **Step 3** radius server server name |  
  Example:  
  Switch(config)# radius server rsim |
| **Step 4** address \{ipv4 | ipv6\} ip address \{ auth-port port number | acct-port port number\} | (Optional) Specifies the RADIUS server parameters.  
  For auth-port port-number, specify the UDP destination port for authentication requests. The default is 1645. The range is 0 to 65536.  
  For acct-port port-number, specify the UDP destination port for authentication requests. The default is 1646.  
  Example:  
  Switch(config-radius-server)# address ipv4 124.2.2.12 auth-port 1612 |
| **Step 5** key string | (Optional) For key string, specify the authentication and encryption key used between the Switch and the RADIUS daemon running on the RADIUS server.  
  Example:  
  Switch(config-radius-server)# key rad123 |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>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 <code>radius server</code> command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>retransmit <em>value</em></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-radius-server)# retransmit 10</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>timeout <em>seconds</em></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-radius-server)# timeout 60</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-server-tacacs)# exit</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# show running-config</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# copy running-config</td>
</tr>
</tbody>
</table>

(Optional) Specifies the number of times a RADIUS request is resent when the server is not responding or responding slowly. The range is 1 to 100. This setting overrides the `radius-server retransmit` global configuration command setting.

(Optional) Specifies the time interval that the Switch waits for the RADIUS server to reply before sending a request again. The range is 1 to 1000. This setting overrides the `radius-server timeout` global configuration command setting.

Exits the RADIUS server mode and enters the global configuration mode.

Returns to privileged EXEC mode.

Verifies your entries.

(Optional) Saves your entries in the configuration file.
Related Topics
- RADIUS Server Host, on page 796
- Defining AAA Server Groups, on page 815
- Configuring Settings for All RADIUS Servers, on page 820

Configuring RADIUS Login Authentication

Follow these steps to configure RADIUS login authentication:

**Before you begin**

To secure the switch for HTTP access by using AAA methods, you must configure the switch with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>aaa new-model</code></td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>`aaa authentication login {default</td>
<td>list-name} method1 [method2...]`</td>
</tr>
</tbody>
</table>

- 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 ports.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For list-name, specify a character string to name the list you are creating.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>Select one of these methods:</td>
<td></td>
</tr>
<tr>
<td>• enable—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the <code>enable password</code> global configuration command.</td>
<td></td>
</tr>
<tr>
<td>• group radius—Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td>• line—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the <code>password password</code> line configuration command.</td>
<td></td>
</tr>
<tr>
<td>• local—Use the local username database for authentication. You must enter username information in the database. Use the <code>username name password</code> global configuration command.</td>
<td></td>
</tr>
<tr>
<td>• local-case—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the <code>username password</code> global configuration command.</td>
<td></td>
</tr>
<tr>
<td>• none—Do not use any authentication for login.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

| line [console | tty | vty] line-number [ending-line-number] |
|----------------|--------------|
| Enters line configuration mode, and configure the lines to which you want to apply the authentication list. |
### Defining AAA Server Groups

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.

Follow these steps to define AAA server groups:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

---

### Related Topics

- RADIUS Login Authentication, on page 797
- RADIUS Server Host, on page 796

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# line 1 4</code></td>
<td>Applies the authentication list to a line or set of lines.</td>
</tr>
<tr>
<td>`Step 6 login authentication {default</td>
<td>list-name}`</td>
</tr>
<tr>
<td><code>Step 7 end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Step 8 show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>Step 9 copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> radius server name</td>
<td>Specifies the name of the RADIUS server configuration for Protected Access Credential (PAC) provisioning and enters RADIUS server configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# radius server ISE</td>
<td>The switch also supports RADIUS for IPv6.</td>
</tr>
<tr>
<td><strong>Step 4</strong> address {ipv4</td>
<td>ipv6} {ip-address</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> key string</td>
<td>Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-radius-server)# key cisco123</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Exits RADIUS server configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-radius-server)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config</td>
<td></td>
</tr>
</tbody>
</table>
Configuring RADIUS Authorization for User Privileged Access and Network Services

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

Follow these steps to configure RADIUS authorization for user privileged access and network services:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the switch for user RADIUS authorization for all network-related service requests.</td>
</tr>
<tr>
<td><code>aaa authorization network radius</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Switch(config)# aaa authorization network radius</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the switch for user RADIUS authorization if the user has privileged EXEC access. The <strong>exec</strong> keyword might return user profile information (such as <strong>autocommand</strong> information).</td>
</tr>
<tr>
<td><code>aaa authorization exec radius</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>Switch(config)# aaa authorization exec radius</code></td>
<td></td>
</tr>
</tbody>
</table>
Starting RADIUS Accounting

Follow these steps to start RADIUS accounting:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>aaa authorization exec radius local</code></td>
<td>Sets parameters for RADIUS accounting.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# aaa authorization exec radius local</code></td>
<td>Enables RADIUS accounting.</td>
</tr>
</tbody>
</table>

**Example:**
```
Switch(config)# enable
Switch> enable
```
### Command or Action

#### Purpose

| Step 2 | configure terminal
   | Example:
   | Switch# configure terminal |
| ------ | -------------- |
| Enters global configuration mode. |

| Step 3 | aaa accounting network start-stop radius
   | Example:
   | Switch(config)# aaa accounting network start-stop radius |
| ------ | ------------------- |
| Enables RADIUS accounting for all network-related service requests. |

| Step 4 | aaa accounting exec start-stop radius
   | Example:
   | Switch(config)# aaa accounting exec start-stop radius |
| ------ | ------------------- |
| Enables RADIUS accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end. |

| Step 5 | end
   | Example:
   | Switch(config)# end |
| ------ | ------------------- |
| Returns to privileged EXEC mode. |

| Step 6 | show running-config
   | Example:
   | Switch# show running-config |
| ------ | ------------------- |
| Verifies your entries. |

| Step 7 | copy running-config startup-config
   | Example:
   | Switch# copy running-config startup-config |
| ------ | ------------------- |
| (Optional) Saves your entries in the configuration file. |

### Related Topics

- [RADIUS Accounting](#), on page 798

### Establishing a Session with a Router if the AAA Server is Unreachable

The `aaa accounting system guarantee-first` command guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the `no aaa accounting system guarantee-first` command.
# Configuring Settings for All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure settings for all RADIUS servers:

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td><code>radius-server key string</code></td>
<td>Specifies the shared secret text string used between the switch and all RADIUS servers. <strong>Note</strong> 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, do not enclose the key in quotation marks unless the quotation marks are part of the key.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# <code>radius-server key your_server_key</code> Switch(config)# <code>key your_server_key</code></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td><code>radius-server retransmit retries</code></td>
<td>Specifies the number of times the switch sends each RADIUS request to the server before giving up. The default is 3; the range 1 to 1000.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# <code>radius-server retransmit 5</code></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td><code>radius-server timeout seconds</code></td>
<td>Specifies the number of seconds a switch waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1 to 1000.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# <code>radius-server timeout 3</code></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td><code>radius-server deadtime minutes</code></td>
<td>When a RADIUS server is not responding to authentication requests, this command specifies a time to stop the request on that server. This avoids the wait for the request to timeout before trying the next configured server. The default is 0; the range is 1 to 1440 minutes.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# <code>radius-server deadtime 0</code></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Configuring the Switch to Use Vendor-Specific RADIUS Attributes

Follow these steps to configure the switch to use vendor-specific RADIUS attributes:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# radius-server vsa send [accounting</td>
<td>authentication]</td>
</tr>
<tr>
<td>Switch(config)# radius-server vsa send accounting</td>
<td>• (Optional) Use the accounting keyword to limit the set of recognized vendor-specific attributes to only accounting attributes.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Identifying the RADIUS Server Host, on page 810
- RADIUS Server Host, on page 796
### Configuring the Switch for Vendor-Proprietary RADIUS Server Communication

Follow these steps to configure the switch to use vendor-proprietary RADIUS server communication:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enable privileged EXEC mode.</td>
</tr>
<tr>
<td><em>enable</em></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><em>Switch&gt; enable</em></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>configure terminal</em></td>
<td></td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 3** | radius server *server name*  
Example:  
Switch(config)# radius server rsim | Specifies the RADIUS server. |
| **Step 4** | address { ipv4 | ipv6 } ip address  
Example:  
Switch(config-radius-server)# address ipv4 172.24.25.10 | (Optional) Specifies the IP address of the RADIUS server. |
| **Step 5** | non-standard  
Example:  
Switch(config-radius-server)# non-standard | Identifies that the RADIUS server using a vendor-proprietary implementation of RADIUS. |
| **Step 6** | key *string*  
Example:  
Switch(config-radius-server)# key rad123 | Specifies the shared secret text string used between the switch and the vendor-proprietary RADIUS server. The switch and the RADIUS server use this text string to encrypt passwords and exchange responses. |
| **Step 7** | exit  
Example:  
Switch(config-radius-server)# exit | Exits the RADIUS server mode and enters the global configuration mode. |
| **Step 8** | end  
Example:  
Switch(config)# end | Returns to privileged EXEC mode. |
| **Step 9** | show running-config  
Example:  
Switch# show running-config | Verifies your entries. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 10</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td>Example: Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics
Vendor-Proprietary RADIUS Server Communication, on page 810

## Configuring CoA on the Switch

Follow these steps to configure CoA on a switch. This procedure is required.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Example: Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td>Step 4 aaa server radius dynamic-author</td>
<td>Configures the switch as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server.</td>
</tr>
<tr>
<td>Example: Switch(config)# aaa server radius dynamic-author</td>
<td></td>
</tr>
<tr>
<td>Step 5 client {ip-address</td>
<td>name} [vrf vriname] [server-key string]</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 6    | server-key \[0 \mid 7\] string  
   Example:  
   Switch(config-sg-radius)# server-key your_server_key | Configures the RADIUS key to be shared between a device and RADIUS clients. |
| 7    | port port-number  
   Example:  
   Switch(config-sg-radius)# port 25 | Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients. |
| 8    | auth-type \{any \mid all \mid session-key\}  
   Example:  
   Switch(config-sg-radius)# auth-type any | Specifies the type of authorization the switch uses for RADIUS clients.  
   The client must match all the configured attributes for authorization. |
| 9    | ignore session-key | (Optional) Configures the switch to ignore the session-key.  
   For more information about the **ignore** command, see the *Cisco IOS Intelligent Services Gateway Command Reference* on Cisco.com. |
| 10   | ignore server-key  
   Example:  
   Switch(config-sg-radius)# ignore server-key | (Optional) Configures the switch to ignore the server-key.  
   For more information about the **ignore** command, see the *Cisco IOS Intelligent Services Gateway Command Reference* on Cisco.com. |
| 11   | authentication command bounce-port ignore  
   Example:  
   Switch(config-sg-radius)# authentication command bounce-port ignore | (Optional) Configures the switch to ignore a CoA request to temporarily disable the port hosting a session. The purpose of temporarily disabling the port is to trigger a DHCP renegotiation from the host when a VLAN change occurs and there is no supplicant on the endpoint to detect the change. |
| 12   | authentication command disable-port ignore  
   Example:  
   Switch(config-sg-radius)# authentication command disable-port ignore | (Optional) Configures the switch to ignore a nonstandard command requesting that the port hosting a session be administratively shut down. Shutting down the port results in termination of the session.  
   Use standard CLI or SNMP commands to re-enable the port. |
### Configuring RADIUS Server Load Balancing

This feature allows access and authentication requests to be evenly across all RADIUS servers in a server group. For more information, see the “RADIUS Server Load Balancing” chapter of the *Cisco IOS Security Configuration Guide, Release 12.4*.

### Monitoring CoA Functionality

#### Table 59: Privileged EXEC show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show aaa attributes protocol radius</td>
<td>Displays AAA attributes of RADIUS commands.</td>
</tr>
</tbody>
</table>

#### Table 60: Global Troubleshooting Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug radius</td>
<td>Displays information for troubleshooting RADIUS.</td>
</tr>
<tr>
<td>debug aaa coa</td>
<td>Displays information for troubleshooting CoA processing.</td>
</tr>
<tr>
<td>debug aaa pod</td>
<td>Displays information for troubleshooting POD packets.</td>
</tr>
<tr>
<td>debug aaa subsys</td>
<td>Displays information for troubleshooting POD packets.</td>
</tr>
<tr>
<td>debug cmdhd [detail</td>
<td>Displays information for troubleshooting command headers.</td>
</tr>
</tbody>
</table>
For detailed information about the fields in these displays, see the command reference for this release.

**Configuration Examples for Controlling Switch Access with RADIUS**

**Examples: Identifying the RADIUS Server Host**

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

```
Switch(config)# radius server server1
Switch(config)# address ipv4 172.29.36.49 auth-port 1612
Switch(config)# key rad1
Switch(config)# address ipv4 172.20.36.50 acct-port 1618
Switch(config)# key rad2
```

**Example: Using Two Different RADIUS Group Servers**

In this example, the switch is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group 1 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.

```
Switch(config)# radius server server1
Switch(config)# address 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# address 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

**Examples: Configuring the Switch to Use Vendor-Specific RADIUS Attributes**

For example, this AV pair activates Cisco’s *multiple named ip address pools* feature during IP authorization (during PPP IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

This example shows how to provide a user logging in from a switch with immediate access to privileged EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

This example shows how to specify an authorized VLAN in the RADIUS server database:
Example: Configuring the Switch for Vendor-Proprietary RADIUS Server Communication

This example shows how to apply an input ACL in ASCII format to an interface for the duration of this connection:

cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"

This example shows how to apply an output ACL in ASCII format to an interface for the duration of this connection:

cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"

Example: Configuring the Switch for Vendor-Proprietary RADIUS Server Communication

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of rad124 between the switch and the server:

Switch(config)# radius server server1
Switch(config)# address ipv4 172.20.30.15
Switch(config)# non-standard
Switch(config)# key rad124

Additional References for Configuring Secure Shell

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Identity Control policies and Identity Service templates for Session Aware networking.</td>
<td>Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.</td>
<td>Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

Error Message Decoder

| Description                                                                 | Link                                                                                           |
|----------------------------------------------------------------------------|                                                                                                |
| To help you research and resolve system error messages in this release, use the Error Message Decoder tool. | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi                                        |
Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature Information for RADIUS

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS 15.2(1)E</td>
<td>The RADIUS Progress Codes feature adds additional progress codes to RADIUS attribute 196 (Ascend-Connect-Progress), which indicates a connection state before a call is disconnected through progress codes.</td>
</tr>
<tr>
<td>Release</td>
<td>Feature Information</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco IOS 15.2(1)E</td>
<td>The Enhanced Test Command feature allows a named user profile to be created with calling line ID (CLID) or Dialed Number Identification Service (DNIS) attribute values. The CLID or DNIS attribute values can be associated with the RADIUS record that is sent with the user profile so that the RADIUS server can access CLID or DNIS attribute information for all incoming calls. The following commands were introduced or modified: <strong>aaa attribute</strong>, <strong>aaa user profile</strong>, and <strong>test aaa group</strong></td>
</tr>
</tbody>
</table>
Configuring Kerberos

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Controlling Switch Access with Kerberos

The following are the prerequisites for controlling switch access with Kerberos.

- So that remote users can authenticate to network services, you must configure the hosts and the KDC in the Kerberos realm to communicate and mutually authenticate users and network services. To do this, you must identify them to each other. You add entries for the hosts to the Kerberos database on the KDC and add KEYTAB files generated by the KDC to all hosts in the Kerberos realm. You also create entries for the users in the KDC database.

- A Kerberos server can be a switch that is configured as a network security server and that can authenticate users by using the Kerberos protocol.

When you add or create entries for the hosts and users, follow these guidelines:

- The Kerberos principal name must be in all lowercase characters.
Restrictions for Controlling Switch Access with Kerberos

The following lists any restrictions for controlling switch access with Kerberos.

Information about Kerberos

This section provides Kerberos information.

Kerberos and Switch Access

This section describes how to enable and configure the Kerberos security system, which authenticates requests for network resources by using a trusted third party.

Note

In the Kerberos configuration examples, the trusted third party can be any switch that supports Kerberos, that is configured as a network security server, and that can authenticate users by using the Kerberos protocol.

Kerberos Overview

Kerberos is a secret-key network authentication protocol, which was developed at the Massachusetts Institute of Technology (MIT). It uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication and authenticates requests for network resources. Kerberos uses the concept of a trusted third party to perform secure verification of users and services. This trusted third party is called the key distribution center (KDC).

Kerberos verifies that users are who they claim to be and the network services that they use are what the services claim to be. To do this, a KDC or trusted Kerberos server issues tickets to users. These tickets, which have a limited life span, are stored in user credential caches. The Kerberos server uses the tickets instead of user names and passwords to authenticate users and network services.

Note

A Kerberos server can be any switch that is configured as a network security server and that can authenticate users by using the Kerberos protocol.

The Kerberos credential scheme uses a process called single logon. This process authenticates a user once and then allows secure authentication (without encrypting another password) wherever that user credential is accepted.

This software release supports Kerberos 5, which allows organizations that are already using Kerberos 5 to use the same Kerberos authentication database on the KDC that they are already using on their other network hosts (such as UNIX servers and PCs).
Kerberos supports these network services:

- Telnet
- rlogin
- rsh

This table lists the common Kerberos-related terms and definitions.

**Table 61: Kerberos Terms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>A process by which a user or service identifies itself to another service. For example, a client can authenticate to a switch or a switch can authenticate to another switch.</td>
</tr>
<tr>
<td>Authorization</td>
<td>A means by which the switch identifies what privileges the user has in a network or on the switch and what actions the user can perform.</td>
</tr>
<tr>
<td>Credential</td>
<td>A general term that refers to authentication tickets, such as TGTs and service credentials. Kerberos credentials verify the identity of a user or service. If a network service decides to trust the Kerberos server that issued a ticket, it can be used in place of re-entering a username and password. Credentials have a default life span of eight hours.</td>
</tr>
<tr>
<td>Instance</td>
<td>An authorization level label for Kerberos principals. Most Kerberos principals are of the form <code>user@REALM</code> (for example, <a href="mailto:smith@example.com">smith@example.com</a>). A Kerberos principal with a Kerberos instance has the form <code>user/instance@REALM</code> (for example, smith/admin@example.com). The Kerberos instance can be used to specify the authorization level for the user if authentication is successful. The server of each network service might implement and enforce the authorization mappings of Kerberos instances but is not required to do so.</td>
</tr>
<tr>
<td></td>
<td>Note The Kerberos principal and instance names must be in all lowercase characters.</td>
</tr>
<tr>
<td></td>
<td>Note The Kerberos realm name must be in all uppercase characters.</td>
</tr>
<tr>
<td>KDC\textsuperscript{8}</td>
<td>Key distribution center that consists of a Kerberos server and database program that is running on a network host.</td>
</tr>
<tr>
<td>Kerberized</td>
<td>A term that describes applications and services that have been modified to support the Kerberos credential infrastructure.</td>
</tr>
<tr>
<td>Kerberos realm</td>
<td>A domain consisting of users, hosts, and network services that are registered to a Kerberos server. The Kerberos server is trusted to verify the identity of a user or network service to another user or network service.</td>
</tr>
<tr>
<td></td>
<td>Note The Kerberos realm name must be in all uppercase characters.</td>
</tr>
<tr>
<td>Kerberos server</td>
<td>A daemon that is running on a network host. Users and network services register their identity with the Kerberos server. Network services query the Kerberos server to authenticate to other network services.</td>
</tr>
</tbody>
</table>
### Kerberos Operation

A Kerberos server can be a switch that is configured as a network security server and that can authenticate remote users by using the Kerberos protocol. Although you can customize Kerberos in a number of ways, remote users attempting to access network services must pass through three layers of security before they can access network services.

To authenticate to network services by using a switch as a Kerberos server, remote users must follow these steps:

#### Authenticating to a Boundary Switch

This section describes the first layer of security through which a remote user must pass. The user must first authenticate to the boundary switch. This process then occurs:

1. The user opens an un-Kerberized Telnet connection to the boundary switch.
2. The switch prompts the user for a username and password.
3. The switch requests a TGT from the KDC for this user.
4. The KDC sends an encrypted TGT that includes the user identity to the switch.
5. The switch attempts to decrypt the TGT by using the password that the user entered.
   - If the decryption is successful, the user is authenticated to the switch.

#### Term-Definition Table

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEYTAB</td>
<td>A password that a network service shares with the KDC. In Kerberos 5 and later Kerberos versions, the network service authenticates an encrypted service credential by using the KEYTAB to decrypt it. In Kerberos versions earlier than Kerberos 5, KEYTAB is referred to as SRVTAB.</td>
</tr>
<tr>
<td>Principal</td>
<td>Also known as a Kerberos identity, this is who you are or what a service is according to the Kerberos server.</td>
</tr>
<tr>
<td>Note</td>
<td>The Kerberos principal name must be in all lowercase characters.</td>
</tr>
<tr>
<td>Service</td>
<td>A credential for a network service. When issued from the KDC, this credential is encrypted with the password shared by the network service and the KDC. The password is also shared with the user TGT.</td>
</tr>
<tr>
<td>credential</td>
<td></td>
</tr>
<tr>
<td>SRVTAB</td>
<td>A password that a network service shares with the KDC. In Kerberos 5 or later Kerberos versions, SRVTAB is referred to as KEYTAB.</td>
</tr>
<tr>
<td>TGT</td>
<td>Ticket granting ticket that is a credential that the KDC issues to authenticated users. When users receive a TGT, they can authenticate to network services within the Kerberos realm represented by the KDC.</td>
</tr>
</tbody>
</table>

---

7 ticket granting ticket  
8 key distribution center  
9 key table  
10 server table
• If the decryption is not successful, the user repeats Step 2 either by re-entering the username and password (noting if Caps Lock or Num Lock is on or off) or by entering a different username and password.

A remote user who initiates a un-Kerberized Telnet session and authenticates to a boundary switch is inside the firewall, but the user must still authenticate directly to the KDC before getting access to the network services. The user must authenticate to the KDC because the TGT that the KDC issues is stored on the switch and cannot be used for additional authentication until the user logs on to the switch.

**Obtaining a TGT from a KDC**

This section describes the second layer of security through which a remote user must pass. The user must now authenticate to a KDC and obtain a TGT from the KDC to access network services.

For instructions about how to authenticate to a KDC, see the “Obtaining a TGT from a KDC” section in the “Security Server Protocols” chapter of the *Cisco IOS Security Configuration Guide, Release 12.4*.

**Authenticating to Network Services**

This section describes the third layer of security through which a remote user must pass. The user with a TGT must now authenticate to the network services in a Kerberos realm.

For instructions about how to authenticate to a network service, see the “Authenticating to Network Services” section in the “Security Server Protocols” chapter of the *Cisco IOS Security Configuration Guide, Release 12.4*.

**How to Configure Kerberos**

To set up a Kerberos-authenticated server-client system, follow these steps:

• Configure the KDC by using Kerberos commands.

• Configure the switch to use the Kerberos protocol.

**Monitoring the Kerberos Configuration**

To display the Kerberos configuration, use the following commands:

• **show running-config**
• **show kerberos creds**: Lists the credentials in a current user’s credentials cache.
• **clear kerberos creds**: Destroys all credentials in a current user’s credentials cache, including those forwarded.
Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos Commands</td>
<td>Cisco IOS Security Command Reference</td>
</tr>
</tbody>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature Information for Kerberos

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring Local Authentication and Authorization

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

How to Configure Local Authentication and Authorization

Configuring the Switch for Local Authentication and Authorization

You can configure AAA to operate without a server by setting the switch to implement AAA in local mode. The switch then handles authentication and authorization. No accounting is available in this configuration.

Note

To secure the switch for HTTP access by using AAA methods, you must configure the switch with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

Follow these steps to configure AAA to operate without a server by setting the switch to implement AAA in local mode:
## Configuring the Switch for Local Authentication and Authorization

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
  **Example:**  
  `Switch> enable`  
  - Enter your password if prompted. |
| Step 2 | `configure terminal` | Enters global configuration mode.  
  **Example:**  
  `Switch# configure terminal` |
| Step 3 | `aaa new-model` | Enables AAA.  
  **Example:**  
  `Switch(config)# aaa new-model` |
| Step 4 | `aaa authentication login default local` | Sets the login authentication to use the local username database. The `default` keyword applies the local user database authentication to all ports.  
  **Example:**  
  `Switch(config)# aaa authentication login default local` |
| Step 5 | `aaa authorization exec default local` | Configures user AAA authorization, check the local database, and allow the user to run an EXEC shell.  
  **Example:**  
  `Switch(config)# aaa authorization exec default local` |
| Step 6 | `aaa authorization network default local` | Configures user AAA authorization for all network-related service requests.  
  **Example:**  
  `Switch(config)# aaa authorization network default local` |
| Step 7 | `username name [privilege level] {password encryption-type password}` | Enters the local database, and establishes a username-based authentication system.  
  **Example:**  
  `Switch(config)# username your_user_name privilege 1 password 7 secret567`  
  - For `name`, specify the user ID as one word. Spaces and quotation marks are not allowed. |
### Command or Action

<table>
<thead>
<tr>
<th></th>
<th>Purpose</th>
</tr>
</thead>
</table>
| | • (Optional) For *level*, specify the privilege level the user has after gaining access. The range is 0 to 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 switch. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the *username* command. |

### Step 8

**end**

**Example:**

```
Switch(config)# end
```

Returns to privileged EXEC mode.

### Step 9

**show running-config**

**Example:**

```
Switch# show running-config
```

Verifies your entries.

### Step 10

**copy running-config startup-config**

**Example:**

```
Switch# copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

### Related Topics

- SSH Servers, Integrated Clients, and Supported Versions, on page 843
- TACACS+ and Switch Access, on page 771
- RADIUS and Switch Access, on page 787
- Setting Up the Switch to Run SSH, on page 845
- SSH Configuration Guidelines, on page 843
Monitoring Local Authentication and Authorization

To display Local Authentication and Authorization configuration, use the `show running-config` privileged EXEC command.

Additional References

**Error Message Decoder**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature Information for Local Authentication and Authorization

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 46

Configuring Secure Shell (SSH)

- Finding Feature Information, on page 841
- Prerequisites for Configuring Secure Shell, on page 841
- Restrictions for Configuring Secure Shell, on page 842
- Information About Configuring Secure Shell, on page 842
- How to Configure SSH, on page 845
- Monitoring the SSH Configuration and Status, on page 848
- Additional References for Configuring Secure Shell, on page 849
- Feature Information for Configuring Secure Shell, on page 850

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Secure Shell

The following are the prerequisites for configuring the switch for secure shell (SSH):

- For SSH to work, the switch needs an Rivest, Shamir, and Adleman (RSA) public/private key pair. This is the same with Secure Copy Protocol (SCP), which relies on SSH for its secure transport.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.

- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

- SCP relies on SSH for security.

- SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.
Restrictions for Configuring Secure Shell

The following are restrictions for configuring the Switch for secure shell.

- The switch supports Rivest, Shamir, and Adelman (RSA) authentication.
- SSH supports only the execution-shell application.
- The SSH server and the SSH client are supported only on Data Encryption Standard (DES) (56-bit) and 3DES (168-bit) data encryption software. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- The Switch supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.
- When using SCP, you cannot enter the password into the `copy` command. You must enter the password when prompted.
- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2.
- The `-l` keyword and userid : {number} {ip-address} delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.

Information About Configuring Secure Shell

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

SSH and Switch Access

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).
SSH functions the same in IPv6 as in IPv4. For IPv6, SSH supports IPv6 addresses and enables secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

**SSH Servers, Integrated Clients, and Supported Versions**

The Secure Shell (SSH) Integrated Client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco device to make a secure, encrypted connection to another Cisco device or to any other device running the SSH server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an unsecured network.

The SSH server and SSH integrated client are applications that run on the switch. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), 3DES, and password authentication.

The switch supports an SSHv1 or an SSHv2 server.

The switch supports an SSHv1 client.

---

**Note**

The SSH client functionality is available only when the SSH server is enabled.

User authentication is performed like that in the Telnet session to the device. SSH also supports the following user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization

**Related Topics**

- Configuring the Switch for Local Authentication and Authorization, on page 837
- TACACS+ and Switch Access, on page 771
- RADIUS and Switch Access, on page 787

**SSH Configuration Guidelines**

Follow these guidelines when configuring the switch as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If the SSH server is running on a stack master and the stack master fails, the new stack master uses the RSA key pair generated by the previous stack master.
- If you get CLI error messages after entering the `crypto key generate rsa` global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the `crypto key generate rsa` command. For more information, see Related Topics below.
- When generating the RSA key pair, the message No host name specified might appear. If it does, you must configure a hostname by using the `hostname` global configuration command.
When generating the RSA key pair, the message No domain specified might appear. If it does, you must configure an IP domain name by using the `ip domain-name` global configuration command.

When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

Related Topics
- Setting Up the Switch to Run SSH, on page 845
- Configuring the Switch for Local Authentication and Authorization, on page 837

Secure Copy Protocol Overview

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

For SSH to work, the switch needs an RSA public/private key pair. This is the same with SCP, which relies on SSH for its secure transport.

Because SSH also relies on AAA authentication, and SCP relies further on AAA authorization, correct configuration is necessary.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

Note
When using SCP, you cannot enter the password into the copy command. You must enter the password when prompted.

Secure Copy Protocol

Isn't Secure Copy Protocol related closely enough to SSH that it could be used in this book? I have moved all of the item in this topic to prerequisites or restrictions.

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. SCP also requires that authentication, authorization, and accounting (AAA) authorization be configured so the switch can determine whether the user has the correct privilege level. To configure the Secure Copy feature, you should understand the SCP concepts.

Related Topics
- Prerequisites for Configuring Secure Shell, on page 841
- Restrictions for Configuring Secure Shell, on page 842
# How to Configure SSH

## Setting Up the Switch to Run SSH

Follow these steps to set up your Switch to run SSH:

### Before you begin

Configure user authentication for local or remote access. This step is required. For more information, see Related Topics below.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt;</code> <code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt;</code> <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>hostname hostname</code></td>
<td>Configures a hostname and IP domain name for your Switch.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# hostname your_hostname</code></td>
<td><strong>Note</strong> Follow this procedure only if you are configuring the Switch as an SSH server.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>ip domain-name domain_name</code></td>
<td>Configures a host domain for your Switch.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# ip domain-name your_domain</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>crypto key generate rsa</code></td>
<td>Enables the SSH server for local and remote authentication on the Switch and generates an RSA key pair. Generating an RSA key pair for the Switch automatically enables SSH. We recommend that a minimum modulus size of 1024 bits.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# crypto key generate rsa</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring the SSH Server

Follow these steps to configure the SSH server:

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Configuring the SSH Server

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch&gt; enable</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

#### Step 2
**configure terminal**

**Example:**

```bash
Switch# configure terminal
```

(Optional) Configures the Switch to run SSH Version 1 or SSH Version 2.

**Example:**

- **1**—Configure the Switch to run SSH Version 1.
  ```bash
  Switch(config)# ip ssh version 1
  ```
- **2**—Configure the Switch to run SSH Version 2.
  ```bash
  Switch(config)# ip ssh version 2
  ```

If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.

#### Step 3
**ip ssh version [1 | 2]**

**Example:**

```bash
Switch(config)# ip ssh version 1
```

#### Step 4
**ip ssh {timeout seconds | authentication-retries number}**

**Example:**

```bash
Switch(config)# ip ssh timeout 90
```

Configures the SSH control parameters:

- Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the Switch uses the default time-out values of the CLI-based sessions.

  By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session time-out value returns to the default of 10 minutes.

  - Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5.

Repeat this step when configuring both parameters.

#### Step 5
**Use one or both of the following:**

- **line**
  ```bash
  vty line_number[ending_line_number]
  ```

(Optional) Configures the virtual terminal line settings.
### Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

**Table 62: Commands for Displaying the SSH Server Configuration and Status**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ssh</td>
<td>Shows the version and configuration information for the SSH server.</td>
</tr>
<tr>
<td>show ssh</td>
<td>Shows the status of the SSH server.</td>
</tr>
</tbody>
</table>
Additional References for Configuring Secure Shell

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Identity Control policies and Identity Service templates for Session Aware networking.</td>
<td>Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.</td>
<td>Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
Feature Information for Configuring Secure Shell

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS 15.2(1)E</td>
<td>The Reverse SSH Enhancements feature, which is supported for SSH Version 1 and 2, provides an alternative way to configure reverse Secure Shell (SSH) so that separate lines do not need to be configured for every terminal or auxiliary line on which SSH must be enabled. This feature also eliminates the rotary-group limitation. This feature was supported on CAT4500-X, CAT4500E-SUP6E, CAT4500E-SUP6L-E, CAT4500E-SUP7E, CAT4500E-SUP7L-E. The following command was introduced: <code>ssh</code>.</td>
</tr>
</tbody>
</table>
CHAPTER 47

Configuring Secure Socket Layer HTTP

- Finding Feature Information, on page 851
- Information about Secure Sockets Layer (SSL) HTTP, on page 851
- How to Configure Secure HTTP Servers and Clients, on page 855
- Monitoring Secure HTTP Server and Client Status, on page 861
- Additional References for Configuring Secure Shell, on page 862
- Feature Information for Secure Socket Layer HTTP, on page 863

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information about Secure Sockets Layer (SSL) HTTP

Secure HTTP Servers and Clients Overview

On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP with SSL encryption provides a secure connection to allow such functions as configuring a switch from a Web browser. Cisco's implementation of the secure HTTP server and secure HTTP client uses an implementation of SSL Version 3.0 with application-layer encryption. HTTP over SSL is abbreviated as HTTPS; the URL of a secure connection begins with https:// instead of http://.

Note

SSL evolved into Transport Layer Security (TLS) in 1999, but is still used in this particular context.

The primary role of the HTTP secure server (the switch) is to listen for HTTPS requests on a designated port (the default HTTPS port is 443) and pass the request to the HTTP 1.1 Web server. The HTTP 1.1 server
processes requests and passes responses (pages) back to the HTTP secure server, which, in turn, responds to the original request.

The primary role of the HTTP secure client (the web browser) is to respond to Cisco IOS application requests for HTTPS User Agent services, perform HTTPS User Agent services for the application, and pass the response back to the application.

BEGINNING WITH CISCO IOS XE DENALI 16.3.1, SUPPORT FOR ATTACHING IPv6 ACL TO THE HTTP SERVER HAS BEEN ENABLED. PRIOR TO CISCO IOS XE DENALI 16.3.1, ONLY IPv4 ACL SUPPORT WAS AVAILABLE FOR CONFIGURING THE SECURE HTTP SERVER. YOU CAN ATTACH THE PRECONFIGURED IPv6 AND IPv4 ACLS TO THE HTTP SERVER USING THE CONFIGURATION CLI FOR THE SECURE HTTP SERVER.

Certificate Authority Trustpoints

Certificate authorities (CAs) manage certificate requests and issue certificates to participating network devices. These services provide centralized security key and certificate management for the participating devices. Specific CA servers are referred to as trustpoints.

When a connection attempt is made, the HTTPS server provides a secure connection by issuing a certified X.509v3 certificate, obtained from a specified CA trustpoint, to the client. The client (usually a Web browser), in turn, has a public key that allows it to authenticate the certificate.

For secure HTTP connections, we highly recommend that you configure a CA trustpoint. If a CA trustpoint is not configured for the device running the HTTPS server, the server certifies itself and generates the needed RSA key pair. Because a self-certified (self-signed) certificate does not provide adequate security, the connecting client generates a notification that the certificate is self-certified, and the user has the opportunity to accept or reject the connection. This option is useful for internal network topologies (such as testing).

If you do not configure a CA trustpoint, when you enable a secure HTTP connection, either a temporary or a persistent self-signed certificate for the secure HTTP server (or client) is automatically generated.

- If the switch is not configured with a hostname and a domain name, a temporary self-signed certificate is generated. If the switch reboots, any temporary self-signed certificate is lost, and a new temporary new self-signed certificate is assigned.
- If the switch has been configured with a host and domain name, a persistent self-signed certificate is generated. This certificate remains active if you reboot the switch or if you disable the secure HTTP server so that it will be there the next time you re-enable a secure HTTP connection.

THE CERTIFICATE AUTHORITIES AND TRUSTPOINTS MUST BE CONFIGURED ON EACH DEVICE INDIVIDUALLY. COPYING THEM FROM OTHER DEVICES MAKES THEM INVALID ON THE SWITCH.

When a new certificate is enrolled, the new configuration change is not applied to the HTTPS server until the server is restarted. You can restart the server using either the CLI or by physical reboot. On restarting the server, the switch starts using the new certificate.

IF A SELF-SIGNED CERTIFICATE HAS BEEN GENERATED, THIS INFORMATION IS INCLUDED IN THE OUTPUT OF THE SHOW running-config PRIVILEGED EXEC COMMAND. THIS IS A PARTIAL SAMPLE OUTPUT FROM THAT COMMAND DISPLAYING A SELF-SIGNED CERTIFICATE.
Switch# show running-config
Building configuration...

<output truncated>
crypto pki trustpoint TP-self-signed-3080755072
    enrollment selfsigned
    subject-name cn=IOS-Self-Signed-Certificate-3080755072
    revocation-check none
    rsakeypair TP-self-signed-3080755072
! 
crypto ca certificate chain TP-self-signed-3080755072
    certificate self-signed 01
    3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
    59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
    69666963 61746966 303595A17 0D323030 31303130 30303030 35395A17 0D323030
    31303130 30303030 305A3059 312F302D
</output truncated>

You can remove this self-signed certificate by disabling the secure HTTP server and entering the no crypto pki trustpoint TP-self-signed-3080755072 global configuration command. If you later re-enable a secure HTTP server, a new self-signed certificate is generated.

---

**Note**

The values that follow *TP self-signed* depend on the serial number of the device.

You can use an optional command (**ip http secure-client-auth**) to allow the HTTPS server to request an X.509v3 certificate from the client. Authenticating the client provides more security than server authentication by itself.

---

**CipherSuites**

A CipherSuite specifies the encryption algorithm and the digest algorithm to use on a SSL connection. When connecting to the HTTPS server, the client Web browser offers a list of supported CipherSuites, and the client and server negotiate the best encryption algorithm to use from those on the list that are supported by both. For example, Netscape Communicator 4.76 supports U.S. security with RSA Public Key Cryptography, MD2, MD5, RC2-CBC, RC4, DES-CBC, and DES-EDE3-CBC.

For the best possible encryption, you should use a client browser that supports 128-bit encryption, such as Microsoft Internet Explorer Version 5.5 (or later) or Netscape Communicator Version 4.76 (or later). The SSL_RSA_WITH_DES_CBC_SHA CipherSuite provides less security than the other CipherSuites, as it does not offer 128-bit encryption.

The more secure and more complex CipherSuites require slightly more processing time. This list defines the CipherSuites supported by the switch and ranks them from fastest to slowest in terms of router processing load (speed):

1. SSL_RSA_WITH_DES_CBC_SHA—RSA key exchange (RSA Public Key Cryptography) with DES-CBC for message encryption and SHA for message digest
2. SSL_RSA_WITH_NULL_SHA key exchange with NULL for message encryption and SHA for message digest (only for SSL 3.0).
3. SSL_RSA_WITH_NULL_MD5 key exchange with NULL for message encryption and MD5 for message digest (only for SSL 3.0).
4. SSL_RSA_WITH_RC4_128_MD5—RSA key exchange with RC4 128-bit encryption and MD5 for message digest
5. SSL_RSA_WITH_RC4_128_SHA—RSA key exchange with RC4 128-bit encryption and SHA for message digest
6. SSL_RSA_WITH_3DES_EDE_CBC_SHA—RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest
7. SSL_RSA_WITH_AES_128_CBC_SHA—RSA key exchange with AES 128-bit encryption and SHA for message digest
8. SSL_RSA_WITH_AES_256_CBC_SHA—RSA key exchange with AES 256-bit encryption and SHA for message digest (only for SSL 3.0).
9. SSL_RSA_WITH_DHE_AES_128_CBC_SHA—RSA key exchange with AES 128-bit encryption and SHA for message digest (only for SSL 3.0).
10. SSL_RSA_WITH_DHE_AES_256_CBC_SHA—RSA key exchange with AES 256-bit encryption and SHA for message digest (only for SSL 3.0).

---

**Note**
The latest versions of Chrome do not support the four original cipher suites, thus disallowing access to both web GUI and guest portals.

RSA (in conjunction with the specified encryption and digest algorithm combinations) is used for both key generation and authentication on SSL connections. This usage is independent of whether or not a CA trustpoint is configured.

### Default SSL Configuration

The standard HTTP server is enabled.
SSL is enabled.
No CA trustpoints are configured.
No self-signed certificates are generated.

### SSL Configuration Guidelines

When SSL is used in a switch cluster, the SSL session terminates at the cluster commander. Cluster member switches must run standard HTTP.

Before you configure a CA trustpoint, you should ensure that the system clock is set. If the clock is not set, the certificate is rejected due to an incorrect date.

In a switch stack, the SSL session terminates at the stack master.
How to Configure Secure HTTP Servers and Clients

Configuring a CA Trustpoint

For secure HTTP connections, we recommend that you configure an official CA trustpoint. A CA trustpoint is more secure than a self-signed certificate.

Beginning in privileged EXEC mode, follow these steps to configure a CA Trustpoint:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>hostname hostname</td>
<td>Specifies the hostname of the switch (required only if you have not previously configured a hostname). The hostname is required for security keys and certificates.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# hostname your_hostname</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip domain-name domain-name</td>
<td>Specifies the IP domain name of the switch (required only if you have not previously configured an IP domain name). The domain name is required for security keys and certificates.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# ip domain-name your_domain</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>crypto key generate rsa</td>
<td>(Optional) Generates an RSA key pair. RSA key pairs are required before you can obtain a certificate for the switch. RSA key pairs are generated automatically. You can use this command to regenerate the keys, if needed.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# crypto key generate rsa</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>crypto ca trustpoint name</td>
<td>Specifies a local configuration name for the CA trustpoint and enter CA trustpoint configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# crypto ca trustpoint your_trustpoint</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>enrollment url url</td>
<td>Specifies the URL to which the switch should send certificate requests.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

---

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
### Configuring a CA Trustpoint

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 7**

```bash
Switch(ca-trustpoint)# enrollment http-proxy
http://your_server:80
```

(Optional) Configures the switch to obtain certificates from the CA through an HTTP proxy server.

- For `host-name`, specify the proxy server used to get the CA.
- For `port-number`, specify the port number used to access the CA.

| **Step 8**

```bash
Switch(ca-trustpoint)# crl query
ldap://your_host:49
```

Configures the switch to request a certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.

| **Step 9**

```bash
Switch(ca-trustpoint)# primary
your_trustpoint
```

(Optional) Specifies that the trustpoint should be used as the primary (default) trustpoint for CA requests.

- For `name`, specify the trustpoint that you just configured.

| **Step 10**

```bash
Switch(ca-trustpoint)# exit
```

Exits CA trustpoint configuration mode and return to global configuration mode.

| **Step 11**

```bash
Switch(config)# crypto ca authentication
your_trustpoint
```

Authenticates the CA by getting the public key of the CA. Use the same name used in Step 5.

| **Step 12**

```bash
Switch(config)# crypto ca enroll
your_trustpoint
```

Obtains the certificate from the specified CA trustpoint. This command requests a signed certificate for each RSA key pair.

| **Step 13**

```bash
Switch(config)# end
```

Returns to privileged EXEC mode.
Configuring the Secure HTTP Server

Beginning in privileged EXEC mode, follow these steps to configure a secure HTTP server:

Before you begin

If you are using a certificate authority for certification, you should use the previous procedure to configure the CA trustpoint on the switch before enabling the HTTP server. If you have not configured a CA trustpoint, a self-signed certificate is generated the first time that you enable the secure HTTP server. After you have configured the server, you can configure options (path, access list to apply, maximum number of connections, or timeout policy) that apply to both standard and secure HTTP servers.

To verify the secure HTTP connection by using a Web browser, enter https://URL, where the URL is the IP address or hostname of the server switch. If you configure a port other than the default port, you must also specify the port number after the URL. For example:

https://209.165.129:1026

or

https://host.domain.com:1026

The existing `ip http access-class access-list-number` command for specifying the access-list (Only IPv4 ACLs) is going to be deprecated. You can still use this command to specify an access list to allow access to the HTTP server. Two new commands have been introduced to enable support for specifying IPv4 and IPv6 ACLs. These are `ip http access-class ipv4 access-list-name | access-list-number` for specifying IPv4 ACLs and `ip http access-class ipv6 access-list-name` for specifying IPv6 ACLs. We recommend using the new CLI to avoid receiving warning messages.

Note the following considerations for specifying access-lists:

- If you specify an access-list that does not exist, the configuration takes place but you receive the below warning message:

  ACL being attached does not exist, please configure it

- If you use the `ip http access-class` command for specifying an access-list for the HTTP server, the below warning message appears:

  This CLI will be deprecated soon, Please use new CLI `ip http access-class ipv4/ipv6 <access-list-name>| <access-list-number>

- If you use `ip http access-class ipv4 access-list-name | access-list-number` or `ip http access-class ipv6 access-list-name`, and an access-list was already configured using `ip http access-class`, the below warning message appears:

  Removing ip http access-class <access-list-number>

`ip http access-class access-list-number` and `ip http access-class ipv4 access-list-name | access-list-number` share the same functionality. Each command overrides the configuration of the previous command. The
following combinations between the configuration of the two commands explain the effect on the running configuration:

- If `ip http access-class access-list-number` is already configured and you try to configure using `ip http access-class ipv4 access-list-number` command, the configuration of `ip http access-class access-list-number` will be removed and the configuration of `ip http access-class ipv4 access-list-number` will be added to the running configuration.

- If `ip http access-class access-list-number` is already configured and you try to configure using `ip http access-class ipv4 access-list-name` command, the configuration of `ip http access-class access-list-number` will be removed and the configuration of `ip http access-class ipv4 access-list-name` will be added to the running configuration.

- If `ip http access-class ipv4 access-list-number` is already configured and you try to configure using `ip http access-class access-list-name`, the configuration of `ip http access-class ipv4 access-list-number` will be removed from configuration and the configuration of `ip http access-class access-list-name` will be added to the running configuration.

- If `ip http access-class ipv4 access-list-name` is already configured and you try to configure using `ip http access-class access-list-number`, the configuration of `ip http access-class ipv4 access-list-name` will be removed from the configuration and the configuration of `ip http access-class access-list-number` will be added to the running configuration.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>show ip http server status</code></td>
<td>(Optional) Displays the status of the HTTP server to determine if the secure HTTP server feature is supported in the software. You should see one of these lines in the output: HTTP secure server capability: Present or HTTP secure server capability: Not present</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch# show ip http server status</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip http secure-server</code></td>
<td>Enables the HTTPS server if it has been disabled. The HTTPS server is enabled by default.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# ip http secure-server</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>4</td>
<td><code>ip http secure-port port-number</code>&lt;br&gt;Example: <code>Switch(config)# ip http secure-port 443</code></td>
<td>(Optional) Specifies the port number to be used for the HTTPS server. The default port number is 443. Valid options are 443 or any number in the range 1025 to 65535.</td>
</tr>
<tr>
<td>5</td>
<td><code>ip http secure-ciphersuite</code>&lt;br&gt;{<code>3des-ede-cbc-sha</code>}&lt;br&gt;{<code>rc4-128-md5</code>}&lt;br&gt;{<code>rc4-128-sha</code>}&lt;br&gt;{<code>des-cbc-sha</code>}&lt;br&gt;Example: <code>Switch(config)# ip http secure-ciphersuite rc4-128-md5</code></td>
<td>(Optional) Specifies the CipherSuites (encryption algorithms) to be used for encryption over the HTTPS connection. If you do not have a reason to specify a particularly CipherSuite, you should allow the server and client to negotiate a CipherSuite that they both support. This is the default.</td>
</tr>
<tr>
<td>6</td>
<td><code>ip http secure-client-auth</code>&lt;br&gt;Example: <code>Switch(config)# ip http secure-client-auth</code></td>
<td>(Optional) Configures the HTTP server to request an X.509v3 certificate from the client for authentication during the connection process. The default is for the client to request a certificate from the server, but the server does not attempt to authenticate the client.</td>
</tr>
<tr>
<td>7</td>
<td><code>ip http secure-trustpoint name</code>&lt;br&gt;Example: <code>Switch(config)# ip http secure-trustpoint your_trustpoint</code></td>
<td>Specifies the CA trustpoint to use to get an X.509v3 security certificate and to authenticate the client certificate connection. <strong>Note</strong> Use of this command assumes you have already configured a CA trustpoint according to the previous procedure.</td>
</tr>
<tr>
<td>8</td>
<td><code>ip http path path-name</code>&lt;br&gt;Example: <code>Switch(config)# ip http path /your_server:80</code></td>
<td>(Optional) Sets a base HTTP path for HTML files. The path specifies the location of the HTTP server files on the local system (usually located in system flash memory).</td>
</tr>
<tr>
<td>9</td>
<td><code>ip http access-class access-list-number</code>&lt;br&gt;Example: <code>Switch(config)# ip http access-class 2</code></td>
<td>(Optional) Specifies an access list to use to allow access to the HTTP server.</td>
</tr>
<tr>
<td>10</td>
<td>`ip http access-class { ipv4 {access-list-number}</td>
<td>access-list-name}</td>
</tr>
</tbody>
</table>
### Configuring the Secure HTTP Client

Beginning in privileged EXEC mode, follow these steps to configure a secure HTTP client:

**Before you begin**

The standard HTTP client and secure HTTP client are always enabled. A certificate authority is required for secure HTTP client certification. This procedure assumes that you have previously configured a CA trustpoint on the switch. If a CA trustpoint is not configured and the remote HTTPS server requires client authentication, connections to the secure HTTP client fail.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# ip http access-class ipv4 4</td>
<td>(Optional) Sets the maximum number of concurrent connections that are allowed to the HTTP server. We recommend that the value be at least 10 and not less. This is required for the UI to function as expected.</td>
</tr>
<tr>
<td><strong>Step 11</strong> ip http max-connections value</td>
<td>(Optional) Specifies how long a connection to the HTTP server can remain open under the defined circumstances:</td>
</tr>
</tbody>
</table>
| Example: Switch(config)# ip http max-connections 4 | • *idle*—the maximum time period when no data is received or response data cannot be sent. The range is 1 to 600 seconds. The default is 180 seconds (3 minutes).
• *life*—the maximum time period from the time that the connection is established. The range is 1 to 86400 seconds (24 hours). The default is 180 seconds.
• *requests*—the maximum number of requests processed on a persistent connection. The maximum value is 86400. The default is 1. |
| **Step 12** ip http timeout-policy idle *seconds* life *seconds* requests *value* | Example: Switch(config)# ip http timeout-policy idle 120 life 240 requests 1 |
| **Step 13** end | Returns to privileged EXEC mode. |
| Example: Switch(config)# end | |
Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ip http client secure-trustpoint name</td>
<td>(Optional) Specifies the CA trustpoint to be used if the remote HTTP server requests client authentication. Using this command assumes that you have already configured a CA trustpoint by using the previous procedure. The command is optional if client authentication is not needed or if a primary trustpoint has been configured.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip http client secure-trustpoint your_trustpoint</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip http client secure-ciphersuite {3des-ede-cbc-sha} [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}</td>
<td>(Optional) Specifies the CipherSuites (encryption algorithms) to be used for encryption over the HTTPS connection. If you do not have a reason to specify a particular CipherSuite, you should allow the server and client to negotiate a CipherSuite that they both support. This is the default.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip http client secure-ciphersuite rc4-128-md5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Monitoring Secure HTTP Server and Client Status

To monitor the SSL secure server and client status, use the privileged EXEC commands in the following table.

Table 63: Commands for Displaying the SSL Secure Server and Client Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip http client secure status</td>
<td>Shows the HTTP secure client configuration.</td>
</tr>
<tr>
<td>show ip http server secure status</td>
<td>Shows the HTTP secure server configuration.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Shows the generated self-signed certificate for secure HTTP connections.</td>
</tr>
</tbody>
</table>
# Additional References for Configuring Secure Shell

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Identity Control policies and Identity Service templates for Session Aware networking.</td>
<td>Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.</td>
<td>Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

## Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

## Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
# Feature Information for Secure Socket Layer HTTP

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
IPv4 ACLs

- Finding Feature Information, on page 865
- Prerequisites for Configuring IPv4 Access Control Lists, on page 865
- Restrictions for Configuring IPv4 Access Control Lists, on page 865
- Information about Network Security with ACLs, on page 867
- How to Configure ACLs, on page 879
- Monitoring IPv4 ACLs, on page 900
- Configuration Examples for ACLs, on page 901
- Additional References, on page 916
- Feature Information for IPv4 Access Control Lists, on page 916

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring IPv4 Access Control Lists

This section lists the prerequisites for configuring network security with access control lists (ACLs).

- On switches running the LAN base feature set, VLAN maps are not supported.

Restrictions for Configuring IPv4 Access Control Lists

General Network Security

The following are restrictions for configuring network security with ACLs:
• Not all commands that accept a numbered ACL accept a named ACL. ACLs for packet filters and route filters on interfaces can use a name.

• A standard ACL and an extended ACL cannot have the same name.

• Though visible in the command-line help strings, **appletalk** is not supported as a matching condition for the **deny** and **permit** MAC access-list configuration mode commands.

• ACL wildcard is not supported in downstream client policy.

### IPv4 ACL Network Interfaces

The following restrictions apply to IPv4 ACLs to network interfaces:

• When controlling access to an interface, you can use a named or numbered ACL.

• If you apply an ACL to a Layer 2 interface that is a member of a VLAN, the Layer 2 (port) ACL takes precedence over an input Layer 3 ACL applied to the VLAN interface or a VLAN map applied to the VLAN.

• If you apply an ACL to a Layer 3 interface and routing is not enabled on the switch, the ACL only filters packets that are intended for the CPU, such as SNMP, Telnet, or web traffic.

• If the **preauth_ipv4_acl** ACL is configured to filter packets, the ACL is removed after authentication.

• You do not have to enable routing to apply ACLs to Layer 2 interfaces.

---

**Note**

By default, the router sends Internet Control Message Protocol (ICMP) unreachable messages when a packet is denied by an access group on a Layer 3 interface. These access-group denied packets are not dropped in hardware but are bridged to the switch CPU so that it can generate the ICMP-unreachable message. They do not generate ICMP unreachable messages. ICMP unreachable messages can be disabled on router ACLs with the **no ip unreachables** interface command.

---

**MAC ACLs on a Layer 2 Interface**

After you create a MAC ACL, you can apply it to a Layer 2 interface to filter non-IP traffic coming in that interface. When you apply the MAC ACL, consider these guidelines:

• You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface. The IP access list filters only IP packets, and the MAC access list filters non-IP packets.

• A Layer 2 interface can have only one MAC access list. If you apply a MAC access list to a Layer 2 interface that has a MAC ACL configured, the new ACL replaces the previously configured one.

---

**Note**

The **mac access-group** interface configuration command is only valid when applied to a physical Layer 2 interface. You cannot use the command on EtherChannel port channels.

---

**IP Access List Entry Sequence Numbering**

• This feature does not support dynamic, reflexive, or firewall access lists.
Information about Network Security with ACLs

This chapter describes how to configure network security on the switch by using access control lists (ACLs), which in commands and tables are also referred to as access lists.

Cisco TrustSec and ACLs

Catalyst 3850 switches running the IP base or IP services feature set also support Cisco TrustSec Security Group Tag (SCT) Exchange Protocol (SXP). This feature supports security group access control lists (SGACLs), which define ACL policies for a group of devices instead of an IP address. The SXP control protocol allows tagging packets with SCTs without a hardware upgrade, and runs between access layer devices at the Cisco TrustSec domain edge and distribution layer devices within the Cisco TrustSec domain. Catalyst 3850 switches operate as access layer switches in the Cisco TrustSec network.

The sections on SXP define the capabilities supported on the Catalyst 3850 switches.

ACL Overview

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs filter traffic as it passes through a router or switch and permit or deny packets crossing specified interfaces or VLANs. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. One by one, it tests packets against the conditions in an access list. The first match decides whether the switch accepts or rejects the packets. Because the switch stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packet. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet. The switch can use ACLs on all packets it forwards, including packets bridged within a VLAN.

You configure access lists on a router or Layer 3 switch to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic. ACLs can be configured to block inbound traffic, outbound traffic, or both.

Access Control Entries

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies permit or deny and a set of conditions the packet must satisfy in order to match the ACE. The meaning of permit or deny depends on the context in which the ACL is used.
ACL Supported Types

The switch supports IP ACLs and Ethernet (MAC) ACLs:

- IP ACLs filter IPv4 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).

- Ethernet ACLs filter non-IP traffic.

This switch also supports quality of service (QoS) classification ACLs.

Supported ACLs

The switch supports three types of ACLs to filter traffic:

- Port ACLs access-control traffic entering a Layer 2 interface. You can apply port ACLs to a Layer 2 interface in each direction to each access list type — IPv4 and MAC.

- Router ACLs access-control routed traffic between VLANs and are applied to Layer 3 interfaces in a specific direction (inbound or outbound).

- VLAN ACLs or VLAN maps access-control all packets (bridged and routed). You can use VLAN maps to filter traffic between devices in the same VLAN. VLAN maps are configured to provide access control based on Layer 3 addresses for IPv4. Unsupported protocols are access-controlled through MAC addresses using Ethernet ACEs. After a VLAN map is applied to a VLAN, all packets (routed or bridged) entering the VLAN are checked against the VLAN map. Packets can either enter the VLAN through a switch port or through a routed port after being routed.

ACL Precedence

When VLAN maps, Port ACLs, and router ACLs are configured on the same switch, the filtering precedence, from greatest to least for ingress traffic is port ACL, VLAN map, and then router ACL. For egress traffic, the filtering precedence is router ACL, VLAN map, and then port ACL.

The following examples describe simple use cases:

- When both an input port ACL and a VLAN map are applied, incoming packets received on ports with a port ACL applied are filtered by the port ACL. Other packets are filtered by the VLAN map.

- When an input router ACL and input port ACL exist in a switch virtual interface (SVI), incoming packets received on ports to which a port ACL is applied are filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.

- When an output router ACL and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IP packets are filtered by the router ACL. Other packets are not filtered.

- When a VLAN map, input router ACL, and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.

- When a VLAN map, output router ACL, and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Outgoing routed IP packets...
are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.

Related Topics
Restrictions for Configuring IPv4 Access Control Lists, on page 865

Port ACLs

Port ACLs are ACLs that are applied to Layer 2 interfaces on a switch. Port ACLs are supported only on physical interfaces and not on EtherChannel interfaces. Port ACLs can be applied to the interface in outbound and inbound direction. The following access lists are supported:

- Standard IP access lists using source addresses
- Extended IP access lists using source and destination addresses and optional protocol type information
- MAC extended access lists using source and destination MAC addresses and optional protocol type information

The switch examines ACLs on an interface and permits or denies packet forwarding based on how the packet matches the entries in the ACL. In this way, ACLs control access to a network or to part of a network.

Figure 44: Using ACLs to Control Traffic in a Network

This is an example of using port ACLs to control access to a network when all workstations are in the same VLAN. ACLs applied at the Layer 2 input would allow Host A to access the Human Resources network, but prevent Host B from accessing the same network. Port ACLs can only be applied to Layer 2 interfaces in the inbound direction.

When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port.

When you apply a port ACL to a port with voice VLAN, the ACL filters traffic on both data and voice VLANs.

With port ACLs, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC addresses. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP access list and a MAC access list to the interface.
You cannot apply more than one IP access list and one MAC access list to a Layer 2 interface. If an IP access list or MAC access list is already configured on a Layer 2 interface and you apply a new IP access list or MAC access list to the interface, the new ACL replaces the previously configured one.

**Router ACLs**

You can apply router ACLs on switch virtual interfaces (SVIs), which are Layer 3 interfaces to VLANs; on physical Layer 3 interfaces; and on Layer 3 EtherChannel interfaces. You apply router ACLs on interfaces for specific directions (inbound or outbound). You can apply one router ACL in each direction on an interface.

The switch supports these access lists for IPv4 traffic:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses and optional protocol type information for matching operations.

As with port ACLs, the switch examines ACLs associated with features configured on a given interface. As packets enter the switch on an interface, ACLs associated with all inbound features configured on that interface are examined. After packets are routed and before they are forwarded to the next hop, all ACLs associated with outbound features configured on the egress interface are examined.

ACLs permit or deny packet forwarding based on how the packet matches the entries in the ACL, and can be used to control access to a network or to part of a network.

**VLAN Maps**

VLAN ACLs or VLAN maps are used to control network traffic within a VLAN. You can apply VLAN maps to all packets that are bridged within a VLAN in the switch or switch stack. VLAN maps are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VLAN maps are not defined by direction (ingress or egress).

All non-IP protocols are access-controlled through MAC addresses and Ethertype using MAC VLAN maps. (IP traffic is not access controlled by MAC VLAN maps.) You can enforce VLAN maps only on packets going through the switch; you cannot enforce VLAN maps on traffic between hosts on a hub or on another switch connected to this switch.

With VLAN maps, forwarding of packets is permitted or denied, based on the action specified in the map.

*Figure 45: Using VLAN Maps to Control Traffic*

This shows how a VLAN map is applied to prevent a specific type of traffic from Host A in VLAN 10 from being forwarded. You can apply only one VLAN map to a VLAN.
ACEs and Fragmented and Unfragmented Traffic

IP packets can be fragmented as they cross the network. When this happens, only the fragment containing the beginning of the packet contains the Layer 4 information, such as TCP or UDP port numbers, ICMP type and code, and so on. All other fragments are missing this information.

Some access control entries (ACEs) do not check Layer 4 information and therefore can be applied to all packet fragments. ACEs that do test Layer 4 information cannot be applied in the standard manner to most of the fragments in a fragmented IP packet. When the fragment contains no Layer 4 information and the ACE tests some Layer 4 information, the matching rules are modified:

- Permit ACEs that check the Layer 3 information in the fragment (including protocol type, such as TCP, UDP, and so on) are considered to match the fragment regardless of what the missing Layer 4 information might have been.
- Deny ACEs that check Layer 4 information never match a fragment unless the fragment contains Layer 4 information.

Note

For TCP ACEs with L4 Ops, the fragmented packets will be dropped per RFC 1858.

ACEs and Fragmented and Unfragmented Traffic Examples

Consider access list 102, configured with these commands, applied to three fragmented packets:

Switch(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config)# access-list 102 permit tcp any host 10.1.1.2
Switch(config)# access-list 102 deny tcp any any

Note

In the first and second ACEs in the examples, the eq keyword after the destination address means to test for the TCP-destination-port well-known numbers equaling Simple Mail Transfer Protocol (SMTP) and Telnet, respectively.

- Packet A is a TCP packet from host 10.2.2.2., port 65000, going to host 10.1.1.1 on the SMTP port. If this packet is fragmented, the first fragment matches the first ACE (a permit) as if it were a complete packet because all Layer 4 information is present. The remaining fragments also match the first ACE, even though they do not contain the SMTP port information, because the first ACE only checks Layer 3 information when applied to fragments. The information in this example is that the packet is TCP and that the destination is 10.1.1.1.

- Packet B is from host 10.2.2.2, port 65001, going to host 10.1.1.2 on the Telnet port. If this packet is fragmented, the first fragment matches the second ACE (a deny) because all Layer 3 and Layer 4 information is present. The remaining fragments in the packet do not match the second ACE because they are missing Layer 4 information. Instead, they match the third ACE (a permit).
Because the first fragment was denied, host 10.1.1.2 cannot reassemble a complete packet, so packet B is effectively denied. However, the later fragments that are permitted will consume bandwidth on the network and resources of host 10.1.1.2 as it tries to reassemble the packet.

- Fragmented packet C is from host 10.2.2.2, port 65001, going to host 10.1.1.3, port ftp. If this packet is fragmented, the first fragment matches the fourth ACE (a deny). All other fragments also match the fourth ACE because that ACE does not check any Layer 4 information and because Layer 3 information in all fragments shows that they are being sent to host 10.1.1.3, and the earlier permit ACEs were checking different hosts.

### ACLs and Switch Stacks

ACL support is the same for a switch stack as for a standalone switch. ACL configuration information is propagated to all switches in the stack. All switches in the stack, including the active switch, process the information and program their hardware.

### Active Switch and ACL Functions

The active switch performs these ACL functions:

- It processes the ACL configuration and propagates the information to all stack members.
- It distributes the ACL information to any switch that joins the stack.
- If packets must be forwarded by software for any reason (for example, not enough hardware resources), the active switch forwards the packets only after applying ACLs on the packets.
- It programs its hardware with the ACL information it processes.

### Stack Member and ACL Functions

Stack members perform these ACL functions:

- They receive the ACL information from the active switch and program their hardware.
- A stack member configured as a standby switch, performs the functions of the active switch in the event the active switch fails.

### Active Switch Failure and ACLs

Both the active and standby switches have the ACL information. When the active switch fails, the standby takes over. The new active switch distributes the ACL information to all stack members.

### Standard and Extended IPv4 ACLs

This section describes IP ACLs.

An ACL is a sequential collection of permit and deny conditions. One by one, the switch tests packets against the conditions in an access list. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing after the first match, the order of the conditions is critical. If no conditions match, the switch denies the packet.

The software supports these types of ACLs or access lists for IPv4:
• Standard IP access lists use source addresses for matching operations.
• Extended IP access lists use source and destination addresses for matching operations and optional protocol-type information for finer granularity of control.

IPv4 ACL Switch Unsupported Features

Configuring IPv4 ACLs on the switch is the same as configuring IPv4 ACLs on other Cisco switches and routers.

The following ACL-related features are not supported:
• Non-IP protocol ACLs
• IP accounting
• Reflexive ACLs and dynamic ACLs are not supported.

Access List Numbers

The number you use to denote your ACL shows the type of access list that you are creating.

This lists the access-list number and corresponding access list type and shows whether or not they are supported in the switch. The switch supports IPv4 standard and extended access lists, numbers 1 to 199 and 1300 to 2699.

Table 64: Access List Numbers

<table>
<thead>
<tr>
<th>Access List Number</th>
<th>Type</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>1–99</td>
<td>IP standard access list</td>
<td>Yes</td>
</tr>
<tr>
<td>100–199</td>
<td>IP extended access list</td>
<td>Yes</td>
</tr>
<tr>
<td>200–299</td>
<td>Protocol type-code access list</td>
<td>No</td>
</tr>
<tr>
<td>300–399</td>
<td>DECnet access list</td>
<td>No</td>
</tr>
<tr>
<td>400–499</td>
<td>XNS standard access list</td>
<td>No</td>
</tr>
<tr>
<td>500–599</td>
<td>XNS extended access list</td>
<td>No</td>
</tr>
<tr>
<td>600–699</td>
<td>AppleTalk access list</td>
<td>No</td>
</tr>
<tr>
<td>700–799</td>
<td>48-bit MAC address access list</td>
<td>No</td>
</tr>
<tr>
<td>800–899</td>
<td>IPX standard access list</td>
<td>No</td>
</tr>
<tr>
<td>900–999</td>
<td>IPX extended access list</td>
<td>No</td>
</tr>
<tr>
<td>1000–1099</td>
<td>IPX SAP access list</td>
<td>No</td>
</tr>
<tr>
<td>1100–1199</td>
<td>Extended 48-bit MAC address access list</td>
<td>No</td>
</tr>
<tr>
<td>1200–1299</td>
<td>IPX summary address access list</td>
<td>No</td>
</tr>
</tbody>
</table>
### Numbered Standard IPv4 ACLs

When creating an ACL, remember that, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end. With standard access lists, if you omit the mask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

The switch always rewrites the order of standard access lists so that entries with *host* matches and entries with matches having a *don't care* mask of 0.0.0.0 are moved to the top of the list, above any entries with *non-zero don't care* masks. Therefore, in *show* command output and in the configuration file, the ACEs do not necessarily appear in the order in which they were entered.

After creating a numbered standard IPv4 ACL, you can apply it to VLANs, to terminal lines, or to interfaces.

### Numbered Extended IPv4 ACLs

Although standard ACLs use only source addresses for matching, you can use extended ACL source and destination addresses for matching operations and optional protocol type information for finer granularity of control. When you are creating ACEs in numbered extended access lists, remember that after you create the ACL, any additions are placed at the end of the list. You cannot reorder the list or selectively add or remove ACEs from a numbered list.

The switch does not support dynamic or reflexive access lists. It also does not support filtering based on the type of service (ToS) minimize-monetary-cost bit.

Some protocols also have specific parameters and keywords that apply to that protocol.

You can define an extended TCP, UDP, ICMP, IGMP, or other IP ACL. The switch also supports these IP protocols:

- **Note**
  - ICMP echo-reply cannot be filtered. All other ICMP codes or types can be filtered.

These IP protocols are supported:

- Authentication Header Protocol (*ahp*)
- Encapsulation Security Payload (*esp*)
- Enhanced Interior Gateway Routing Protocol (*eigrp*)
- generic routing encapsulation (*gre*)
Named IPv4 ACLs

You can identify IPv4 ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IPv4 access lists in a router than if you were to use numbered access lists. If you identify your access list with a name rather than a number, the mode and command syntax are slightly different. However, not all commands that use IP access lists accept a named access list.

The name you give to a standard or extended ACL can also be a number in the supported range of access list numbers. That is, the name of a standard IP ACL can be 1 to 99 and . The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Consider these guidelines before configuring named ACLs:

- Numbered ACLs are also available.
- A standard ACL and an extended ACL cannot have the same name.
- You can use standard or extended ACLs (named or numbered) in VLAN maps.

ACL Logging

The switch software can provide logging messages about packets permitted or denied by a standard IP access list. That is, any packet that matches the ACL causes an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the logging console commands controlling the syslog messages.

ACL logging is only supported for RACL.
Because routing is done in hardware and logging is done in software, if a large number of packets match a permit or deny ACE containing a log keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

The first packet that triggers the ACL causes a logging message right away, and subsequent packets are collected over 5-minute intervals before they appear or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.

The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

Smart Logging

When smart logging is enabled on the switch and an ACL configured with smart logging is attached to a Layer 2 interface (port ACL), the contents of packets denied or permitted because of the ACL are also sent to a specified NetFlow collector.

Hardware and Software Treatment of IP ACLs

ACL processing is performed in hardware. If the hardware reaches its capacity to store ACL configurations, all packets on that interface are dropped.

If an ACL configuration cannot be implemented in hardware due to an out-of-resource condition on a switch or stack member, then only the traffic in that VLAN arriving on that switch is affected.

For router ACLs, other factors can cause packets to be sent to the CPU:

- Using the log keyword
- Generating ICMP unreachable messages

When you enter the show ip access-lists privileged EXEC command, the match count displayed does not account for packets that are access controlled in hardware. Use the show platform acl counters hardware privileged EXEC command to obtain some basic hardware ACL statistics for switched and routed packets.

Router ACLs function as follows:

- The hardware controls permit and deny actions of standard and extended ACLs (input and output) for security access control.

- If log has not been specified, the flows that match a deny statement in a security ACL are dropped by the hardware if ip unreachables is disabled. The flows matching a permit statement are switched in hardware.
• Adding the `log` keyword to an ACE in a router ACL causes a copy of the packet to be sent to the CPU for logging only. If the ACE is a `permit` statement, the packet is still switched and routed in hardware.

### VLAN Map Configuration Guidelines

VLAN maps are the only way to control filtering within a VLAN. VLAN maps have no direction. To filter traffic in a specific direction by using a VLAN map, you need to include an ACL with specific source or destination addresses. If there is a match clause for that type of packet (IP or MAC) in the VLAN map, the default action is to drop the packet if the packet does not match any of the entries within the map. If there is no match clause for that type of packet, the default is to forward the packet.

The following are the VLAN map configuration guidelines:

- If there is no ACL configured to deny traffic on an interface and no VLAN map is configured, all traffic is permitted.
- Each VLAN map consists of a series of entries. The order of entries in an VLAN map is important. A packet that comes into the switch is tested against the first entry in the VLAN map. If it matches, the action specified for that part of the VLAN map is taken. If there is no match, the packet is tested against the next entry in the map.
- If the VLAN map has at least one match clause for the type of packet (IP or MAC) and the packet does not match any of these match clauses, the default is to drop the packet. If there is no match clause for that type of packet in the VLAN map, the default is to forward the packet.
- Logging is not supported for VLAN maps.
- When a switch has an IP access list or MAC access list applied to a Layer 2 interface, and you apply a VLAN map to a VLAN that the port belongs to, the port ACL takes precedence over the VLAN map.
- If a VLAN map configuration cannot be applied in hardware, all packets in that VLAN are dropped.

### VLAN Maps with Router ACLs

To access control both bridged and routed traffic, you can use VLAN maps only or a combination of router ACLs and VLAN maps. You can define router ACLs on both input and output routed VLAN interfaces, and you can define a VLAN map to access control the bridged traffic.

If a packet flow matches a VLAN-map deny clause in the ACL, regardless of the router ACL configuration, the packet flow is denied.

---

**Note**

When you use router ACLs with VLAN maps, packets that require logging on the router ACLs are not logged if they are denied by a VLAN map.

If the VLAN map has a match clause for the type of packet (IP or MAC) and the packet does not match the type, the default is to drop the packet. If there is no match clause in the VLAN map, and no action specified, the packet is forwarded if it does not match any VLAN map entry.
VLAN Maps and Router ACL Configuration Guidelines

These guidelines are for configurations where you need to have an router ACL and a VLAN map on the same VLAN. These guidelines do not apply to configurations where you are mapping router ACLs and VLAN maps on different VLANs.

If you must configure a router ACL and a VLAN map on the same VLAN, use these guidelines for both router ACL and VLAN map configuration:

- You can configure only one VLAN map and one router ACL in each direction (input/output) on a VLAN interface.
- Whenever possible, try to write the ACL with all entries having a single action except for the final, default action of the other type. That is, write the ACL using one of these two forms:
  
  permit... permit... permit... deny ip any any
  
or
  
deny... deny... deny... permit ip any any

- To define multiple actions in an ACL (permit, deny), group each action type together to reduce the number of entries.
- Avoid including Layer 4 information in an ACL; adding this information complicates the merging process. The best merge results are obtained if the ACLs are filtered based on IP addresses (source and destination) and not on the full flow (source IP address, destination IP address, protocol, and protocol ports). It is also helpful to use don’t care bits in the IP address, whenever possible.

If you need to specify the full-flow mode and the ACL contains both IP ACEs and TCP/UDP/ICMP ACEs with Layer 4 information, put the Layer 4 ACEs at the end of the list. This gives priority to the filtering of traffic based on IP addresses.

Time Ranges for ACLs

You can selectively apply extended ACLs based on the time of day and the week by using the `time-range` global configuration command. First, define a time-range name and set the times and the dates or the days of the week in the time range. Then enter the time-range name when applying an ACL to set restrictions to the access list. You can use the time range to define when the permit or deny statements in the ACL are in effect, for example, during a specified time period or on specified days of the week. The `time-range` keyword and argument are referenced in the named and numbered extended ACL task tables.

These are some benefits of using time ranges:

- You have more control over permitting or denying a user access to resources, such as an application (identified by an IP address/mask pair and a port number).

- You can control logging messages. ACL entries can be set to log traffic only at certain times of the day. Therefore, you can simply deny access without needing to analyze many logs generated during peak hours.

Time-based access lists trigger CPU activity because the new configuration of the access list must be merged with other features and the combined configuration loaded into the hardware memory. For this reason, you should be careful not to have several access lists configured to take effect in close succession (within a small number of minutes of each other.)
The timer range relies on the switch system clock; therefore, you need a reliable clock source. We recommend that you use Network Time Protocol (NTP) to synchronize the switch clock.

Related Topics
- Configuring Time Ranges for ACLs, on page 887

IPv4 ACL Interface Considerations

When you apply the `ip access-group` interface configuration command to a Layer 3 interface (an SVI, a Layer 3 EtherChannel, or a routed port), the interface must have been configured with an IP address. Layer 3 access groups filter packets that are routed or are received by Layer 3 processes on the CPU. They do not affect packets bridged within a VLAN.

For inbound ACLs, after receiving a packet, the switch checks the packet against the ACL. If the ACL permits the packet, the switch continues to process the packet. If the ACL rejects the packet, the switch discards the packet.

For outbound ACLs, after receiving and routing a packet to a controlled interface, the switch checks the packet against the ACL. If the ACL permits the packet, the switch sends the packet. If the ACL rejects the packet, the switch discards the packet.

By default, the input interface sends ICMP Unreachable messages whenever a packet is discarded, regardless of whether the packet was discarded because of an ACL on the input interface or because of an ACL on the output interface. ICMP Unreachables are normally limited to no more than one every one-half second per input interface, but this can be changed by using the `ip icmp rate-limit unreachable` global configuration command.

When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied to the interface and permits all packets. Remember this behavior if you use undefined ACLs for network security.

Related Topics
- Applying an IPv4 ACL to an Interface, on page 890
- Restrictions for Configuring IPv4 Access Control Lists, on page 865

How to Configure ACLs

Configuring IPv4 ACLs

These are the steps to use IP ACLs on the switch:

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create an ACL by specifying an access list number or name and the access conditions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Apply the ACL to interfaces or terminal lines. You can also apply standard and extended IP ACLs to VLAN maps.</td>
</tr>
</tbody>
</table>
## Creating a Numbered Standard ACL

Follow these steps to create a numbered standard ACL:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`access-list access-list-number {deny</td>
<td>permit} source source-wildcard [log]`</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# access-list 2 deny your_host</code></td>
<td>The <code>access-list-number</code> is a decimal number from 1 to 99 or 1300 to 1999. Enter <code>deny</code> or <code>permit</code> to specify whether to deny or permit access if conditions are matched. The <code>source</code> is the source address of the network or host from which the packet is being sent specified as:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The 32-bit quantity in dotted-decimal format.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The keyword <code>any</code> as an abbreviation for <code>source</code> and <code>source-wildcard</code> of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The keyword <code>host</code> as an abbreviation for <code>source</code> and <code>source-wildcard</code> of <code>source</code> 0.0.0.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional) The <code>source-wildcard</code> applies wildcard bits to the source.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional) Enter <code>log</code> to cause an informational logging message about the packet that matches the entry to be sent to the console.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Logging is supported only on ACLs attached to Layer 3 interfaces.</td>
<td></td>
</tr>
</tbody>
</table>
Creating a Numbered Extended ACL

Follow these steps to create a numbered extended ACL:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>access-list access-list-number {deny</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log</td>
</tr>
</tbody>
</table>

**Access-List Numbering**

A numbered extended ACL uses a range of access-list numbers starting from 100 to 199 or 2000 to 2699. Lower numbers are typically associated with older access-list models, which used only 16 standard access lists. This range of extended access-list numbers is used to filter traffic based on more complex conditions.

**Access-List Conditions**

Access-list conditions define which traffic should be allowed or denied. Some common conditions include:

- **protocol**: Specifies the protocol used by the traffic. Options include ahp, eigrp, esp, gre, icmp, igmp, igrp, ip, ipinip, nos, ospf, pcp, pim, tcp, or udp.
- **source source-wildcard**: Specifies the source address and wildcard used to determine how to match the traffic.
- **destination destination-wildcard**: Specifies the destination address and wildcard used to determine how to match the traffic.
- **precedence precedence**: Allows or denies traffic based on the precedence value.
- **tos tos**: Allows or denies traffic based on the type of service value.
- **fragments**: Applies to fragmented traffic.
- **log [log-input]**: Logs packets that match the access list conditions.
- **time-range time-range-name**
- **dscp dscp**: Allows or denies traffic based on the differentiated services code point (DSCP) value.

**Example of Allowing Traffic Based on Protocol and Source Address**

```bash
Switch(config)# access-list 200 permit tcp host 10.1.1.2 any precedence 0 tos 0 log
```

**Example of Denying Traffic Based on Protocol and Source Address**

```bash
Switch(config)# access-list 202 deny tcp host 10.1.1.2 any precedence 0 tos 0 log
```

**Example of Filtering Traffic Based on Protocol and Source Address with Wildcard**

```bash
Switch(config)# access-list 203 permit tcp host 10.1.1.2 host 10.1.1.3 precedence 0 tos 0 log
```

**Example of Filtering Traffic Based on Precedence and TOS**

```bash
Switch(config)# access-list 204 permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 precedence 0 tos 0 log
```

**Example of Filtering Traffic Based on Protocol and Time Range**

```bash
Switch(config)# access-list 205 permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 time-range my_schedule precedence 0 tos 0 log
```

**Example of Filtering Traffic Based on Protocol, Source Address, and DSCP**

```bash
Switch(config)# access-list 206 permit tcp host 10.1.1.2 host 10.1.1.3 dscp 5 precedence 0 tos 0 log
```

**Example of Filtering Traffic Based on Protocol, Source Address, and Type of Service**

```bash
Switch(config)# access-list 207 permit tcp host 10.1.1.2 host 10.1.1.3 tos 5 precedence 0 log
```

**Example of Filtering Traffic Based on Protocol, Source Address, and Precedence**

```bash
Switch(config)# access-list 208 permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 precedence 5 log
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword <code>ip</code>.</td>
<td></td>
</tr>
</tbody>
</table>

**Note** This step includes options for most IP protocols. For additional specific parameters for TCP, UDP, ICMP, and IGMP, see the following steps.

The *source* is the number of the network or host from which the packet is sent.

The *source-wildcard* applies wildcard bits to the source.

The *destination* is the network or host number to which the packet is sent.

The *destination-wildcard* applies wildcard bits to the destination.

Source, source-wildcard, destination, and destination-wildcard can be specified as:

- The 32-bit quantity in dotted-decimal format.
- The keyword `any` for 0.0.0.0 255.255.255.255 (any host).
- The keyword `host` for a single host 0.0.0.0.

The other keywords are optional and have these meanings:

- **precedence**—Enter to match packets with a precedence level specified as a number from 0 to 7 or by name: `routine` (0), `priority` (1), `immediate` (2), `flash` (3), `flash-override` (4), `critical` (5), `internet` (6), `network` (7).

- **fragments**—Enter to check non-initial fragments.

- **tos**—Enter to match by type of service level, specified by a number from 0 to 15 or a name: `normal` (0), `max-reliability` (2), `max-throughput` (4), `min-delay` (8).

- **log**—Enter to create an informational logging message to be sent to the console about the packet that matches the entry or `log-input` to include the input interface in the log entry.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• time-range—Specify the time-range name.</td>
<td></td>
</tr>
<tr>
<td>• dscp—Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> If you enter a dscp value, you cannot enter tos or precedence. You can enter both a tos and a precedence value with no dscp.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

```
access-list access-list-number {deny | permit} tcp source source-wildcard [operator port]
destination destination-wildcard [operator port]
established [precedence precedence] [tos tos] [fragments] [log [log-input] [time-range time-range-name] [dscp dscp] [flag]
```

**Example:**

```
Switch(config)# access-list 101 permit tcp any any eq 500
```

Defines an extended TCP access list and the access conditions.

The parameters are the same as those described for an extended IPv4 ACL, with these exceptions:

(Optional) Enter an operator and port to compare source (if positioned after source source-wildcard) or destination (if positioned after destination destination-wildcard) port. Possible operators include eq (equal), gt (greater than), lt (less than), neq (not equal), and range (inclusive range). Operators require a port number (range requires two port numbers separated by a space).

Enter the port number as a decimal number (from 0 to 65535) or the name of a TCP port. Use only TCP port numbers or names when filtering TCP.

The other optional keywords have these meanings:

• established—Enter to match an established connection. This has the same function as matching on the ack or rst flag.

• flag—Enter one of these flags to match by the specified TCP header bits: ack (acknowledge), fin (finish), psh (push), rst (reset), syn (synchronize), or urg (urgent).

**Step 4**

```
access-list access-list-number {deny | permit} udp source source-wildcard [operator port]
destination destination-wildcard [operator port]
precedence precedence [tos tos] [fragments]
```

(Optional) Defines an extended UDP access list and the access conditions.

The UDP parameters are the same as those described for TCP except that the [operator
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>[log [log-input] [time-range time-range-name] [dscp dscp]]</td>
<td>[port] port number or name must be a UDP port number or name, and the flag and established keywords are not valid for UDP.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# access-list 101 permit udp any any eq 100</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

```
access-list access-list-number {deny | permit} icmp source source-wildcard destination destination-wildcard [icmp-type | [icmp-type icmp-code] | [icmp-type icmp-code] | [precedence precedence] | [tos tos] | [fragments] | [log log-input] | [time-range time-range-name] | [dscp dscp]]
```

**Example:**

Switch(config)# access-list 101 permit icmp any any 200

Defines an extended ICMP access list and the access conditions.

The ICMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:

- **icmp-type**—Enter to filter by ICMP message type, a number from 0 to 255.
- **icmp-code**—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.
- **icmp-message**—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name.

**Step 6**

```
access-list access-list-number {deny | permit} igmp source source-wildcard destination destination-wildcard [precedence precedence] | [tos tos] | [fragments] | [log log-input] | [time-range time-range-name] | [dscp dscp]]
```

**Example:**

Switch(config)# access-list 101 permit igmp any any 14

(Optional) Defines an extended IGMP access list and the access conditions.

The IGMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with this optional parameter.

**igmp-type**—To match IGMP message type, enter a number from 0 to 15, or enter the message name: **dvmrp**, **host-query**, **host-report**, **pim**, or **trace**.

**Step 7**

```
end
```

**Example:**

Switch(config)# end

Returns to privileged EXEC mode.

---

**Related Topics**

- Configuring VLAN Maps, on page 894
Creating Named Standard ACLs

Follow these steps to create a standard ACL using names:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip access-list standard name</td>
<td>Defines a standard IPv4 access list using a name, and enter access-list configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ip access-list standard 20</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Use one of the following:</td>
<td>In access-list configuration mode, specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.255.0 0.0.255.255</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td>Switch(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-std-nacl)# end</td>
<td></td>
</tr>
</tbody>
</table>
## Creating Extended Named ACLs

Follow these steps to create an extended ACL using names:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>ip access-list extended name</code></td>
<td>Defines an extended IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 100 to 199.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# ip access-list extended 150</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>`{deny</td>
<td>permit} protocol {source [source-wildcard]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Example:</code></td>
<td><strong>host source</strong>—A source and source wildcard of <code>source 0.0.0.0</code>.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config-ext-nacl)# permit 0 any any</code></td>
<td>• <strong>host destination</strong>—A destination and destination wildcard of <code>destination 0.0.0.0</code>. • <strong>any</strong>—A source and source wildcard or destination and destination wildcard of <code>0.0.0.0 255.255.255.255</code>.</td>
</tr>
</tbody>
</table>

### Step 5

**Example:**

```
Switch(config-ext-nacl)# end
```

Returns to privileged EXEC mode.

### Step 6

**Example:**

```
Switch# show running-config
```

Verifies your entries.

### Step 7

**Example:**

```
Switch# copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

---

When you are creating extended ACLs, remember that, by default, the end of the ACL contains an implicit deny statement for everything if it did not find a match before reaching the end. For standard ACLs, if you omit the mask from an associated IP host address access list specification, `0.0.0.0` is assumed to be the mask.

After you create an ACL, any additions are placed at the end of the list. You cannot selectively add ACL entries to a specific ACL. However, you can use `no permit` and `no deny` access-list configuration mode commands to remove entries from a named ACL.

Being able to selectively remove lines from a named ACL is one reason you might use named ACLs instead of numbered ACLs.

### What to do next

After creating a named ACL, you can apply it to interfaces or to VLANs.

---

### Configuring Time Ranges for ACLs

Follow these steps to configure a time-range parameter for an ACL:
### Configuring Time Ranges for ACLs

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>time-range time-range-name</td>
<td>Assigns a meaningful name (for example, workhours) to the time range to be created, and enter time-range configuration mode. The name cannot contain a space or quotation mark and must begin with a letter.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# time-range workhours</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Use one of the following:</td>
<td>Specifies when the function it will be applied to is operational.</td>
</tr>
<tr>
<td></td>
<td>• absolute [start time date] [end time date]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• periodic day-of-the-week hh:mm to [day-of-the-week] hh:mm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• periodic [weekdays</td>
<td>weekend</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Specifying the function it will be applied to is operational.</td>
</tr>
<tr>
<td></td>
<td>Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-time-range)# periodic weekdays 8:00 to 12:00</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show running-config</td>
<td></td>
</tr>
</tbody>
</table>
Applying an IPv4 ACL to a Terminal Line

You can use numbered ACLs to control access to one or more terminal lines. You cannot apply named ACLs to lines. You must set identical restrictions on all the virtual terminal lines because a user can attempt to connect to any of them.

Follow these steps to restrict incoming and outgoing connections between a virtual terminal line and the addresses in an ACL:

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>line [console</td>
<td>vty] line-number</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# line console 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• console—Specifies the console terminal line. The console port is DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• vty—Specifies a virtual terminal for remote console access.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The line-number is the first line number in a contiguous group that you want to configure</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- Time Ranges for ACLs, on page 878
Applying an IPv4 ACL to an Interface

This section describes how to apply IPv4 ACLs to network interfaces.

Beginning in privileged EXEC mode, follow these steps to control access to an interface:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Identifies a specific interface for configuration, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> access-class access-list-number {in</td>
<td>out}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-line)# access-class 10 in</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-line)# end</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Creating Named MAC Extended ACLs

You can filter non-IPv4 traffic on a VLAN or on a Layer 2 interface by using MAC addresses and named MAC extended ACLs. The procedure is similar to that of configuring other extended named ACLs.

Follow these steps to create a named MAC extended ACL:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
</tbody>
</table>

### Related Topics

- IPv4 ACL Interface Considerations, on page 879
- Restrictions for Configuring IPv4 Access Control Lists, on page 865
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2** configure terminal  
Example:  
Switch# configure terminal | Enters global configuration mode. |
| **Step 3** mac access-list extended name  
Example:  
Switch(config)# mac access-list extended mac1 | Defines an extended MAC access list using a name. |
| **Step 4** {deny | permit} {any | host source MAC address | source MAC address mask} {any | host destination MAC address | destination MAC address mask} {type mask | lsap lsap mask | aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp | 0-65535} [cos cos]  
Example:  
Switch(config-ext-macl)# deny any any decnet-iv  
or  
Switch(config-ext-macl)# permit any any  
(Optional) You can also enter these options:  
• *type mask*—An arbitrary EtherType number of a packet with Ethernet II or SNAP encapsulation in decimal, hexadecimal, or octal with optional mask of *don’t care* bits applied to the EtherType before testing for a match.  
• *lsap lsap mask*—An LSAP number of a packet with IEEE 802.2 encapsulation in decimal, hexadecimal, or octal with optional mask of *don’t care* bits.  
• *aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp*—A non-IP protocol.  
• *cos cos*—An IEEE 802.1Q cost of service number from 0 to 7 used to set priority. | In extended MAC access-list configuration mode, specifies to permit or deny any source MAC address, a source MAC address with a mask, or a specific host source MAC address and any destination MAC address, destination MAC address with a mask, or a specific destination MAC address. |
| **Step 5** end  
Example:  
Switch(config-ext-macl)# end | Returns to privileged EXEC mode. |
### Applying a MAC ACL to a Layer 2 Interface

Follow these steps to apply a MAC access list to control access to a Layer 2 interface:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Identifies a specific interface, and enter interface configuration mode. The interface must be a physical Layer 2 interface (port ACL).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet1/0/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> mac access-group {name} {in</td>
<td>out }</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# mac access-group mac1</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>in</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

end  
Example:  
Switch(config-if)# end

Returns to privileged EXEC mode.

**Step 6**

show mac access-group [interface interface-id]  
Example:  
Switch# show mac access-group interface gigabitethernet1/0/2

Displays the MAC access list applied to the interface or all Layer 2 interfaces.

**Step 7**

configure terminal  
Example:  
Switch# configure terminal

Enters global configuration mode.

**Step 8**

configure terminal  
Example:  
Switch# configure terminal

Enters global configuration mode.

After receiving a packet, the switch checks it against the inbound ACL. If the ACL permits it, the switch continues to process the packet. If the ACL rejects the packet, the switch discards it. When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied and permits all packets. Remember this behavior if you use undefined ACLs for network security.

**Related Topics**

Restrictions for Configuring IPv4 Access Control Lists, on page 865

---

**Configuring VLAN Maps**

To create a VLAN map and apply it to one or more VLANs, perform these steps:

**Before you begin**

Create the standard or extended IPv4 ACLs or named MAC extended ACLs that you want to apply to the VLAN.
# Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Creates a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map.</td>
</tr>
<tr>
<td><code>vlan access-map name [number]</code></td>
<td>When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>VLAN maps do not use the specific permit or deny keywords. To deny a packet by using VLAN maps, create an ACL that would match the packet, and set the action to drop. A permit in the ACL counts as a match. A deny in the ACL means no match.</td>
</tr>
<tr>
<td><code>Switch(config)# vlan access-map map_1 20</code></td>
<td>Entering this command changes to access-map configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Match the packet (using either the IP or MAC address) against one or more standard or extended access lists. Note that packets are only matched against access lists of the correct protocol type. IP packets are matched against standard or extended IP access lists. Non-IP packets are only matched against named MAC extended access lists.</td>
</tr>
<tr>
<td>`match {ip</td>
<td>mac} address {name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-access-map)# match ip address ip2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the action for the map entry.</td>
</tr>
<tr>
<td>Enter one of the following commands to specify an IP packet or a non-IP packet (with only a known MAC address) and to match the packet against one or more ACLs (standard or extended):</td>
<td></td>
</tr>
<tr>
<td>- <code>action { forward}</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-access-map)# action forward</code></td>
<td></td>
</tr>
<tr>
<td>- <code>action { drop}</code></td>
<td></td>
</tr>
</tbody>
</table>

---

**Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E**
### Creating a VLAN Map

Each VLAN map consists of an ordered series of entries. Beginning in privileged EXEC mode, follow these steps to create, add to, or delete a VLAN map entry:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> vlan access-map name [number]</td>
<td>Creates a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# vlan access-map map_1 20</td>
<td></td>
</tr>
</tbody>
</table>

When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete.

VLAN maps do not use the specific permit or deny keywords. To deny a packet by using VLAN maps, create an ACL that would match the packet, and set the action to drop. A permit
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>in the ACL counts as a match. A deny in the ACL means no match. Entering this command changes to access-map configuration mode.</td>
</tr>
<tr>
<td>Step 3 match {ip | mac} address {name | number} [name | number]</td>
<td>Match the packet (using either the IP or MAC address) against one or more standard or extended access lists. Note that packets are only matched against access lists of the correct protocol type. IP packets are matched against standard or extended IP access lists. Non-IP packets are only matched against named MAC extended access lists.</td>
</tr>
<tr>
<td>Example: Switch(config-access-map)# match ip address ip2</td>
<td></td>
</tr>
<tr>
<td>Step 4 action {drop | forward}</td>
<td>(Optional) Sets the action for the map entry. The default is to forward.</td>
</tr>
<tr>
<td>Example: Switch(config-access-map)# action forward</td>
<td></td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config-access-map)# end</td>
<td></td>
</tr>
<tr>
<td>Step 6 show running-config</td>
<td>Displays the access list configuration.</td>
</tr>
<tr>
<td>Example: Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 7 copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example: Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

[Configuring VLAN Maps](#), on page 894

**Applying a VLAN Map to a VLAN**

Beginning in privileged EXEC mode, follow these steps to apply a VLAN map to one or more VLANs:
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>vlan filter mapname vlan-list list</td>
<td>Applies the VLAN map to one or more VLAN IDs.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>The list can be a single VLAN ID (22), a consecutive list (10-22), or a string of VLAN IDs (12, 22, 30). Spaces around the comma and hyphen are optional.</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# vlan filter map 1 vlan-list 20-22</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
<td>Displays the access list configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

#### Related Topics

- **Configuring VLAN Maps**, on page 894

---

### Configuring VACL Logging

Beginning in privileged EXEC mode:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring VACL Logging

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Switch# configure terminal | |}

#### Step 2

<table>
<thead>
<tr>
<th>vlan access-map name [number]</th>
<th>Creates a VLAN map. Give it a name and optionally a number. The number is the sequence number of the entry within the map. The sequence number range is from 0 to 65535. When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete. Specifying the map name and optionally a number enters the access-map configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# vlan access-map gandymede 10</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 3

<table>
<thead>
<tr>
<th>action drop log</th>
<th>Sets the VLAN access map to drop and log IP packets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-access-map)# action drop log</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 4

<table>
<thead>
<tr>
<th>exit</th>
<th>Exits the VLAN access map configuration mode and return to the global configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-access-map)# exit</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 5

| vlan access-log {maxflow max_number | threshold pkt_count} | Configures the VACL logging parameters. |
|-----------------------|------------------------------------------------|
| Switch(config)# vlan access-log threshold 4000 | |

- **maxflow max_number**—Sets the log table size. The content of the log table can be deleted by setting the maxflow to 0. When the log table is full, the software drops logged packets from new flows.
  The range is from 0 to 2048. The default is 500.

- **threshold pkt_count**—Sets the logging threshold. A logging message is generated if the threshold for a flow is reached before the 5-minute interval.
  The threshold range is from 0 to 2147483647. The default threshold is 0, which means that a syslog message is generated every 5 minutes.
Monitoring IPv4 ACLs

You can monitor IPv4 ACLs by displaying the ACLs that are configured on the switch, and displaying the ACLs that have been applied to interfaces and VLANs.

When you use the `ip access-group` interface configuration command to apply ACLs to a Layer 2 or 3 interface, you can display the access groups on the interface. You can also display the MAC ACLs applied to a Layer 2 interface. You can use the privileged EXEC commands as described in this table to display this information.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show access-lists [number</td>
<td>name]`</td>
</tr>
<tr>
<td>`show ip access-lists [number</td>
<td>name]`</td>
</tr>
<tr>
<td><code>show ip interface interface-id</code></td>
<td>Displays detailed configuration and status of an interface. If IP is enabled on the interface and ACLs have been applied by using the <code>ip access-group</code> interface configuration command, the access groups are included in the display.</td>
</tr>
<tr>
<td><code>show running-config [interface interface-id]</code></td>
<td>Displays the contents of the configuration file for the switch or the specified interface, including all configured MAC and IP access lists and which access groups are applied to an interface.</td>
</tr>
<tr>
<td><code>show mac access-group [interface interface-id]</code></td>
<td>Displays MAC access lists applied to all Layer 2 interfaces or the specified Layer 2 interface.</td>
</tr>
</tbody>
</table>
Configuration Examples for ACLs

Examples: Using Time Ranges with ACLs

This example shows how to verify after you configure time ranges for workhours and to configure January 1, 2006, as a company holiday.

Switch# show time-range
time-range entry: new_year_day_2003 (inactive)
   absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
   periodic weekdays 8:00 to 12:00
   periodic weekdays 13:00 to 17:00

To apply a time range, enter the time-range name in an extended ACL that can implement time ranges. This example shows how to create and verify extended access list 188 that denies TCP traffic from any source to any destination during the defined holiday times and permits all TCP traffic during work hours.

Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
  10 deny tcp any any time-range new_year_day_2006 (inactive)
  20 permit tcp any any time-range workhours (inactive)

This example uses named ACLs to permit and deny the same traffic.

Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list lplip_default
  10 permit ip any
Extended IP access list deny_access
  10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
  10 permit tcp any any time-range workhours (inactive)

Examples: Including Comments in ACLs

You can use the remark keyword to include comments (remarks) about entries in any IP standard or extended ACL. The remarks make the ACL easier for you to understand and scan. Each remark line is limited to 100 characters.

The remark can go before or after a permit or deny statement. You should be consistent about where you put the remark so that it is clear which remark describes which permit or deny statement. For example, it would
be confusing to have some remarks before the associated permit or deny statements and some remarks after the associated statements.

To include a comment for IP numbered standard or extended ACLs, use the `access-list access-list-number remark remark` global configuration command. To remove the remark, use the `no` form of this command.

In this example, the workstation that belongs to Jones is allowed access, and the workstation that belongs to Smith is not allowed access:

```plaintext
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith through
Switch(config)# access-list 1 deny 171.69.3.13
```

For an entry in a named IP ACL, use the `remark` access-list configuration command. To remove the remark, use the `no` form of this command.

In this example, the Jones subnet is not allowed to use outbound Telnet:

```plaintext
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

### Examples: Troubleshooting ACLs

If this ACL manager message appears and [chars] is the access-list name,

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

The switch has insufficient resources to create a hardware representation of the ACL. The resources include hardware memory and label space but not CPU memory. A lack of available logical operation units or specialized hardware resources causes this problem. Logical operation units are needed for a TCP flag match or a test other than `eq` (`ne`, `gt`, `lt`, or `range`) on TCP, UDP, or SCTP port numbers.

Use one of these workarounds:

- Modify the ACL configuration to use fewer resources.
- Rename the ACL with a name or number that alphanumerically precedes the ACL names or numbers.

To determine the specialized hardware resources, enter the `show platform layer4 acl` map privileged EXEC command. If the switch does not have available resources, the output shows that index 0 to index 15 are not available.

For more information about configuring ACLs with insufficient resources, see CSCsq63926 in the Bug Toolkit.

For example, if you apply this ACL to an interface:

```plaintext
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
permit tcp source source-wildcard destination destination-wildcard
```

And if this message appears:
ACLmgr-2-novmr: Cannot generate hardware representation of access list [chars]

The flag-related operators are not available. To avoid this issue,

- Move the fourth ACE before the first ACE by using `ip access-list resequence` global configuration command:

  permit tcp source source-wildcard destination destination-wildcard
  permit tcp source source-wildcard destination destination-wildcard range 5 60
  permit tcp source source-wildcard destination destination-wildcard range 15 160
  permit tcp source source-wildcard destination destination-wildcard range 115 1660

  or

- Rename the ACL with a name or number that alphanumerically precedes the other ACLs (for example, rename ACL 79 to ACL 1).

You can now apply the first ACE in the ACL to the interface. The switch allocates the ACE to available mapping bits in the Opselect index and then allocates flag-related operators to use the same bits in the hardware memory.

IPv4 ACL Configuration Examples

This section provides examples of configuring and applying IPv4 ACLs. For detailed information about compiling ACLs, see the Cisco IOS Security Configuration Guide, Release 12.4 and to the Configuring IP Services” section in the “IP Addressing and Services” chapter of the Cisco IOS IP Configuration Guide, Release 12.4.

ACLs in a Small Networked Office

Figure 46: Using Router ACLs to Control Traffic

This shows a small networked office environment with routed Port 2 connected to Server A, containing benefits and other information that all employees can access, and routed Port 1 connected to Server B, containing
confidential payroll data. All users can access Server A, but Server B has restricted access.

Use router ACLs to do this in one of two ways:

- Create a standard ACL, and filter traffic coming to the server from Port 1.
- Create an extended ACL, and filter traffic coming from the server into Port 1.

**Examples: ACLs in a Small Networked Office**

This example uses a standard ACL to filter traffic coming into Server B from a port, permitting traffic only from Accounting’s source addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic coming out of routed Port 1 from the specified source address.

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch(config)# show access-lists
Standard IP access list 6
    10 permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 6 out
```

This example uses an extended ACL to filter traffic coming from Server B into a port, permitting traffic from any source address (in this case Server B) to only the Accounting destination addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic going into routed Port 1, permitting it to go only to the specified destination addresses. Note that with extended ACLs, you must enter the protocol (IP) before the source and destination information.

```
Switch(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# end
Switch(config)# show access-lists
Extended IP access list 106
```
Example: Numbered ACLs

In this example, network 10.0.0.0 is a Class A network whose second octet specifies a subnet; that is, its subnet mask is 255.255.0.0. The third and fourth octets of a network 10.0.0.0 address specify a particular host. Using access list 2, the switch accepts one address on subnet 48 and reject all others on that subnet. The last line of the list shows that the switch accepts addresses on all other network 10.0.0.0 subnets. The ACL is applied to packets entering a port.

Examples: Extended ACLs

In this example, the first line permits any incoming TCP connections with destination ports greater than 1023. The second line permits incoming TCP connections to the Simple Mail Transfer Protocol (SMTP) port of host 128.88.1.2. The third line permits incoming ICMP messages for error feedback.

In this example, suppose that you have a network connected to the Internet, and you want any host on the network to be able to form TCP connections to any host on the Internet. However, you do not want IP hosts to be able to form TCP connections to hosts on your network, except to the mail (SMTP) port of a dedicated mail host.

SMTP uses TCP port 25 on one end of the connection and a random port number on the other end. The same port numbers are used throughout the life of the connection. Mail packets coming in from the Internet have a destination port of 25. Outbound packets have the port numbers reversed. Because the secure system of the network always accepts mail connections on port 25, the incoming and outgoing services are separately controlled. The ACL must be configured as an input ACL on the outbound interface and an output ACL on the inbound interface.

In this example, the network is a Class B network with the address 128.88.0.0, and the mail host address is 128.88.1.2. The established keyword is used only for the TCP to show an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which show that the packet belongs to an existing connection. Gigabit Ethernet interface 1 on stack member 1 is the interface that connects the router to the Internet.
Examples: Named ACLs

Creating named standard and extended ACLs

This example creates a standard ACL named internet_filter and an extended ACL named marketing_group. The internet_filter ACL allows all traffic from the source address 1.2.3.4.

Switch(config)# ip access-list standard Internet_filter
Switch(config-ext-nacl)# permit 1.2.3.4
Switch(config-ext-nacl)# exit

The marketing_group ACL allows any TCP Telnet traffic to the destination address and wildcard 171.69.0.0 0.0.255.255 and denies any other TCP traffic. It permits ICMP traffic, denies UDP traffic from any source to the destination address range 171.69.0.0 through 179.69.255.255 with a destination port less than 1024, denies any other IP traffic, and provides a log of the result.

Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit icmp any any
Switch(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Switch(config-ext-nacl)# deny ip any any log
Switch(config-ext-nacl)# exit

The Internet_filter ACL is applied to outgoing traffic and the marketing_group ACL is applied to incoming traffic on a Layer 3 port.

Switch(config)# interface gigabitethernet3/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 2.0.5.1 255.255.255.0
Switch(config-if)# ip access-group Internet_filter out
Switch(config-if)# ip access-group marketing_group in

Deleting individual ACEs from named ACLs

This example shows how you can delete individual ACEs from the named access list border-list:

Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any

Examples: Time Range Applied to an IP ACL

This example denies HTTP traffic on IP on Monday through Friday between the hours of 8:00 a.m. and 6:00 p.m (18:00). The example allows UDP traffic only on Saturday and Sunday from noon to 8:00 p.m. (20:00).
Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
!
Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
!
Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
!
Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip access-group strict in

Examples: Configuring Commented IP ACL Entries

In this example of a numbered ACL, the workstation that belongs to Jones is allowed access, and the workstation that belongs to Smith is not allowed access:

Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13

In this example of a numbered ACL, the Winter and Smith workstations are not allowed to browse the web:

Switch(config)# access-list 100 remark Do not allow Winter to browse the web
Switch(config)# access-list 100 deny host 171.69.3.85 any eq www
Switch(config)# access-list 100 remark Do not allow Smith to browse the web
Switch(config)# access-list 100 deny host 171.69.3.13 any eq www

In this example of a named ACL, the Jones subnet is not allowed access:

Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255

In this example of a named ACL, the Jones subnet is not allowed to use outbound Telnet:

Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet

Examples: ACL Logging

Two variations of logging are supported on router ACLs. The log keyword sends an informational logging message to the console about the packet that matches the entry; the log-input keyword includes the input interface in the log entry.

In this example, standard named access list stanl denies traffic from 10.1.1.0 0.0.0.255, allows traffic from all other sources, and includes the log keyword.
Switch(config)# ip access-list standard stan1
Switch(config-standard-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-standard-nacl)# permit any log
Switch(config-standard-nacl)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end
Switch# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 37 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 37 messages logged
  File logging: disabled
  Trap logging: level debugging, 39 message lines logged
Log Buffer (4096 bytes):

00:00:48: NTP: authentication delay calculation problems
<output truncated>

00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet

This example is a named extended access list ext1 that permits ICMP packets from any source to 10.1.1.0 0.0.0.255 and denies all UDP packets.

Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-standard-nacl)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip access-group ext1 in

This is an example of a log for an extended ACL:

01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (Vlan1 0001.42ef.a400), 1 packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7 packets
01:26:12:%SEC-6-IPACCESSLOGDP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1 packet
01:31:33:%SEC-6-IPACCESSLOGDP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8 packets

Note that all logging entries for IP ACLs start with %SEC-6-IPACCESSLOG with minor variations in format depending on the kind of ACL and the access entry that has been matched.

This is an example of an output message when the log-input keyword is entered:

00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1 0001.42ef.a400) -> 10.1.1.61 (0/0), 1 packet

A log message for the same sort of packet using the log keyword does not include the input interface information:
Configuration Examples for ACLs and VLAN Maps

Example: Creating an ACL and a VLAN Map to Deny a Packet

This example shows how to create an ACL and a VLAN map to deny a packet. In the first map, any packets that match the ip1 ACL (TCP packets) would be dropped. You first create the ip1 ACL to permit any TCP packet and no other packets. Because there is a match clause for IP packets in the VLAN map, the default action is to drop any IP packet that does not match any of the match clauses.

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 10
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

Example: Creating an ACL and a VLAN Map to Permit a Packet

This example shows how to create a VLAN map to permit a packet. ACL ip2 permits UDP packets and any packets that match the ip2 ACL are forwarded. In this map, any IP packets that did not match any of the previous ACLs (that is, packets that are not TCP packets or UDP packets) would get dropped.

```
Switch(config)# ip access-list extended ip2
Switch(config-ext-nacl)# permit udp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 20
Switch(config-access-map)# match ip address ip2
Switch(config-access-map)# action forward
```

Example: Default Action of Dropping IP Packets and Forwarding MAC Packets

In this example, the VLAN map has a default action of drop for IP packets and a default action of forward for MAC packets. Used with standard ACL 101 and extended named access lists igmp-match and tcp-match, the map will have the following results:

- Forward all UDP packets
- Drop all IGMP packets
- Forward all TCP packets
- Drop all other IP packets
- Forward all non-IP packets

```
Switch(config)# access-list 101 permit udp any any
Switch(config)# ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any
Switch(config)# action forward
```
Example: Default Action of Dropping MAC Packets and Forwarding IP Packets

In this example, the VLAN map has a default action of drop for MAC packets and a default action of forward for IP packets. Used with MAC extended access lists *good-hosts* and *good-protocols*, the map will have the following results:

- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Forward MAC packets with decnet-iv or vines-ip protocols
- Drop all other non-IP packets
- Forward all IP packets

```bash
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-macl)# permit host 000.0c00.0111 any
Switch(config-ext-macl)# permit host 000.0c00.0211 any
Switch(config-ext-nacl)# exit
Switch(config)# action forward
Switch(config)# mac access-list extended good-protocols
Switch(config-ext-macl)# permit any any vines-ip
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-mac-default 10
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-mac-default 20
Switch(config-access-map)# match mac address good-protocols
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

Example: Default Action of Dropping All Packets

In this example, the VLAN map has a default action of drop for all packets (IP and non-IP). Used with access lists *tcp-match* and *good-hosts* from Examples 2 and 3, the map will have the following results:

- Forward all TCP packets
- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Drop all other IP packets
- Drop all other MAC packets

```bash
Switch(config)# vlan access-map drop-all-default 10
```
Configuration Examples for Using VLAN Maps in Your Network

Example: Wiring Closet Configuration

Figure 47: Wiring Closet Configuration

In a wiring closet configuration, routing might not be enabled on the switch. In this configuration, the switch can still support a VLAN map and a QoS classification ACL. Assume that Host X and Host Y are in different VLANs and are connected to wiring closet switches A and C. Traffic from Host X to Host Y is eventually being routed by Switch B, a Layer 3 switch with routing enabled. Traffic from Host X to Host Y can be access-controlled at the traffic entry point, Switch A.

If you do not want HTTP traffic switched from Host X to Host Y, you can configure a VLAN map on Switch A to drop all HTTP traffic from Host X (IP address 10.1.1.32) to Host Y (IP address 10.1.1.34) at Switch A and not bridge it to Switch B.

First, define the IP access list http that permits (matches) any TCP traffic on the HTTP port.

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

Next, create VLAN access map map2 so that traffic that matches the http access list is dropped and all other IP traffic is forwarded.

```
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
```
Example: Restricting Access to a Server on Another VLAN

You can restrict access to a server on another VLAN. For example, server 10.1.1.100 in VLAN 10 needs to have access denied to these hosts:

- Hosts in subnet 10.1.2.0/8 in VLAN 20 should not have access.
- Hosts 10.1.1.4 and 10.1.1.8 in VLAN 10 should not have access.

Example: Denying Access to a Server on Another VLAN

This example shows how to deny access to a server on another VLAN by creating the VLAN map SERVER1 that denies access to hosts in subnet 10.1.2.0/8, host 10.1.1.4, and host 10.1.1.8 and permits other IP traffic. The final step is to apply the map SERVER1 to VLAN 10.

Define the IP ACL that will match the correct packets.

```
Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl)# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl)# exit
```
Define a VLAN map using this ACL that will drop IP packets that match SERVER1_ACL and forward IP packets that do not match the ACL.

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

Apply the VLAN map to VLAN 10.

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10
```

### Configuration Examples of Router ACLs and VLAN Maps Applied to VLANs

This section gives examples of applying router ACLs and VLAN maps to a VLAN for switched, bridged, routed, and multicast packets. Although the following illustrations show packets being forwarded to their destination, each time the packet’s path crosses a line indicating a VLAN map or an ACL, it is also possible that the packet might be dropped, rather than forwarded.

#### Example: ACLs and Switched Packets

*Figure 49: Applying ACLs on Switched Packets*

This example shows how an ACL is applied on packets that are switched within a VLAN. Packets switched within the VLAN without being routed or forwarded by fallback bridging are only subject to the VLAN map of the input VLAN.
Example: ACLs and Bridged Packets

This example shows how an ACL is applied on fallback-bridged packets. For bridged packets, only Layer 2 ACLs are applied to the input VLAN. Only non-IP, non-ARP packets can be fallback-bridged.

Example: ACLs and Routed Packets

This example shows how ACLs are applied on routed packets. The ACLs are applied in this order:

1. VLAN map for input VLAN
2. Input router ACL
3. Output router ACL
4. VLAN map for output VLAN
Example: ACLs and Multicast Packets

This example shows how ACLs are applied on packets that are replicated for IP multicasting. A multicast packet being routed has two different kinds of filters applied: one for destinations that are other ports in the input VLAN and another for each of the destinations that are in other VLANs to which the packet has been routed. The packet might be routed to more than one output VLAN, in which case a different router output ACL and VLAN map would apply for each destination VLAN. The final result is that the packet might be permitted in some of the output VLANs and not in others. A copy of the packet is forwarded to those destinations where it is permitted. However, if the input VLAN map drops the packet, no destination receives a copy of the packet.
Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for IPv4 Access Control Lists

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>IPv4 Access Control Lists perform packet filtering to control which packets move through the network and where. Such control provides security by helping to limit network traffic, restrict the access of users and devices to the network, and prevent traffic from leaving a network. This feature was introduced.</td>
</tr>
<tr>
<td>Release</td>
<td>Feature Information</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco IOS 15.2(2)E</td>
<td>The Named ACL Support for Noncontiguous Ports on an Access Control Entry feature allows you to specify noncontiguous ports in a single access control entry, which greatly reduces the number of entries required in an access control list when several entries have the same source address, destination address, and protocol, but differ only in the ports.</td>
</tr>
<tr>
<td>Cisco IOS 15.2(2)E</td>
<td>The IP Access List Entry Sequence Numbering feature helps users to apply sequence numbers to permit or deny statements and also reorder, add, or remove such statements from a named IP access list. This feature makes revising IP access lists much easier. Prior to this feature, users could add access list entries to the end of an access list only; therefore needing to add statements anywhere except the end required reconfiguring the access list entirely. The following commands were introduced or modified: <code>deny (IP)</code>, <code>ip access-list resequence deny (IP)</code>, <code>permit (IP)</code>.</td>
</tr>
</tbody>
</table>
IPv6 ACLs

- Finding Feature Information, on page 919
- IPv6 ACLs Overview, on page 919
- Restrictions for IPv6 ACLs, on page 920
- Default Configuration for IPv6 ACLs, on page 921
- Configuring IPv6 ACLs, on page 921
- Attaching an IPv6 ACL to an Interface, on page 925
- Monitoring IPv6 ACLs, on page 926
- Additional References, on page 927

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

IPv6 ACLs Overview

You can filter IP Version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similar to how you create and apply IP Version 4 (IPv4) named ACLs. You can also create and apply input router ACLs to filter Layer 3 management traffic when the switch is running IP base and LAN base feature sets.

A switch supports three types of IPv6 ACLs:

- IPv6 router ACLs are supported on outbound or inbound traffic on Layer 3 interfaces, which can be routed ports, switch virtual interfaces (SVIs), or Layer 3 EtherChannels. IPv6 router ACLs apply only to IPv6 packets that are routed.

- IPv6 port ACLs are supported on outbound and inbound Layer 2 interfaces. IPv6 port ACLs are applied to all IPv6 packets entering the interface.
• VLAN ACLs or VLAN maps access-control all packets in a VLAN. You can use VLAN maps to filter traffic between devices in the same VLAN. ACL VLAN maps are applied on L2 VLANs. VLAN maps are configured to provide access control based on Layer 3 addresses for IPv6. Unsupported protocols are access-controlled through MAC addresses using Ethernet ACEs. After a VLAN map is applied to a VLAN, all packets entering the VLAN are checked against the VLAN map.

The switch supports VLAN ACLs (VLAN maps) for IPv6 traffic.

You can apply both IPv4 and IPv6 ACLs to an interface. As with IPv4 ACLs, IPv6 port ACLs take precedence over router ACLs.

### Switch Stacks and IPv6 ACLs

The active switch supports IPv6 ACLs in hardware and distributes the IPv6 ACLs to the stack members. If a standby switch takes over as the active switch, it distributes the ACL configuration to all stack members. The member switches sync up the configuration distributed by the new active switch and flush out entries that are not required.

When an ACL is modified, attached to, or detached from an interface, the active switch distributes the change to all stack members.

### Interactions with Other Features and Switches

• If an IPv6 router ACL is configured to deny a packet, the packet is not routed. A copy of the packet is sent to the Internet Control Message Protocol (ICMP) queue to generate an ICMP unreachable message for the frame.

• If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.

• You can create both IPv4 and IPv6 ACLs on a switch or switch stack, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.

  You use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 or Layer 3 interface. If you use the wrong command to attach an ACL (for example, an IPv4 command to attach an IPv6 ACL), you receive an error message.

• You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.

• If the hardware memory is full, packets are dropped on the interface and an unload error message is logged.

### Restrictions for IPv6 ACLs

With IPv4, you can configure standard and extended numbered IP ACLs, named IP ACLs, and MAC ACLs. IPv6 supports only named ACLs.

The switch supports most Cisco IOS-supported IPv6 ACLs with some exceptions:

• The switch does not support matching on these keywords: `routing header`, and `undetermined-transport`.

• The switch does not support reflexive ACLs (the `reflect` keyword).
• This release supports port ACLs, router ACLs and VLAN ACLs (VLAN maps) for IPv6.

• The switch does not apply MAC-based ACLs on IPv6 frames.

• When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware forwarding (physical ports or SVIs), the switch checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.

• If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the switch does not allow the ACE to be added to the ACL that is currently attached to the interface.

IPv6 ACLs on the switch have these characteristics:

• Fragmented frames (the fragments keyword as in IPv4) are supported

• The same statistics supported in IPv4 are supported for IPv6 ACLs.

• If the switch runs out of hardware space, the packets associated with the ACL are dropped on the interface.

• Logging is supported for router ACLs, but not for port ACLs.

• The switch supports IPv6 address-matching for a full range of prefix-lengths.

Default Configuration for IPv6 ACLs

The default IPv6 ACL configuration is as follows:

```
Switch# show access-lists preauth_ipv6_acl
IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100
```

Configuring IPv6 ACLs

To filter IPv6 traffic, you perform these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; <strong>enable</strong></td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**
Configure terminal

Example:
Switch# configure terminal

**Step 3**

- [no] **ipv6 access-list list-name**
- **client**
- **permit-control-packets**
- **log-update**
- **threshold**
- **role-based list-name**

Example:
Switch(config)# ipv6 access-list example_acl_list

**Step 4**

- [no] **deny**
- **permit**
- **protocol**
- **source-ipv6-prefix/prefix-length**
- **any**
- **threshold**
- **host source-ipv6-address**
- **operator [port-number]**
- **destination-ipv6-prefix/prefix-length**
- **any**
- **host destination-ipv6-address**
- **operator [port-number]**
- **[dscp value]**
- **[fragments]**
- **[log]**
- **[log-input]**
- **[sequence value]**
- **[time-range name]**

Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions:

- For **protocol**, enter the name or number of an Internet protocol: **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **step**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IPv6 protocol number.

- The **source-ipv6-prefix/prefix-length** or **destination-ipv6-prefix/prefix-length** is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373).

- Enter any as an abbreviation for the IPv6 prefix **::/0**.

- For **host source-ipv6-address** or **destination-ipv6-address**, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons.

- (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range**.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the operator follows the <code>source-ipv6-prefix/prefix-length</code> argument, it must match the source port. If the operator follows the <code>destination-ipv6-prefix/prefix-length</code> argument, it must match the destination port.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) The <code>port-number</code> is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter <code>dscp</code> value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter <code>fragments</code> to check noninitial fragments. This keyword is visible only if the protocol is ipv6.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter <code>log</code> to cause an logging message to be sent to the console about the packet that matches the entry. Enter <code>log-input</code> to include the input interface in the log entry. Logging is supported only for router ACLs.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter <code>routing</code> to specify that IPv6 packets be routed.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter <code>sequence value</code> to specify the sequence number for the access list statement. The acceptable range is from 1 to 4,294,967,295.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter <code>time-range</code> name to specify the time range that applies to the deny or permit statement.</td>
<td></td>
</tr>
</tbody>
</table>
| Step 5 | `{deny | permit} tcp `  
| `source-ipv6-prefix/prefix-length | any | host `  
| `source-ipv6-address} [operator `  
| `[port-number]] `  
| `destination-ipv6-prefix/prefix-length | any | host `  
| `destination-ipv6-address} [operator `  
| `[port-number]] [ack] [dscp value]`  |
| (Optional) Define a TCP access list and the access conditions. |
| Enter `tcp` for Transmission Control Protocol. The parameters are the same as those described in Step 3a, with these additional optional parameters:
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>{{established}}</td>
<td>• \text{ack} — Acknowledgment bit set.</td>
</tr>
<tr>
<td>{{[fin]}}</td>
<td>• \text{established} — An established connection. A match occurs if the TCP datagram has the ACK or RST bits set.</td>
</tr>
<tr>
<td>{{[log]}}</td>
<td>• \text{fin} — Finished bit set; no more data from sender.</td>
</tr>
<tr>
<td>{{[log-input]}}</td>
<td>• \text{neq} {\text{port}</td>
</tr>
<tr>
<td>{{[neq} {\text{port}</td>
<td>\text{protocol}}}</td>
</tr>
<tr>
<td>{{[range} {\text{port}</td>
<td>\text{protocol}}}</td>
</tr>
<tr>
<td>{{[rst]}}</td>
<td>• \text{rst} — Reset bit set.</td>
</tr>
<tr>
<td>{{[sequence value]}}</td>
<td>• \text{syn} — Synchronize bit set.</td>
</tr>
<tr>
<td>{{[time-range name]}}</td>
<td>• \text{urg} — Urgent pointer bit set.</td>
</tr>
</tbody>
</table>

**Step 6**

\begin{verbatim}
{deny | permit} udp
{source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]]
{destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator [port-number]]
[dscp value] [log] [log-input]
[neq \{\text{port} | \text{protocol}\}] [range \{\text{port} | \text{protocol}\}]
[sequence value] [time-range name]
\end{verbatim}

(Optional) Define a UDP access list and the access conditions.

Enter \text{udp} for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the \{operator [\text{port}]\} port number or name must be a UDP port number or name, and the established parameter is not valid for UDP.

**Step 7**

\begin{verbatim}
{deny | permit} icmp
{source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]]
{destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator [port-number]]
[icmp-type] [icmp-code] [icmp-message]
[dscp value] [log] [log-input]
[sequence value] [time-range name]
\end{verbatim}

(Optional) Define an ICMP access list and the access conditions.

Enter \text{icmp} for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 1, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:

• \text{icmp-type} — Enter to filter by ICMP message type, a number from 0 to 255.

• \text{icmp-code} — Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.

• \text{icmp-message} — Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code.
### Security

#### Attaching an IPv6 ACL to an Interface

You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces, or to inbound traffic on Layer 2 interfaces. You can also apply ACLs only to inbound management traffic on Layer 3 interfaces.

Follow these steps to control access to an interface:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

---

**What to do next**

Attach the IPv6 ACL to an Interface

---

### Example:

- **Step 8**
  - `end`
  - Return to privileged EXEC mode.

- **Step 9**
  - `show ipv6 access-list`
  - Verify the access list configuration.

- **Step 10**
  - `show running-config`
  - Verifies your entries.

- **Example:**
  
  ```
  Switch# show running-config
  ```

- **Step 11**
  - `copy running-config startup-config`
  - (Optional) Saves your entries in the configuration file.
  
  ```
  Switch# copy running-config startup-config
  ```

---

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E

925
### Monitoring IPv6 ACLs

You can display information about all configured access lists, all IPv6 access lists, or a specific access list by using one or more of the privileged EXEC commands shown in the table below:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show access-lists</td>
<td>Displays all access lists configured on the switch.</td>
</tr>
<tr>
<td>show ipv6 access-list [access-list-name]</td>
<td>Displays all configured IPv6 access lists or the access list specified by name.</td>
</tr>
<tr>
<td>show vlan access-map[map-name]</td>
<td>Displays VLAN access map configuration.</td>
</tr>
<tr>
<td>show vlan filter[access-map</td>
<td>access-map_vlan</td>
</tr>
</tbody>
</table>
This is an example of the output from the show access-lists privileged EXEC command. The output shows all access lists that are configured on the switch or switch stack.

Switch # show access-lists
Extended IP access list hello
   10 permit ip any any
IPv6 access list ipv6
   permit ipv6 any any sequence 10

This is an example of the output from the show ipv6 access-list privileged EXEC command. The output shows only IPv6 access lists configured on the switch or switch stack.

Switch# show ipv6 access-list
IPv6 access list inbound
   permit tcp any any eq bgp (8 matches) sequence 10
   permit tcp any any eq telnet (15 matches) sequence 20
   permit udp any any sequence 30
IPv6 access list outbound
   deny udp any any sequence 10
   deny tcp any any eq telnet sequence 20

This is an example of the output from the show vlan access-map privileged EXEC command. The output shows VLAN access map information.

Switch# show vlan access-map
Vlan access-map "m1" 10
Match clauses:
   ipv6 address: ip2
Action: drop

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td><em>Cisco IOS Master Command List, All Releases</em></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring DHCP

- Finding Feature Information, on page 929
- Information About DHCP, on page 929
- How to Configure DHCP Features, on page 936
- Configuring DHCP Server Port-Based Address Allocation, on page 945

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About DHCP

DHCP Server

The DHCP server assigns IP addresses from specified address pools on a switch or router to DHCP clients and manages them. If the DHCP server cannot give the DHCP client the requested configuration parameters from its database, it forwards the request to one or more secondary DHCP servers defined by the network administrator. The switch can act as a DHCP server.

DHCP Relay Agent

A DHCP relay agent is a Layer 3 device that forwards DHCP packets between clients and servers. Relay agents forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is different from the normal Layer 2 forwarding, in which IP datagrams are switched transparently between networks. Relay agents receive DHCP messages and generate new DHCP messages to send on output interfaces.
DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

**Note**

For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces.

An untrusted DHCP message is a message that is received through an untrusted interface. By default, the switch considers all interfaces untrusted. So, the switch must be configured to trust some interfaces to use DHCP Snooping. When you use DHCP snooping in a service-provider environment, an untrusted message is sent from a device that is not in the service-provider network, such as a customer’s switch. Messages from unknown devices are untrusted because they can be sources of traffic attacks.

The DHCP snooping binding database has the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local untrusted interfaces of a switch. It does not have information regarding hosts interconnected with a trusted interface.

In a service-provider network, an example of an interface you might configure as trusted is one connected to a port on a device in the same network. An example of an untrusted interface is one that is connected to an untrusted interface in the network or to an interface on a device that is not in the network.

When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If the addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of these situations occurs:

- A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from outside the network or firewall.
- A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.
- The switch receives a DHCPRELEASE or DHCPDECLINE broadcast message that has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received.
- A DHCP relay agent forwards a DHCP packet that includes a relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port.
- The maximum snooping queue size of 1000 is exceeded when DHCP snooping is enabled.

**Note**

This is applicable from Cisco IOS XE Denali 16.1.x release onwards.
If the switch is an aggregation switch supporting DHCP snooping and is connected to an edge switch that is inserting DHCP option-82 information, the switch drops packets with option-82 information when packets are received on an untrusted interface. If DHCP snooping is enabled and packets are received on a trusted port, the aggregation switch does not learn the DHCP snooping bindings for connected devices and cannot build a complete DHCP snooping binding database.

When an aggregation switch can be connected to an edge switch through an untrusted interface and you enter the `ip dhcp snooping information option allow-untrusted` global configuration command, the aggregation switch accepts packets with option-82 information from the edge switch. The aggregation switch learns the bindings for hosts connected through an untrusted switch interface. The DHCP security features, such as dynamic ARP inspection or IP source guard, can still be enabled on the aggregation switch while the switch receives packets with option-82 information on untrusted input interfaces to which hosts are connected. The port on the edge switch that connects to the aggregation switch must be configured as a trusted interface.

Normally, it is not desirable to broadcast packets to wireless clients. So, DHCP snooping replaces destination broadcast MAC address (ffff.ffff.ffff) with unicast MAC address for DHCP packets that are going from server to wireless clients. The unicast MAC address is retrieved from CHADDR field in the DHCP payload. This processing is applied for server to client packets such as DHCP OFFER, DHCP ACK, and DHCP NACK messages. The `ip dhcp snooping wireless bootp-broadcast enable` can be used to revert this behavior. When the wireless BOOTP broadcast is enabled, the broadcast DHCP packets from server are forwarded to wireless clients without changing the destination MAC address.

### Option-82 Data Insertion

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

---

**Note**

The DHCP option-82 feature is supported only when DHCP snooping is globally enabled on the VLANs to which subscriber devices using option-82 are assigned.

The following illustration shows a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the switch at the access layer. Because the DHCP clients and their associated DHCP server do not reside on the same IP network or subnet, a DHCP relay agent (the Catalyst switch) is configured with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.
When you enable the DHCP snooping information option 82 on the switch, the following sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. By default, the remote-ID suboption is the switch MAC address, and the circuit-ID suboption is the port identifier, **vlan-mod-port**, from which the packet is received. You can configure the remote ID and circuit ID.
- If the IP address of the relay agent is configured, the switch adds this IP address in the DHCP packet.
- The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
- The DHCP server receives the packet. If the server is option-82-capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.
- The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. The switch verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

In the default suboption configuration, when the described sequence of events occurs, the values in these fields do not change (see the illustration, **Suboption Packet Formats**):

- Circuit-ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Circuit-ID type
  - Length of the circuit-ID type

- Remote-ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Remote-ID type
• Length of the remote-ID type

In the port field of the circuit ID suboption, the port numbers start at 3. For example, on a switch with 24 10/100/1000 ports and four small form-factor pluggable (SFP) module slots, port 3 is the Gigabit Ethernet 1/0/1 port, port 4 is the Gigabit Ethernet 1/0/2 port, and so forth. Port 27 is the SFP module slot Gigabit Ethernet1/0/25, and so forth.

The illustration, Suboption Packet Formats, shows the packet formats for the remote-ID suboption and the circuit-ID suboption when the default suboption configuration is used. For the circuit-ID suboption, the module number corresponds to the switch number in the stack. The switch uses the packet formats when you globally enable DHCP snooping and enter the ip dhcp snooping information option global configuration command.

![Suboption Packet Formats](image)

The illustration, User-Configured Suboption Packet Formats, shows the packet formats for user-configured remote-ID and circuit-ID suboptions The switch uses these packet formats when DHCP snooping is globally enabled and when the `ip dhcp snooping information option format remote-id` global configuration command and the `ip dhcp snooping vlan information option format-type circuit-id string` interface configuration command are entered.

The values for these fields in the packets change from the default values when you configure the remote-ID and circuit-ID suboptions:

• Circuit-ID suboption fields
  • The circuit-ID type is 1.
  • The length values are variable, depending on the length of the string that you configure.

• Remote-ID suboption fields
  • The remote-ID type is 1.
  • The length values are variable, depending on the length of the string that you configure.
Cisco IOS DHCP Server Database

During the DHCP-based autoconfiguration process, the designated DHCP server uses the Cisco IOS DHCP server database. It has IP addresses, address bindings, and configuration parameters, such as the boot file.

An address binding is a mapping between an IP address and a MAC address of a host in the Cisco IOS DHCP server database. You can manually assign the client IP address, or the DHCP server can allocate an IP address from a DHCP address pool. For more information about manual and automatic address bindings, see the “Configuring DHCP” chapter of the Cisco IOS IP Configuration Guide, Release 12.4.

For procedures to enable and configure the Cisco IOS DHCP server database, see the “DHCP Configuration Task List” section in the “Configuring DHCP” chapter of the Cisco IOS IP Configuration Guide, Release 12.4.

DHCP Snooping Binding Database

When DHCP snooping is enabled, the switch uses the DHCP snooping binding database to store information about untrusted interfaces. The database can have up to 64,000 bindings.

Each database entry (binding) has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. The database agent stores the bindings in a file at a configured location. At the end of each entry is a checksum that accounts for all the bytes from the start of the file through all the bytes associated with the entry. Each entry is 72 bytes, followed by a space and then the checksum value.

To keep the bindings when the switch reloads, you must use the DHCP snooping database agent. If the agent is disabled, dynamic ARP inspection or IP source guard is enabled, and the DHCP snooping binding database has dynamic bindings, the switch loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DHCP spoofing attacks.

When reloading, the switch reads the binding file to build the DHCP snooping binding database. The switch updates the file when the database changes.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. The switch also updates the entries in the binding file. The frequency at which the file is
updated is based on a configurable delay, and the updates are batched. If the file is not updated in a specified
time (set by the write-delay and abort-timeout values), the update stops.

This is the format of the file with bindings:

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
<entry-n> <checksum-1-2-..-n>
END
```

Each entry in the file is tagged with a checksum value that the switch uses to verify the entries when it reads
the file. The initial-checksum entry on the first line distinguishes entries associated with the latest file update
from entries associated with a previous file update.

This is an example of a binding file:

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Gi1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Gi1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Gi1/0/4 584a38f0
END
```

When the switch starts and the calculated checksum value equals the stored checksum value, the switch reads
entries from the binding file and adds the bindings to its DHCP snooping binding database. The switch ignores
an entry when one of these situations occurs:

- The switch reads the entry and the calculated checksum value does not equal the stored checksum value.
  The entry and the ones following it are ignored.
- An entry has an expired lease time (the switch might not remove a binding entry when the lease time
  expires).
- The interface in the entry no longer exists on the system.
- The interface is a routed interface or a DHCP snooping-trusted interface.

**DHCP Snooping and Switch Stacks**

DHCP snooping is managed on the stack master. When a new switch joins the stack, the switch receives the
DHCP snooping configuration from the stack master. When a member leaves the stack, all DHCP snooping
address bindings associated with the switch age out.

All snooping statistics are generated on the stack master. If a new stack master is elected, the statistics counters
reset.

When a stack merge occurs, all DHCP snooping bindings in the stack master are lost if it is no longer the
stack master. With a stack partition, the existing stack master is unchanged, and the bindings belonging to the

partitioned switches age out. The new master of the partitioned stack begins processing the new incoming DHCP packets.

How to Configure DHCP Features

Default DHCP Snooping Configuration

Table 66: Default DHCP Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server</td>
<td>Enabled in Cisco IOS software, requires configuration.</td>
</tr>
<tr>
<td>DHCP relay agent</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP packet forwarding address</td>
<td>None configured</td>
</tr>
<tr>
<td>Checking the relay agent information</td>
<td>Enabled (invalid messages are dropped)</td>
</tr>
<tr>
<td>DHCP relay agent forwarding policy</td>
<td>Replace the existing relay agent information</td>
</tr>
<tr>
<td>DHCP snooping enabled globally</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping information option</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP snooping option to accept packets on untrusted input interfaces</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping limit rate</td>
<td>None configured</td>
</tr>
<tr>
<td>DHCP snooping trust</td>
<td>Untrusted</td>
</tr>
<tr>
<td>DHCP snooping VLAN</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping MAC address verification</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco IOS DHCP server binding database</td>
<td>Enabled in Cisco IOS software, requires configuration. Note The switch gets network addresses and configuration parameters only from a device configured as a DHCP server.</td>
</tr>
<tr>
<td>DHCP snooping binding database agent</td>
<td>Enabled in Cisco IOS software, requires configuration. This feature is operational only when a destination is configured.</td>
</tr>
</tbody>
</table>

11 The switch responds to DHCP requests only if it is configured as a DHCP server.
12 The switch relays DHCP packets only if the IP address of the DHCP server is configured on the SVI of the DHCP client.
DHCP Snooping Configuration Guidelines

- If a switch port is connected to a DHCP server, configure a port as trusted by entering the `ip dhcp snooping trust interface` configuration command.

- If a switch port is connected to a DHCP client, configure a port as untrusted by entering the `no ip dhcp snooping trust interface` configuration command.

- You can display DHCP snooping statistics by entering the `show ip dhcp snooping statistics` user EXEC command, and you can clear the snooping statistics counters by entering the `clear ip dhcp snooping statistics` privileged EXEC command.

Configuring the DHCP Server

The switch can act as a DHCP server.

For procedures to configure the switch as a DHCP server, see the “Configuring DHCP” section of the “IP addressing and Services” section of the Cisco IOS IP Configuration Guide, Release 12.4.

DHCP Server and Switch Stacks

The DHCP binding database is managed on the stack master. When a new stack master is assigned, the new master downloads the saved binding database from the TFTP server. When a switchover happens, the new active stack master will use its database file that has been synced from the old active stack master using the SSO function. The IP addresses associated with the lost bindings are released. You should configure an automatic backup by using the `ip dhcp database url [timeout seconds | write-delay seconds]` global configuration command.

Configuring the DHCP Relay Agent

Follow these steps to enable the DHCP relay agent on the switch:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Specifying the Packet Forwarding Address

If the DHCP server and the DHCP clients are on different networks or subnets, you must configure the switch with the `ip helper-address address` interface configuration command. The general rule is to configure the command on the Layer 3 interface closest to the client. The address used in the `ip helper-address` command can be a specific DHCP server IP address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables any DHCP server to respond to requests.

Beginning in privileged EXEC mode, follow these steps to specify the packet forwarding address:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

---

### What to do next
- Checking (validating) the relay agent information
- Configuring the relay agent forwarding policy

---

### Specifying the Packet Forwarding Address

If the DHCP server and the DHCP clients are on different networks or subnets, you must configure the switch with the `ip helper-address address` interface configuration command. The general rule is to configure the command on the Layer 3 interface closest to the client. The address used in the `ip helper-address` command can be a specific DHCP server IP address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables any DHCP server to respond to requests.

Beginning in privileged EXEC mode, follow these steps to specify the packet forwarding address:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>service dhcp</td>
<td>Enables the DHCP server and relay agent on your switch. By default, this feature is enabled.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# service dhcp</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface vlan vlan-id</td>
<td>Creates a switch virtual interface by entering a VLAN ID, and enter interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config)# interface vlan 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip address ip-address subnet-mask</td>
<td>Configures the interface with an IP address and an IP subnet.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# ip address 192.108.1.27 255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ip helper-address address</td>
<td>Specifies the DHCP packet forwarding address.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# ip helper-address 172.16.1.2</td>
<td>The helper address can be a specific DHCP server address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables other servers to respond to DHCP requests.</td>
<td></td>
</tr>
<tr>
<td>If you have multiple servers, you can configure one helper address for each server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# end</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> Use one of the following: • interface range port-range • interface interface-id</td>
<td>Configures multiple physical ports that are connected to the DHCP clients, and enter interface range configuration mode. or Configures a single physical port that is connected to the DHCP client, and enter interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet1/0/2</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> switchport mode access</td>
<td>Defines the VLAN membership mode for the port.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# switchport mode access</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Prerequisites for Configuring DHCP Snooping and Option 82

The prerequisites for DHCP Snooping and Option 82 are as follows:

- You must globally enable DHCP snooping on the switch.

- Before globally enabling DHCP snooping on the switch, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.

- If you want the switch to respond to DHCP requests, it must be configured as a DHCP server.

- Before configuring the DHCP snooping information option on your switch, be sure to configure the device that is acting as the DHCP server. You must specify the IP addresses that the DHCP server can assign or exclude, or you must configure DHCP options for these devices.

- For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces. In a service-provider network, a trusted interface is connected to a port on a device in the same network.

- You must configure the switch to use the Cisco IOS DHCP server binding database to use it for DHCP snooping.

- To use the DHCP snooping option of accepting packets on untrusted inputs, the switch must be an aggregation switch that receives packets with option-82 information from an edge switch.

- The following prerequisites apply to DHCP snooping binding database configuration:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong></td>
<td>Assigns the ports to the same VLAN as configured in Step 2.</td>
</tr>
<tr>
<td>switchport access vlan <em>vlan-id</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# switchport access vlan 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
• You must configure a destination on the DHCP snooping binding database to use the switch for DHCP snooping.

• Because both NVRAM and the flash memory have limited storage capacity, we recommend that you store the binding file on a TFTP server.

• For network-based URLs (such as TFTP and FTP), you must create an empty file at the configured URL before the switch can write bindings to the binding file at that URL. See the documentation for your TFTP server to determine whether you must first create an empty file on the server; some TFTP servers cannot be configured this way.

• To ensure that the lease time in the database is accurate, we recommend that you enable and configure Network Time Protocol (NTP).

• If NTP is configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.

• Before configuring the DHCP relay agent on your switch, make sure to configure the device that is acting as the DHCP server. You must specify the IP addresses that the DHCP server can assign or exclude, configure DHCP options for devices, or set up the DHCP database agent.

• If you want the switch to relay DHCP packets, the IP address of the DHCP server must be configured on the switch virtual interface (SVI) of the DHCP client.

• If a switch port is connected to a DHCP server, configure a port as trusted by entering the `ip dhcp snooping trust interface` configuration command.

• If a switch port is connected to a DHCP client, configure a port as untrusted by entering the `no ip dhcp snooping trust` interface configuration command.

### Enabling DHCP Snooping and Option 82

Follow these steps to enable DHCP snooping on the switch:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch&gt; <code>enable</code></td>
<td><code>•</code> Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ip dhcp snooping</code></td>
<td>Enables DHCP snooping globally.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# ip dhcp snooping</td>
<td>Enables DHCP snooping on a VLAN or range of VLANs. The range is 1 to 4094. You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.</td>
</tr>
</tbody>
</table>

**Step 4**

<table>
<thead>
<tr>
<th>ip dhcp snooping vlan vlan-range</th>
<th>Enables the switch to insert and remove DHCP relay information (option-82 field) in forwarded DHCP request messages to the DHCP server. This is the default setting.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip dhcp snooping vlan 10</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

<table>
<thead>
<tr>
<th>ip dhcp snooping information option</th>
<th>Enables the switch to insert and remove DHCP relay information (option-82 field) in forwarded DHCP request messages to the DHCP server. This is the default setting.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip dhcp snooping information option</td>
<td></td>
</tr>
</tbody>
</table>

**Step 6**

| ip dhcp snooping information option format remote-id [string ASCII-string | (Optional) Configures the remote-ID suboption. |
| format remote-id string ascii| You can configure the remote ID as: |
|                             | • String of up to 63 ASCII characters (no spaces) |
|                             | • Configured hostname for the switch |
|                             | **Note** If the hostname is longer than 63 characters, it is truncated to 63 characters in the remote-ID configuration. |
|                             | The default remote ID is the switch MAC address. |
| Example:                     |                                                 |
| Switch(config)# ip dhcp snooping information option format remote-id string ascii |                                                 |

**Step 7**

<table>
<thead>
<tr>
<th>ip dhcp snooping information option allow-untrusted</th>
<th>(Optional) If the switch is an aggregation switch connected to an edge switch, this command enables the switch to accept incoming DHCP snooping packets with option-82 information from the edge switch. The default setting is disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip dhcp snooping information option allow-untrusted</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Enter this command only on aggregation switches that are connected to trusted devices.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Enables broadcast address sent by the server to be retained by the switch when it forwards DHCP packets to wireless clients.</td>
</tr>
<tr>
<td>ip dhcp snooping wireless bootp-broadcast enable (optional)</td>
<td>Enables broadcast address sent by the server to be retained by the switch when it forwards DHCP packets to wireless clients.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip dhcp snooping wireless bootp-broadcast enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>(Optional) Configures the circuit-ID suboption for the specified interface.</td>
</tr>
<tr>
<td>ip dhcp snooping vlan vlan information option format-type circuit-id override string ASCII-string</td>
<td>(Optional) Configures the circuit-ID suboption for the specified interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip dhcp snooping vlan 1 information option format-type circuit-id override string override2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>(Optional) Configures the interface as trusted or untrusted. Use the no keyword to configure an interface to receive messages from an untrusted client. The default setting is untrusted.</td>
</tr>
<tr>
<td>ip dhcp snooping trust</td>
<td>(Optional) Configures the interface as trusted or untrusted. Use the no keyword to configure an interface to receive messages from an untrusted client. The default setting is untrusted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip dhcp snooping trust</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>(Optional) Configures the number of DHCP packets per second that an interface can receive. The range is 1 to 2048. By default, no rate limit is configured.</td>
</tr>
<tr>
<td>ip dhcp snooping limit rate rate</td>
<td>(Optional) Configures the number of DHCP packets per second that an interface can receive. The range is 1 to 2048. By default, no rate limit is configured.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip dhcp snooping limit rate 100</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>We recommend an untrusted rate limit of not more than 100 packets per second. If you configure rate limiting for trusted interfaces, you might need to increase the rate limit if the port is a trunk port assigned to more than one VLAN with DHCP snooping.</td>
</tr>
<tr>
<td>Step 13</td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# exit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 14</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip dhcp snooping verify mac-address</td>
<td>(Optional) Configures the switch to verify that the source MAC address in a DHCP packet received on untrusted ports matches the client hardware address in the packet. The default is to verify that the source MAC address matches the client hardware address in the packet.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ip dhcp snooping verify mac-address</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 15</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 16</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show running-config</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 17</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

---

**Enabling the Cisco IOS DHCP Server Database**

For procedures to enable and configure the Cisco IOS DHCP server database, see the “DHCP Configuration Task List” section in the “Configuring DHCP” chapter of the Cisco IOS IP Configuration Guide, Release 12.4

**Monitoring DHCP Snooping Information**

*Table 67: Commands for Displaying DHCP Information*

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip dhcp snooping</td>
<td>Displays the DHCP snooping configuration for a switch</td>
</tr>
<tr>
<td>show ip dhcp snooping binding</td>
<td>Displays only the dynamically configured bindings in the DHCP snooping binding database, also referred to as a binding table.</td>
</tr>
</tbody>
</table>
Configuring DHCP Server Port-Based Address Allocation

Information About Configuring DHCP Server Port-Based Address Allocation

DHCP server port-based address allocation is a feature that enables DHCP to maintain the same IP address on an Ethernet switch port regardless of the attached device client identifier or client hardware address.

When Ethernet switches are deployed in the network, they offer connectivity to the directly connected devices. In some environments, such as on a factory floor, if a device fails, the replacement device must be working immediately in the existing network. With the current DHCP implementation, there is no guarantee that DHCP would offer the same IP address to the replacement device. Control, monitoring, and other software expect a stable IP address associated with each device. If a device is replaced, the address assignment should remain stable even though the DHCP client has changed.

When configured, the DHCP server port-based address allocation feature ensures that the same IP address is always offered to the same connected port even as the client identifier or client hardware address changes in the DHCP messages received on that port. The DHCP protocol recognizes DHCP clients by the client identifier option in the DHCP packet. Clients that do not include the client identifier option are identified by the client hardware address. When you configure this feature, the port name of the interface overrides the client identifier or hardware address and the actual point of connection, the switch port, becomes the client identifier.

In all cases, by connecting the Ethernet cable to the same port, the same IP address is allocated through DHCP to the attached device.

The DHCP server port-based address allocation feature is only supported on a Cisco IOS DHCP server and not a third-party server.

Default Port-Based Address Allocation Configuration

By default, DHCP server port-based address allocation is disabled.

Port-Based Address Allocation Configuration Guidelines

- By default, DHCP server port-based address allocation is disabled.
• To restrict assignments from the DHCP pool to preconfigured reservations (unreserved addresses are not offered to the client and other clients are not served by the pool), you can enter the `reserved-only` DHCP pool configuration command.

## Enabling the DHCP Snooping Binding Database Agent

Beginning in privileged EXEC mode, follow these steps to enable and configure the DHCP snooping binding database agent on the switch:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip dhcp snooping database</td>
<td>Specifies the URL for the database agent or the binding file by using one of these forms:</td>
</tr>
<tr>
<td>{flash[number]:/filename</td>
<td>ftp://user:password@host/filename</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Optional) Use the <code>number</code> parameter to specify the stack member number of the stack master. The range for <code>number</code> is 1 to 9.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip dhcp snooping database timeout <code>seconds</code></td>
<td>Specifies (in seconds) how long to wait for the database transfer process to finish before stopping the process.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# ip dhcp snooping database timeout 300</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default is 300 seconds. The range is 0 to 86400. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely.</td>
</tr>
</tbody>
</table>
### Enabling DHCP Server Port-Based Address Allocation

Follow these steps to globally enable port-based address allocation and to automatically generate a subscriber identifier on an interface.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 5** | **ip dhcp snooping database write-delay seconds**  
**Example:**  
Switch(config)# ip dhcp snooping database write-delay 15 |
| Specifies the duration for which the transfer should be delayed after the binding database changes. The range is from 15 to 86400 seconds. The default is 300 seconds (5 minutes). |
| **Step 6** | **end**  
**Example:**  
Switch(config)# end |
| Returns to privileged EXEC mode. |
| **Step 7** | **ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry expiry seconds**  
**Example:**  
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000 |
| (Optional) Adds binding entries to the DHCP snooping binding database. The vlan-id range is from 1 to 4904. The seconds range is from 1 to 4294967295. |
| **Step 8** | **show ip dhcp snooping database [detail]**  
**Example:**  
Switch# show ip dhcp snooping database detail |
| Displays the status and statistics of the DHCP snooping binding database agent. |
| **Step 9** | **show running-config**  
**Example:**  
Switch# show running-config |
| Verifies your entries. |
| **Step 10** | **copy running-config startup-config**  
**Example:**  
Switch# copy running-config startup-config |
| (Optional) Saves your entries in the configuration file. |
## Enabling DHCP Server Port-Based Address Allocation

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code> <strong>Example:</strong> <code>Switch&gt; enable</code></td>
<td>Enables privileged EXEC mode. <em>- Enter your password if prompted.</em></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code> <strong>Example:</strong> <code>Switch# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ip dhcp use subscriber-id client-id</code> <strong>Example:</strong> <code>Switch(config)# ip dhcp use subscriber-id client-id</code></td>
<td>Configures the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>ip dhcp subscriber-id interface-name</code> <strong>Example:</strong> <code>Switch(config)# ip dhcp subscriber-id interface-name</code></td>
<td>Automatically generates a subscriber identifier based on the short name of the interface. A subscriber identifier configured on a specific interface takes precedence over this command.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>interface interface-id</code> <strong>Example:</strong> <code>Switch(config)# interface gigabitethernet1/0/1</code></td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>ip dhcp server use subscriber-id client-id</code> <strong>Example:</strong> <code>Switch(config-if)# ip dhcp server use subscriber-id client-id</code></td>
<td>Configures the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on the interface.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>end</code> <strong>Example:</strong> <code>Switch(config)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>show running-config</code> <strong>Example:</strong> <code>Switch# show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
</tbody>
</table>
Monitoring DHCP Server Port-Based Address Allocation

Table 68: Commands for Displaying DHCP Port-Based Address Allocation Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface interface id</td>
<td>Displays the status and configuration of a specific interface.</td>
</tr>
<tr>
<td>show ip dhcp pool</td>
<td>Displays the DHCP address pools.</td>
</tr>
<tr>
<td>show ip dhcp binding</td>
<td>Displays address bindings on the Cisco IOS DHCP server.</td>
</tr>
</tbody>
</table>

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for DHCP Snooping and Option 82

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td></td>
<td>Introduced support for the following commands:</td>
</tr>
<tr>
<td></td>
<td>• <strong>show ip dhcp snooping statistics</strong> user EXEC command for displaying DHCP snooping</td>
</tr>
<tr>
<td></td>
<td>statistics.</td>
</tr>
<tr>
<td></td>
<td>• <strong>clear ip dhcp snooping statistics</strong> privileged EXEC command for clearing the</td>
</tr>
<tr>
<td></td>
<td>snooping statistics counters.</td>
</tr>
</tbody>
</table>
CHAPTER 51

Configuring IP Source Guard

IP Source Guard (IPSG) is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings.

This chapter contains the following topics:

• Finding Feature Information, on page 951
• Information About IP Source Guard, on page 951
• How to Configure IP Source Guard, on page 953
• Monitoring IP Source Guard, on page 956
• Additional References, on page 957

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IP Source Guard

IP Source Guard

You can use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor and you can enable IP source guard when DHCP snooping is enabled on an untrusted interface.

After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping.

The switch uses a source IP lookup table in hardware to bind IP addresses to ports. For IP and MAC filtering, a combination of source IP and source MAC lookups are used. IP traffic with a source IP address in the binding table is allowed, all other traffic is denied.
The IP source binding table has bindings that are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled. IPSG is supported only on Layer 2 ports, including access and trunk ports. You can configure IPSG with source IP address filtering or with source IP and MAC address filtering.

**IP Source Guard for Static Hosts**

- **Note**
  Do not use IPSG (IP source guard) for static hosts on uplink ports or trunk ports.

IPSG for static hosts extends the IPSG capability to non-DHCP and static environments. The previous IPSG used the entries created by DHCP snooping to validate the hosts connected to a switch. Any traffic received from a host without a valid DHCP binding entry is dropped. This security feature restricts IP traffic on nonrouted Layer 2 interfaces. It filters traffic based on the DHCP snooping binding database and on manually configured IP source bindings. The previous version of IPSG required a DHCP environment for IPSG to work.

IPSG for static hosts allows IPSG to work without DHCP. IPSG for static hosts relies on IP device tracking-table entries to install port ACLs. The switch creates static entries based on ARP requests or other IP packets to maintain the list of valid hosts for a given port. You can also specify the number of hosts allowed to send traffic to a given port. This is equivalent to port security at Layer 3.

IPSG for static hosts also supports dynamic hosts. If a dynamic host receives a DHCP-assigned IP address that is available in the IP DHCP snooping table, the same entry is learned by the IP device tracking table. In a stacked environment, when the master failover occurs, the IP source guard entries for static hosts attached to member ports are retained. When you enter the `show ip device tracking all` EXEC command, the IP device tracking table displays the entries as **ACTIVE**.

- **Note**
  Some IP hosts with multiple network interfaces can inject some invalid packets into a network interface. The invalid packets contain the IP or MAC address for another network interface of the host as the source address. The invalid packets can cause IPSG for static hosts to connect to the host, to learn the invalid IP or MAC address bindings, and to reject the valid bindings. Consult the vendor of the corresponding operating system and the network interface to prevent the host from injecting invalid packets.

IPSG for static hosts initially learns IP or MAC bindings dynamically through an ACL-based snooping mechanism. IP or MAC bindings are learned from static hosts by ARP and IP packets. They are stored in the device tracking database. When the number of IP addresses that have been dynamically learned or statically configured on a given port reaches a maximum, the hardware drops any packet with a new IP address. To resolve hosts that have moved or gone away for any reason, IPSG for static hosts leverages IP device tracking to age out dynamically learned IP address bindings. This feature can be used with DHCP snooping. Multiple bindings are established on a port that is connected to both DHCP and static hosts. For example, bindings are stored in both the device tracking database as well as in the DHCP snooping binding database.
IP Source Guard Configuration Guidelines

- You can configure static IP bindings only on nonrouted ports. If you enter the `ip source binding mac-address vlan vlan-id ip-address interface interface-id` global configuration command on a routed interface, this error message appears:

  Static IP source binding can only be configured on switch port.

- When IP source guard with source IP filtering is enabled on an interface, DHCP snooping must be enabled on the access VLAN for that interface.

- If you are enabling IP source guard on a trunk interface with multiple VLANs and DHCP snooping is enabled on all the VLANs, the source IP address filter is applied on all the VLANs.

  **Note**
  If IP source guard is enabled and you enable or disable DHCP snooping on a VLAN on the trunk interface, the switch might not properly filter traffic.

- You can enable this feature when 802.1x port-based authentication is enabled.

- When you configure IP source guard smart logging, packets with a source address other than the specified address or an address learned by DHCP are denied, and the packet contents are sent to a NetFlow collector. If you configure this feature, make sure that smart logging is globally enabled.

- In a switch stack, if IP source guard is configured on a stack member interface and you remove the the configuration of that switch by entering the `no switch stack-member-number provision` global configuration command, the interface static bindings are removed from the binding table, but they are not removed from the running configuration. If you again provision the switch by entering the `switch stack-member-number provision` command, the binding is restored.

To remove the binding from the running configuration, you must disable IP source guard before entering the `no switch provision` command. The configuration is also removed if the switch reloads while the interface is removed from the binding table.

How to Configure IP Source Guard

Enabling IP Source Guard

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt;</code> <strong>enable</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface interface-id</td>
<td>Specifies the interface to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 1/0/1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip verify source [mac-check ]</td>
<td>Enables IP source guard with source IP address filtering.</td>
</tr>
<tr>
<td>(Optional) mac-check—Enables IP Source Guard with source IP address and MAC address filtering.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip verify source</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# exit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip source binding mac-address vlan vlan-id ip-address interface interface-id</td>
<td>Adds a static IP source binding.</td>
</tr>
<tr>
<td>Enter this command for each static binding.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port

You must configure the `ip device tracking maximum limit-number` interface configuration command globally for IPSG for static hosts to work. If you only configure this command on a port without enabling IP device tracking globally or by setting an IP device tracking maximum on that interface, IPSG with static hosts rejects all the IP traffic from that interface.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch# copy running-config startup-config</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><code>Switch(config)# ip device tracking</code></td>
<td>Configures a port as access.</td>
</tr>
<tr>
<td><code>Switch(config)# interface gigabitethernet 1/0/1</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Switch(config)# interface gigabitethernet 1/0/1</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode access</code></td>
<td>Configures a port as access.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Configures the VLAN for this port.</td>
</tr>
<tr>
<td>switchport access vlan ( \text{vlan-id} )</td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Switch(config-if)# switchport access vlan 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Establishes a maximum limit for the number of static IPs that the IP device tracking table allows on the port. The range is 1 to 10. The maximum number is 10.</td>
</tr>
<tr>
<td>ip device tracking maximum ( \text{number} )</td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Switch(config-if)# ip device tracking maximum 8</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You must configure the <code>ip device tracking maximum limit-number</code> interface configuration command.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Monitoring IP Source Guard**

**Table 68: Privileged EXEC show Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip verify source [ interface interface-id ]</code></td>
<td>Displays the IP source guard configuration on the switch or on a specific interface.</td>
</tr>
<tr>
<td>`show ip device tracking { all</td>
<td>interface interface-id [ ip ip-address</td>
</tr>
</tbody>
</table>

**Table 70: Interface Configuration Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip verify source tracking</code></td>
<td>Verifies the data source.</td>
</tr>
</tbody>
</table>

For detailed information about the fields in these displays, see the command reference for this release.
# Additional References

## Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Dynamic ARP Inspection

This section lists the restrictions and guidelines for configuring Dynamic ARP Inspection on the switch.

• Dynamic ARP inspection is an ingress security feature; it does not perform any egress checking.

• Dynamic ARP inspection is not effective for hosts connected to switches that do not support dynamic ARP inspection or that do not have this feature enabled. Because man-in-the-middle attacks are limited to a single Layer 2 broadcast domain, separate the domain with dynamic ARP inspection checks from the one with no checking. This action secures the ARP caches of hosts in the domain enabled for dynamic ARP inspection.
• Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses.

When DHCP snooping is disabled or in non-DHCP environments, use ARP ACLs to permit or to deny packets.

• Dynamic ARP inspection is supported on access ports, trunk ports, and EtherChannel ports.

Note

Do not enable Dynamic ARP inspection on RSPAN VLANs. If Dynamic ARP inspection is enabled on RSPAN VLANs, Dynamic ARP inspection packets might not reach the RSPAN destination port.

• A physical port can join an EtherChannel port channel only when the trust state of the physical port and the channel port match. Otherwise, the physical port remains suspended in the port channel. A port channel inherits its trust state from the first physical port that joins the channel. Consequently, the trust state of the first physical port need not match the trust state of the channel.

Conversely, when you change the trust state on the port channel, the switch configures a new trust state on all the physical ports that comprise the channel.

• The rate limit is calculated separately on each switch in a switch stack. For a cross-stack EtherChannel, this means that the actual rate limit might be higher than the configured value. For example, if you set the rate limit to 30 pps on an EtherChannel that has one port on switch 1 and one port on switch 2, each port can receive packets at 29 pps without causing the EtherChannel to become error-disabled.

• The operating rate for the port channel is cumulative across all the physical ports within the channel. For example, if you configure the port channel with an ARP rate-limit of 400 pps, all the interfaces combined on the channel receive an aggregate 400 pps. The rate of incoming ARP packets on EtherChannel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for EtherChannel ports only after examining the rate of incoming ARP packets on the channel-port members.

The rate of incoming packets on a physical port is checked against the port-channel configuration rather than the physical-ports configuration. The rate-limit configuration on a port channel is independent of the configuration on its physical ports.

If the EtherChannel receives more ARP packets than the configured rate, the channel (including all physical ports) is placed in the error-disabled state.

• Make sure to limit the rate of ARP packets on incoming trunk ports. Configure trunk ports with higher rates to reflect their aggregation and to handle packets across multiple dynamic ARP inspection-enabled VLANs. You also can use the `ip arp inspection limit none` interface configuration command to make the rate unlimited. A high rate-limit on one VLAN can cause a denial-of-service attack to other VLANs when the software places the port in the error-disabled state.

• When you enable dynamic ARP inspection on the switch, policers that were configured to police ARP traffic are no longer effective. The result is that all ARP traffic is sent to the CPU.
Understanding Dynamic ARP Inspection

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, Host B wants to send information to Host A but does not have the MAC address of Host A in its ARP cache. Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All hosts within the broadcast domain receive the ARP request, and Host A responds with its MAC address. However, because ARP allows a gratuitous reply from a host even if an ARP request was not received, an ARP spoofing attack and the poisoning of ARP caches can occur. After the attack, all traffic from the device under attack flows through the attacker’s computer and then to the router, switch, or host.

A malicious user can attack hosts, switches, and routers connected to your Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. Figure 26-1 shows an example of ARP cache poisoning.

Figure 56: ARP Cache Poisoning

Hosts A, B, and C are connected to the switch on interfaces A, B and C, all of which are on the same subnet. Their IP and MAC addresses are shown in parentheses; for example, Host A uses IP address IA and MAC address MA. When Host A needs to communicate to Host B at the IP layer, it broadcasts an ARP request for the MAC address associated with IP address IB. When the switch and Host B receive the ARP request, they populate their ARP caches with an ARP binding for a host with the IP address IA and a MAC address MA; for example, IP address IA is bound to MAC address MA. When Host B responds, the switch and Host A populate their ARP caches with a binding for a host with the IP address IB and the MAC address MB.

Host C can poison the ARP caches of the switch, Host A, and Host B by broadcasting forged ARP responses with bindings for a host with an IP address of IA (or IB) and a MAC address of MC. Hosts with poisoned ARP caches use the MAC address MC as the destination MAC address for traffic intended for IA or IB. This means that Host C intercepts that traffic. Because Host C knows the true MAC addresses associated with IA and IB, it can forward the intercepted traffic to those hosts by using the correct MAC address as the destination. Host C has inserted itself into the traffic stream from Host A to Host B, the classic man-in-the-middle attack.

Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination
- Drops invalid ARP packets
Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

You enable dynamic ARP inspection on a per-VLAN basis by using the `ip arp inspection vlan vlan-range` global configuration command.

In non-DHCP environments, dynamic ARP inspection can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses. You define an ARP ACL by using the `arp access-list acl-name` global configuration command.

You can configure dynamic ARP inspection to drop ARP packets when the IP addresses in the packets are invalid or when the MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header. Use the `ip arp inspection validate {src-mac | dst-mac | ip}` global configuration command.

**Interface Trust States and Network Security**

Dynamic ARP inspection associates a trust state with each interface on the switch. Packets arriving on trusted interfaces bypass all dynamic ARP inspection validation checks, and those arriving on untrusted interfaces undergo the dynamic ARP inspection validation process.

In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches as trusted. With this configuration, all ARP packets entering the network from a given switch bypass the security check. No other validation is needed at any other place in the VLAN or in the network. You configure the trust setting by using the `ip arp inspection trust interface` configuration command.

---

**Caution**

Use the trust state configuration carefully. Configuring interfaces as untrusted when they should be trusted can result in a loss of connectivity.

In the following figure, assume that both Switch A and Switch B are running dynamic ARP inspection on the VLAN that includes Host 1 and Host 2. If Host 1 and Host 2 acquire their IP addresses from the DHCP server connected to Switch A, only Switch A binds the IP-to-MAC address of Host 1. Therefore, if the interface between Switch A and Switch B is untrusted, the ARP packets from Host 1 are dropped by Switch B. Connectivity between Host 1 and Host 2 is lost.
Configuring interfaces to be trusted when they are actually untrusted leaves a security hole in the network. If Switch A is not running dynamic ARP inspection, Host 1 can easily poison the ARP cache of Switch B (and Host 2, if the link between the switches is configured as trusted). This condition can occur even though Switch B is running dynamic ARP inspection.

Dynamic ARP inspection ensures that hosts (on untrusted interfaces) connected to a switch running dynamic ARP inspection do not poison the ARP caches of other hosts in the network. However, dynamic ARP inspection does not prevent hosts in other portions of the network from poisoning the caches of the hosts that are connected to a switch running dynamic ARP inspection.

In cases in which some switches in a VLAN run dynamic ARP inspection and other switches do not, configure the interfaces connecting such switches as untrusted. However, to validate the bindings of packets from nondynamic ARP inspection switches, configure the switch running dynamic ARP inspection with ARP ACLs. When you cannot determine such bindings, at Layer 3, isolate switches running dynamic ARP inspection from switches not running dynamic ARP inspection switches.

---

**Note**

Depending on the setup of the DHCP server and the network, it might not be possible to validate a given ARP packet on all switches in the VLAN.

---

### Rate Limiting of ARP Packets

The switch CPU performs dynamic ARP inspection validation checks; therefore, the number of incoming ARP packets is rate-limited to prevent a denial-of-service attack. By default, the rate for untrusted interfaces is 15 packets per second (pps). Trusted interfaces are not rate-limited. You can change this setting by using the `ip arp inspection limit` interface configuration command.

When the rate of incoming ARP packets exceeds the configured limit, the switch places the port in the error-disabled state. The port remains in that state until you intervene. You can use the `errdisable recovery` global configuration command to enable error disable recovery so that ports automatically emerge from this state after a specified timeout period.
Relative Priority of ARP ACLs and DHCP Snooping Entries

Dynamic ARP inspection uses the DHCP snooping binding database for the list of valid IP-to-MAC address bindings.

ARP ACLs take precedence over entries in the DHCP snooping binding database. The switch uses ACLs only if you configure them by using the `ip arp inspection filter vlan` global configuration command. The switch first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch also denies the packet even if a valid binding exists in the database populated by DHCP snooping.

Logging of Dropped Packets

When the switch drops a packet, it places an entry in the log buffer and then generates system messages on a rate-controlled basis. After the message is generated, the switch clears the entry from the log buffer. Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.

You use the `ip arp inspection log-buffer` global configuration command to configure the number of entries in the buffer and the number of entries needed in the specified interval to generate system messages. You specify the type of packets that are logged by using the `ip arp inspection vlan logging` global configuration command.

Default Dynamic ARP Inspection Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic ARP inspection</td>
<td>Disabled on all VLANs.</td>
</tr>
<tr>
<td>Interface trust state</td>
<td>All interfaces are untrusted.</td>
</tr>
<tr>
<td>Rate limit of incoming ARP packets</td>
<td>The rate is 15 pps on untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second. The rate is unlimited on all trusted interfaces. The burst interval is 1 second.</td>
</tr>
<tr>
<td>ARP ACLs for non-DHCP environments</td>
<td>No ARP ACLs are defined.</td>
</tr>
<tr>
<td>Validation checks</td>
<td>No checks are performed.</td>
</tr>
</tbody>
</table>
Relative Priority of ARP ACLs and DHCP Snooping Entries

Dynamic ARP inspection uses the DHCP snooping binding database for the list of valid IP-to-MAC address bindings.

ARP ACLs take precedence over entries in the DHCP snooping binding database. The switch uses ACLs only if you configure them by using the ip arp inspection filter vlan global configuration command. The switch first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch also denies the packet even if a valid binding exists in the database populated by DHCP snooping.

Configuring ARP ACLs for Non-DHCP Environments

This procedure shows how to configure dynamic ARP inspection when Switch B shown in Figure 2 does not support dynamic ARP inspection or DHCP snooping.

If you configure port 1 on Switch A as trusted, a security hole is created because both Switch A and Host 1 could be attacked by either Switch B or Host 2. To prevent this possibility, you must configure port 1 on Switch A as untrusted. To permit ARP packets from Host 2, you must set up an ARP ACL and apply it to VLAN 1. If the IP address of Host 2 is not static (it is impossible to apply the ACL configuration on Switch A) you must separate Switch A from Switch B at Layer 3 and use a router to route packets between them.

Follow these steps to configure an ARP ACL on Switch A. This procedure is required in non-DHCP environments.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

### Step 3

**arp access-list acl-name**

Defines an ARP ACL, and enters ARP access-list configuration mode. By default, no ARP access lists are defined.

**Note**

At the end of the ARP access list, there is an implicit `deny ip any mac any` command.

### Step 4

**permit ip host sender-ip mac host sender-mac**

Permits ARP packets from the specified host (Host 2).

- For `sender-ip`, enter the IP address of Host 2.
- For `sender-mac`, enter the MAC address of Host 2.

### Step 5

**exit**

Returns to global configuration mode.

### Step 6

**ip arp inspection filter arp-acl-name vlan vlan-range [static]**

Applies ARP ACL to the VLAN. By default, no defined ARP ACLs are applied to any VLAN.

- For `arp-acl-name`, specify the name of the ACL created in Step 2.
- For `vlan-range`, specify the VLAN that the switches and hosts are in. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
- (Optional) Specify `static` to treat implicit denies in the ARP ACL as explicit denies and to drop packets that do not match any previous clauses in the ACL. DHCP bindings are not used.

If you do not specify this keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL.

ARP packets containing only IP-to-MAC address bindings are compared against the...
### Configuring Dynamic ARP Inspection in DHCP Environments

#### Before you begin
This procedure shows how to configure dynamic ARP inspection when two switches support this feature. Host 1 is connected to Switch A, and Host 2 is connected to Switch B. Both switches are running dynamic...
ARP inspection on VLAN 1 where the hosts are located. A DHCP server is connected to Switch A. Both hosts acquire their IP addresses from the same DHCP server. Therefore, Switch A has the bindings for Host 1 and Host 2, and Switch B has the binding for Host 2.

Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses.

Follow these steps to configure dynamic ARP inspection. You must perform this procedure on both switches. This procedure is required.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code> &lt;br&gt; <strong>Example:</strong>&lt;br&gt;Switch&gt; <code>enable</code></td>
<td>Enables privileged EXEC mode.  &lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>show cdp neighbors</code> &lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch(config-if)# <code>show cdp neighbors</code></td>
<td>Verify the connection between the switches.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>configure terminal</code> &lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch# <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ip arp inspection vlan vlan-range</code> &lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch(config)# <code>ip arp inspection vlan 1</code></td>
<td>Enable dynamic ARP inspection on a per-VLAN basis. By default, dynamic ARP inspection is disabled on all VLANs. For vlan-range, specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. Specify the same VLAN ID for both switches.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>Interface interface-id</code> &lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch(config)# <code>interface gigabitethernet1/0/1</code></td>
<td>Specifies the interface connected to the other switch, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>ip arp inspection trust</code> &lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch(config-if)# <code>ip arp inspection trust</code></td>
<td>Configures the connection between the switches as trusted. By default, all interfaces are untrusted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>The switch does not check ARP packets that it receives from the other switch on the trusted interface. It simply forwards the packets. For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the <code>ip arp inspection vlan logging</code> global configuration command.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 7**

```
    end
Example:
Switch(config-if)#end
```

Returns to privileged EXEC mode.

**Step 8**

```
    show ip arp inspection interfaces
Example:
```

Verifies the dynamic ARP inspection configuration on interfaces.

**Step 9**

```
    show ip arp inspection vlan vlan-range
Example:
Switch(config-if)#show ip arp inspection vlan 1
```

Verifies the dynamic ARP inspection configuration on VLAN.

**Step 10**

```
    show ip dhcp snooping binding
Example:
Switch(config-if)#show ip dhcp snooping binding
```

Verifies the DHCP bindings.

**Step 11**

```
    show ip arp inspection statistics vlan vlan-range
Example:
Switch(config-if)#show ip arp inspection statistics vlan 1
```

Checks the dynamic ARP inspection statistics on VLAN.

**Step 12**

```
    configure terminal
Example:
Switch# configure terminal
```

Enters global configuration mode.

**Step 13**

```
    configure terminal
Example:
Switch# configure terminal
```

Enters global configuration mode.
Limiting the Rate of Incoming ARP Packets

The switch CPU performs dynamic ARP inspection validation checks; therefore, the number of incoming ARP packets is rate-limited to prevent a denial-of-service attack.

When the rate of incoming ARP packets exceeds the configured limit, the switch places the port in the error-disabled state. The port remains in that state until you enable error-disabled recovery so that ports automatically emerge from this state after a specified timeout period.

Note

Unless you configure a rate limit on an interface, changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed. If you enter the `no ip arp inspection limit` interface configuration command, the interface reverts to its default rate limit.

Follow these steps to limit the rate of incoming ARP packets. This procedure is optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt;</code> <code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

| **Step 2**        |         |
| `configure terminal` | Enters global configuration mode. |
| **Example:**      |         |
| `Switch# configure terminal` | |

| **Step 3**        |         |
| `interface interface-id` | Specifies the interface to be rate-limited, and enter interface configuration mode. |

| **Step 4**        |         |
| `ip arp inspection limit {rate pps [burst interval seconds] | none}` | Limits the rate of incoming ARP requests and responses on the interface. The default rate is 15 pps on untrusted interfaces and unlimited on trusted interfaces. The burst interval is 1 second. |

The keywords have these meanings:

• For `rate pps`, specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 pps.

• (Optional) For `burst interval seconds`, specify the consecutive interval in
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds, over which the interface is monitored for a high rate of ARP packets. The range is 1 to 15.</td>
</tr>
<tr>
<td>• For rate none, specify no upper limit for the rate of incoming ARP packets that can be processed.</td>
</tr>
</tbody>
</table>

### Step 5

**exit**

Returns to global configuration mode.

### Step 6

**Use the following commands:**

- `errdisable detect cause arp-inspection`
- `errdisable recovery cause arp-inspection`
- `errdisable recovery interval interval`  

(Optional) Enables error recovery from the dynamic ARP inspection error-disabled state, and configure the dynamic ARP inspection recover mechanism variables.

By default, recovery is disabled, and the recovery interval is 300 seconds.

For `interval interval`, specify the time in seconds to recover from the error-disabled state. The range is 30 to 86400.

### Step 7

**exit**

Returns to privileged EXEC mode.

### Step 8

**Use the following show commands:**

- `show ip arp inspection interfaces`
- `show errdisable recovery`

Verifies your settings.

### Step 9

**show running-config**

**Example:**

Switch# show running-config

Verifies your entries.

### Step 10

**copy running-config startup-config**

**Example:**

Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.

---

### Performing Dynamic ARP Inspection Validation Checks

Dynamic ARP inspection intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. You can configure the switch to perform additional checks on the destination MAC address, the sender and target IP addresses, and the source MAC address.

Follow these steps to perform specific checks on incoming ARP packets. This procedure is optional.
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted.  
  
  Switch> enable |
| **Step 2** configure terminal | Enters global configuration mode.  
  
  Switch# configure terminal |
| **Step 3** ip arp inspection validate {{src-mac} [dst-mac] [ip]} | Performs a specific check on incoming ARP packets. By default, no checks are performed.  
  The keywords have these meanings:  
  • For **src-mac**, check the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.  
  • For **dst-mac**, check the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.  
  • For **ip**, check the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.  
  You must specify at least one of the keywords. Each command overrides the configuration of the previous command; that is, if a command enables src and dst mac validations, and a second command enables IP validation only, the src and dst mac validations are disabled as a result of the second command. |
| **Step 4** exit | Returns to privileged EXEC mode. |
### Verifying the DAI Configuration

To display and verify the DAI configuration, use the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show arp access-list [acl-name]</code></td>
<td>Displays detailed information about ARP ACLs.</td>
</tr>
</tbody>
</table>
### Command Line Interface (CLI) Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip arp inspection interfaces [interface-id]</code></td>
<td>Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.</td>
</tr>
<tr>
<td><code>show ip arp inspection vlan vlan-range</code></td>
<td>Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN. If no VLANs are specified or if a range is specified, displays information only for VLANs with dynamic ARP inspection enabled (active).</td>
</tr>
</tbody>
</table>

### Additional References

#### Error Message Decoder

To help you research and resolve system error messages in this release, use the Error Message Decoder tool.

- **Description**: To help you research and resolve system error messages in this release, use the Error Message Decoder tool.
- **Link**: [https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi](https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi)

#### MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

- **MIB**: All the supported MIBs for this release.
- **MIBs Link**: [http://www.cisco.com/go/mibs](http://www.cisco.com/go/mibs)

#### Technical Assistance

The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.

To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.

Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.

- **Description**: The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.
- **Link**: [http://www.cisco.com/support](http://www.cisco.com/support)
CHAPTER 53

Configuring IEEE 802.1x Port-Based Authentication

This chapter describes how to configure IEEE 802.1x port-based authentication. IEEE 802.1x authentication prevents unauthorized devices (clients) from gaining access to the network. Unless otherwise noted, the term switch refers to a standalone switch or a switch stack.

- Finding Feature Information, on page 975
- Information About 802.1x Port-Based Authentication, on page 975
- How to Configure 802.1x Port-Based Authentication, on page 1008
- Monitoring 802.1x Statistics and Status, on page 1057
- Additional References for IEEE 802.1x Port-Based Authentication, on page 1058
- Feature Information for 802.1x Port-Based Authentication, on page 1059

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About 802.1x Port-Based Authentication

The 802.1x standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Note

TACACS is not supported with 802.1x authentication.
Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

The table shown below lists the maximum number of each client session supported on Catalyst 3850 and Catalyst 3650 switches:

<table>
<thead>
<tr>
<th>Client session</th>
<th>Maximum sessions supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum dot1x or MAB client sessions</td>
<td>2000</td>
</tr>
<tr>
<td>Maximum web-based authentication sessions</td>
<td>2000</td>
</tr>
<tr>
<td>Maximum dot1x sessions with critical-auth VLAN enabled and server re-initialized</td>
<td>2000</td>
</tr>
<tr>
<td>Maximum MAB sessions with various session features applied</td>
<td>2000</td>
</tr>
<tr>
<td>Maximum dot1x sessions with service templates or session features applied</td>
<td>2000</td>
</tr>
</tbody>
</table>

**Port-Based Authentication Process**

To configure IEEE 802.1X port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

The AAA process begins with authentication. When 802.1x port-based authentication is enabled and the client supports 802.1x-compliant client software, these events occur:

- If the client identity is valid and the 802.1x authentication succeeds, the switch grants the client access to the network.

- If 802.1x authentication times out while waiting for an EAPOL message exchange and MAC authentication bypass is enabled, the switch can use the client MAC address for authorization. If the client MAC address is valid and the authorization succeeds, the switch grants the client access to the network. If the client MAC address is invalid and the authorization fails, the switch assigns the client to a guest VLAN that provides limited services if a guest VLAN is configured.

- If the switch gets an invalid identity from an 802.1x-capable client and a restricted VLAN is specified, the switch can assign the client to a restricted VLAN that provides limited services.

- If the RADIUS authentication server is unavailable (down) and inaccessible authentication bypass is enabled, the switch grants the client access to the network by putting the port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN.

**Note**

Inaccessible authentication bypass is also referred to as critical authentication or the AAA failure policy.

If Multi Domain Authentication (MDA) is enabled on a port, this flow can be used with some exceptions that are applicable to voice authorization.
This figure shows the authentication process.

The switch re-authenticates a client when one of these situations occurs:

- Periodic re-authentication is enabled, and the re-authentication timer expires.

You can configure the re-authentication timer to use a switch-specific value or to be based on values from the RADIUS server.

After 802.1x authentication using a RADIUS server is configured, the switch uses timers based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]).

The Session-Timeout RADIUS attribute (Attribute[27]) specifies the time after which re-authentication occurs.

The Termination-Action RADIUS attribute (Attribute [29]) specifies the action to take during re-authentication. The actions are Initialize and ReAuthenticate. When the Initialize action is set (the attribute value is DEFAULT), the 802.1x session ends, and connectivity is lost during re-authentication. When the ReAuthenticate action is set (the attribute value is RADIUS-Request), the session is not affected during re-authentication.

- You manually re-authenticate the client by entering the `dot1x re-authenticate interface interface-id` privileged EXEC command.
Port-Based Authentication Initiation and Message Exchange

During 802.1x authentication, the switch or the client can initiate authentication. If you enable authentication on a port by using the `authentication port-control auto` interface configuration command, the switch initiates authentication when the link state changes from down to up or periodically as long as the port remains up and unauthenticated. The switch sends an EAP-request/identity frame to the client to request its identity. Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client’s identity.

---

**Note**

If 802.1x authentication is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client sends frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized. If the authentication fails, authentication can be retried, the port might be assigned to a VLAN that provides limited services, or network access is not granted.

The specific exchange of EAP frames depends on the authentication method being used.

*Figure 59: Message Exchange*

This figure shows a message exchange initiated by the client when the client uses the One-Time-Password (OTP) authentication method with a RADIUS server.

---

If 802.1x authentication times out while waiting for an EAPOL message exchange and MAC authentication bypass is enabled, the switch can authorize the client when the switch detects an Ethernet packet from the
client. The switch uses the MAC address of the client as its identity and includes this information in the RADIUS-access/request frame that is sent to the RADIUS server. After the server sends the switch the RADIUS-access/accept frame (authorization is successful), the port becomes authorized. If authorization fails and a guest VLAN is specified, the switch assigns the port to the guest VLAN. If the switch detects an EAPOL packet while waiting for an Ethernet packet, the switch stops the MAC authentication bypass process and starts 802.1x authentication.

Figure 60: Message Exchange During MAC Authentication Bypass

This figure shows the message exchange during MAC authentication bypass.

Authentication Manager for Port-Based Authentication

Port-Based Authentication Methods

Table 71: 802.1x Features

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Mode</th>
<th>Single host</th>
<th>Multiple host</th>
<th>MDA</th>
<th>Multiple Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
</tr>
<tr>
<td></td>
<td>Per-user ACL</td>
<td>Per-user ACL</td>
<td>Per-user ACL</td>
<td>Per-user ACL</td>
<td>Per-user ACL</td>
</tr>
<tr>
<td></td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
</tr>
<tr>
<td></td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
</tr>
<tr>
<td></td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
</tr>
</tbody>
</table>
### Authentication method

<table>
<thead>
<tr>
<th>Mode</th>
<th>Single host</th>
<th>Multiple host</th>
<th>MDA</th>
<th>Multiple Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC authentication bypass</td>
<td>VLAN assignment&lt;br&gt;Per-user ACL&lt;br&gt;Filter-ID attribute&lt;br&gt;Downloadable ACL&lt;br&gt;Redirect URL</td>
<td>VLAN assignment&lt;br&gt;Per-user ACL&lt;br&gt;Filter-ID attribute&lt;br&gt;Downloadable ACL&lt;br&gt;Redirect URL</td>
<td>VLAN assignment&lt;br&gt;Per-user ACL&lt;br&gt;Filter-ID attribute&lt;br&gt;Downloadable ACL&lt;br&gt;Redirect URL</td>
<td>VLAN assignment&lt;br&gt;Per-user ACL&lt;br&gt;Filter-ID attribute&lt;br&gt;Downloadable ACL&lt;br&gt;Redirect URL</td>
</tr>
<tr>
<td>Standalone web authentication</td>
<td>Proxy ACL, Filter-Id attribute, downloadable ACL</td>
<td>Proxy ACL, Filter-Id attribute, downloadable ACL</td>
<td>Proxy ACL, Filter-Id attribute, downloadable ACL</td>
<td>Proxy ACL, Filter-Id attribute, downloadable ACL</td>
</tr>
<tr>
<td>NAC Layer 2 IP validation</td>
<td>Filter-ID attribute&lt;br&gt;Downloadable ACL&lt;br&gt;Redirect URL</td>
<td>Filter-ID attribute&lt;br&gt;Downloadable ACL&lt;br&gt;Redirect URL</td>
<td>Filter-ID attribute&lt;br&gt;Downloadable ACL&lt;br&gt;Redirect URL</td>
<td>Filter-ID attribute&lt;br&gt;Downloadable ACL&lt;br&gt;Redirect URL</td>
</tr>
<tr>
<td>Web authentication as fallback method</td>
<td>Proxy ACL&lt;br&gt;Filter-ID attribute&lt;br&gt;Downloadable ACL</td>
<td>Proxy ACL&lt;br&gt;Filter-ID attribute&lt;br&gt;Downloadable ACL</td>
<td>Proxy ACL&lt;br&gt;Filter-ID attribute&lt;br&gt;Downloadable ACL</td>
<td>Proxy ACL&lt;br&gt;Filter-ID attribute&lt;br&gt;Downloadable ACL</td>
</tr>
</tbody>
</table>

---

14 Supported in Cisco IOS Release 12.2(50)SE and later.<br>
15 For clients that do not support 802.1x authentication.

---

### Per-User ACLs and Filter-Ids

**Note**

You can only set `any` as the source in the ACL.

**Note**

For any ACL configured for multiple-host mode, the source portion of statement must be `any`. (For example, `permit icmp any host 10.10.1.1`.)

You must specify `any` in the source ports of any defined ACL. Otherwise, the ACL cannot be applied and authorization fails. Single host is the only exception to support backward compatibility.

More than one host can be authenticated on MDA-enabled and multiauth ports. The ACL policy applied for one host does not effect the traffic of another host. If only one host is authenticated on a multi-host port, and the other hosts gain network access without authentication, the ACL policy for the first host can be applied to the other connected hosts by specifying any in the source address.
Port-Based Authentication Manager CLI Commands

The authentication-manager interface-configuration commands control all the authentication methods, such as 802.1x, MAC authentication bypass, and web authentication. The authentication manager commands determine the priority and order of authentication methods applied to a connected host.

The authentication manager commands control generic authentication features, such as host-mode, violation mode, and the authentication timer. Generic authentication commands include the **authentication host-mode**, **authentication violation**, and **authentication timer** interface configuration commands.

802.1x-specific commands begin with the `dot1x` keyword. For example, the **authentication port-control auto** interface configuration command enables authentication on an interface.

To disable dot1x on a switch, remove the configuration globally by using the no dot1x system-auth-control, and also remove it from all configured interfaces.

---

**Note**

If 802.1x authentication is globally disabled, other authentication methods are still enabled on that port, such as web authentication.

The **authentication manager** commands provide the same functionality as earlier 802.1x commands.

When filtering out verbose system messages generated by the authentication manager, the filtered content typically relates to authentication success. You can also filter verbose messages for 802.1x authentication and MAB authentication. There is a separate command for each authentication method:

- The **no authentication logging verbose** global configuration command filters verbose messages from the authentication manager.
- The **no dot1x logging verbose** global configuration command filters 802.1x authentication verbose messages.
- The **no mab logging verbose** global configuration command filters MAC authentication bypass (MAB) verbose messages

---

**Table 72: Authentication Manager Commands and Earlier 802.1x Commands**

<table>
<thead>
<tr>
<th>The authentication manager commands in Cisco IOS Release 12.2(50)SE or later</th>
<th>The equivalent 802.1x commands in Cisco IOS Release 12.2(46)SE and earlier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>authentication control-direction</strong> {both</td>
<td>in}</td>
<td><strong>dot1x control-direction</strong> {both</td>
</tr>
<tr>
<td><strong>authentication event</strong></td>
<td><strong>dot1x auth-fail vlan</strong>&lt;br&gt;<strong>dot1x critical (interface configuration)</strong>&lt;br&gt;<strong>dot1x guest-vlan6</strong></td>
<td>Enable the restricted VLAN on a port.&lt;br&gt;Enable the inaccessible-authentication-bypass feature.&lt;br&gt;Specify an active VLAN as an 802.1x guest VLAN.</td>
</tr>
<tr>
<td>The authentication manager commands in Cisco IOS Release 12.2(50)SE or later</td>
<td>The equivalent 802.1x commands in Cisco IOS Release 12.2(46)SE and earlier</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>authentication fallback</strong>&lt;br&gt;<em>fallback-profile</em></td>
<td><strong>dot1x fallback</strong>&lt;br&gt;<em>fallback-profile</em></td>
<td>Configure a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.</td>
</tr>
<tr>
<td><strong>authentication host-mode</strong>&lt;br&gt;multi-auth</td>
<td><strong>dot1x host-mode</strong> single-host</td>
<td>Allow a single host (client) or multiple hosts on an 802.1x-authorized port.</td>
</tr>
<tr>
<td><strong>authentication host-mode</strong>&lt;br&gt;multi-domain</td>
<td><strong>dot1x host-mode</strong> multi-host</td>
<td></td>
</tr>
<tr>
<td><strong>authentication host-mode</strong>&lt;br&gt;multi-host</td>
<td><strong>dot1x host-mode</strong> multi-domain</td>
<td></td>
</tr>
<tr>
<td><strong>authentication order</strong></td>
<td><strong>mab</strong></td>
<td>Provides the flexibility to define the order of authentication methods to be used.</td>
</tr>
<tr>
<td><strong>authentication order</strong></td>
<td><strong>dot1x reauthentication</strong></td>
<td>Enable periodic re-authentication of the client.</td>
</tr>
<tr>
<td><strong>authentication port-control</strong> auto</td>
<td><strong>dot1x port-control</strong> auto</td>
<td>Enable manual control of the authorization state of the port.</td>
</tr>
<tr>
<td></td>
<td>force-authorized</td>
<td></td>
</tr>
<tr>
<td></td>
<td>force-unauthorized</td>
<td></td>
</tr>
<tr>
<td><strong>authentication timer</strong></td>
<td><strong>dot1x timeout</strong></td>
<td>Set the 802.1x timers.</td>
</tr>
<tr>
<td><strong>authentication violation</strong> protect</td>
<td><strong>dot1x violation-mode</strong> shutdown</td>
<td>Configure the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.</td>
</tr>
<tr>
<td></td>
<td>restrict</td>
<td></td>
</tr>
<tr>
<td></td>
<td>shutdown</td>
<td></td>
</tr>
<tr>
<td></td>
<td>protect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>restrict</td>
<td></td>
</tr>
</tbody>
</table>

### Ports in Authorized and Unauthorized States

During 802.1x authentication, depending on the switch port state, the switch can grant a client access to the network. The port starts in the unauthorized state. While in this state, the port that is not configured as a voice VLAN port disallows all ingress and egress traffic except for 802.1x authentication, CDP, and STP packets. When a client is successfully authenticated, the port changes to the authorized state, allowing all traffic for the client to flow normally. If the port is configured as a voice VLAN port, the port allows VoIP traffic and 802.1x protocol packets before the client is successfully authenticated.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP bypass is not supported and may cause a port to go into err-disabled state.</td>
</tr>
</tbody>
</table>

If a client that does not support 802.1x authentication connects to an unauthorized 802.1x port, the switch requests the client’s identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1x-enabled client connects to a port that is not running the 802.1x standard, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the...
client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.

You control the port authorization state by using the **authentication port-control** interface configuration command and these keywords:

- **force-authorized** — disables 802.1x authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without 802.1x-based authentication of the client. This is the default setting.

- **force-unauthorized** — causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.

- **auto** — enables 802.1x authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client MAC address.

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can resend the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to change to the unauthorized state.

If the link state of a port changes from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

### Port-Based Authentication and Switch Stacks

If a switch is added to or removed from a switch stack, 802.1x authentication is not affected as long as the IP connectivity between the RADIUS server and the stack remains intact. This statement also applies if the stack master is removed from the switch stack. Note that if the stack master fails, a stack member becomes the new stack master by using the election process, and the 802.1x authentication process continues as usual.

If IP connectivity to the RADIUS server is interrupted because the switch that was connected to the server is removed or fails, these events occur:

- Ports that are already authenticated and that do not have periodic re-authentication enabled remain in the authenticated state. Communication with the RADIUS server is not required.

- Ports that are already authenticated and that have periodic re-authentication enabled (with the `dot1x re-authentication` global configuration command) fail the authentication process when the re-authentication occurs. Ports return to the unauthenticated state during the re-authentication process. Communication with the RADIUS server is required.

  For an ongoing authentication, the authentication fails immediately because there is no server connectivity.

If the switch that failed comes up and rejoins the switch stack, the authentications might or might not fail depending on the boot-up time and whether the connectivity to the RADIUS server is re-established by the time the authentication is attempted.
To avoid loss of connectivity to the RADIUS server, you should ensure that there is a redundant connection to it. For example, you can have a redundant connection to the stack master and another to a stack member, and if the stack master fails, the switch stack still has connectivity to the RADIUS server.

### 802.1x Host Mode

You can configure an 802.1x port for single-host or for multiple-hosts mode. In single-host mode, only one client can be connected to the 802.1x-enabled switch port. The switch detects the client by sending an EAPOL frame when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

In multiple-hosts mode, you can attach multiple hosts to a single 802.1x-enabled port. In this mode, only one of the attached clients must be authorized for all clients to be granted network access. If the port becomes unauthorized (re-authentication fails or an EAPOL-logoff message is received), the switch denies network access to all of the attached clients.

In this topology, the wireless access point is responsible for authenticating the clients attached to it, and it also acts as a client to the switch.

*Figure 61: Multiple Host Mode Example*

For all host modes, the line protocol stays up before authorization when port-based authentication is configured.

The switch supports multidomain authentication (MDA), which allows both a data device and a voice device, such as an IP Phone (Cisco or non-Cisco), to connect to the same switch port.

### 802.1x Multiple Authentication Mode

Multiple-authentication (multiauth) mode allows multiple authenticated clients on the data VLAN. Each host is individually authenticated. If a voice VLAN is configured, this mode also allows one client on the VLAN. (If the port detects any additional voice clients, they are discarded from the port, but no violation errors occur.)

If a hub or access point is connected to an 802.1x-enabled port, each connected client must be authenticated. For non-802.1x devices, you can use MAC authentication bypass or web authentication as the per-host authentication fallback method to authenticate different hosts with different methods on a single port.

There is no limit to the number of data hosts can authenticate on a multiauthport. However, only one voice device is allowed if the voice VLAN is configured. Since there is no host limit defined violation will not be trigger, if a second voice is seen we silently discard it but do not trigger violation. For MDA functionality on the voice VLAN, multiple-authentication mode assigns authenticated devices to either a data or a voice VLAN, depending on the VSAs received from the authentication server.
When a port is in multiple-authentication mode, the guest VLAN and the authentication-failed VLAN features do not activate.

You can assign a RADIUS-server-supplied VLAN in multi-auth mode, under the following conditions:

- The host is the first host authorized on the port, and the RADIUS server supplies VLAN information.
- Subsequent hosts are authorized with a VLAN that matches the operational VLAN.
- A host is authorized on the port with no VLAN assignment, and subsequent hosts either have no VLAN assignment, or their VLAN information matches the operational VLAN.
- The first host authorized on the port has a group VLAN assignment, and subsequent hosts either have no VLAN assignment, or their group VLAN matches the group VLAN on the port. Subsequent hosts must use the same VLAN from the VLAN group as the first host. If a VLAN list is used, all hosts are subject to the conditions specified in the VLAN list.
- Only one voice VLAN assignment is supported on a multi-auth port.
- After a VLAN is assigned to a host on the port, subsequent hosts must have matching VLAN information or be denied access to the port.
- You cannot configure a guest VLAN or an auth-fail VLAN in multi-auth mode.
- The behavior of the critical-auth VLAN is not changed for multi-auth mode. When a host tries to authenticate and the server is not reachable, all authorized hosts are reinitialized in the configured VLAN.

Multi-auth Per User VLAN assignment

The Multi-auth Per User VLAN assignment feature allows you to create multiple operational access VLANs based on VLANs assigned to the clients on the port that has a single configured access VLAN. The port configured as an access port where the traffic for all the VLANs associated with data domain is not dot1q tagged, and these VLANs are treated as native VLANs.

The number of hosts per multi-auth port is 8, however there can be more hosts.

The Multi-auth Per User VLAN assignment feature is not supported for Voice domain. All clients in Voice domain on a port must use the same VLAN.

The following scenarios are associated with the multi-auth Per User VLAN assignments:

Scenario one

When a hub is connected to an access port, and the port is configured with an access VLAN (V0).

The host (H1) is assigned to VLAN (V1) through the hub. The operational VLAN of the port is changed to V1. This behaviour is similar on a single-host or multi-domain-auth port.

When a second host (H2) is connected and gets assigned to VLAN (V2), the port will have two operational VLANs (V1 and V2). If H1 and H2 sends untagged ingress traffic, H1 traffic is mapped to VLAN (V1) and H2 traffic to VLAN (V2), all egress traffic going out of the port on VLAN (V1) and VLAN (V2) are untagged.
If both the hosts, H1 and H2 are logged out or the sessions are removed due to some reason then VLAN (V1) and VLAN (V2) are removed from the port, and the configured VLAN (V0) is restored on the port.

**Scenario two**

When a hub is connected to an access port, and the port is configured with an access VLAN (V0). The host (H1) is assigned to VLAN (V1) through the hub. The operational VLAN of the port is changed to V1.

When a second host (H2) is connected and gets authorized without explicit vlan policy, H2 is expected to use the configured VLAN (V0) that is restored on the port. All egress traffic going out of two operational VLANs, VLAN (V0) and VLAN (V1) are untagged.

If host (H2) is logged out or the session is removed due to some reason then the configured VLAN (V0) is removed from the port, and VLAN (V1) becomes the only operational VLAN on the port.

**Scenario three**

When a hub is connected to an access port in open mode, and the port is configured with an access VLAN (V0).

The host (H1) is assigned to VLAN (V1) through the hub. The operational VLAN of the port is changed to V1. When a second host (H2) is connected and remains unauthorized, it still has access to operational VLAN (V1) due to open mode.

If host H1 is logged out or the session is removed due to some reason, VLAN (V1) is removed from the port and host (H2) gets assigned to VLAN (V0).

---

**Note**

The combination of Open mode and VLAN assignment has an adverse affect on host (H2) because it has an IP address in the subnet that corresponds to VLAN (V1).

---

**Limitation in Multi-auth Per User VLAN assignment**

In the Multi-auth Per User VLAN assignment feature, egress traffic from multiple vlans are untagged on a port where the hosts receive traffic that is not meant for them. This can be a problem with broadcast and multicast traffic.

- **IPv4 ARPs**: Hosts receive ARP packets from other subnets. This is a problem if two subnets in different Virtual Routing and Forwarding (VRF) tables with overlapping IP address range are active on the port. The host ARP cache may get invalid entries.

- **IPv6 control packets**: In IPv6 deployments, Router Advertisements (RA) are processed by hosts that are not supposed to receive them. When a host from one VLAN receives RA from a different VLAN, the host assign incorrect IPv6 address to itself. Such a host is unable to get access to the network.

  The workaround is to enable the IPv6 first hop security so that the broadcast ICMPv6 packets are converted to unicast and sent out from multi-auth enabled ports. The packet is replicated for each client in multi-auth port belonging to the VLAN and the destination MAC is set to an individual client. Ports having one VLAN, ICMPv6 packets broadcast normally.

- **IP multicast**: Multicast traffic destined to a multicast group gets replicated for different VLANs if the hosts on those VLANs join the multicast group. When two hosts in different VLANs join a multicast group (on the same multi-auth port), two copies of each multicast packet are sent out from that port.
MAC Move

When a MAC address is authenticated on one switch port, that address is not allowed on another authentication manager-enabled port of the switch. If the switch detects that same MAC address on another authentication manager-enabled port, the address is not allowed.

There are situations where a MAC address might need to move from one port to another on the same switch. For example, when there is another device (for example a hub or an IP phone) between an authenticated host and a switch port, you might want to disconnect the host from the device and connect it directly to another port on the same switch.

You can globally enable MAC move so the device is reauthenticated on the new port. When a host moves to a second port, the session on the first port is deleted, and the host is reauthenticated on the new port. MAC move is supported on all host modes. (The authenticated host can move to any port on the switch, no matter which host mode is enabled on the that port.) When a MAC address moves from one port to another, the switch terminates the authenticated session on the original port and initiates a new authentication sequence on the new port. The MAC move feature applies to both voice and data hosts.

In open authentication mode, a MAC address is immediately moved from the original port to the new port, with no requirement for authorization on the new port.

MAC Replace

The MAC replace feature can be configured to address the violation that occurs when a host attempts to connect to a port where another host was previously authenticated.

This feature does not apply to ports in multi-auth mode, because violations are not triggered in that mode. It does not apply to ports in multiple host mode, because in that mode, only the first host requires authentication.

If you configure the `authentication violation` interface configuration command with the `replace` keyword, the authentication process on a port in multi-domain mode is:

- A new MAC address is received on a port with an existing authenticated MAC address.
- The authentication manager replaces the MAC address of the current data host on the port with the new MAC address.
- The authentication manager initiates the authentication process for the new MAC address.
- If the authentication manager determines that the new host is a voice host, the original voice host is removed.

If a port is in open authentication mode, any new MAC address is immediately added to the MAC address table.
802.1x Accounting

The 802.1x standard defines how users are authorized and authenticated for network access but does not keep track of network usage. 802.1x accounting is disabled by default. You can enable 802.1x accounting to monitor this activity on 802.1x-enabled ports:

- User successfully authenticates.
- User logs off.
- Link-down occurs.
- Re-authentication successfully occurs.
- Re-authentication fails.

The switch does not log 802.1x accounting information. Instead, it sends this information to the RADIUS server, which must be configured to log accounting messages.

802.1x Accounting Attribute-Value Pairs

The information sent to the RADIUS server is represented in the form of Attribute-Value (AV) pairs. These AV pairs provide data for different applications. (For example, a billing application might require information that is in the Acct-Input-Octets or the Acct-Output-Octets attributes of a RADIUS packet.)

AV pairs are automatically sent by a switch that is configured for 802.1x accounting. Three types of RADIUS accounting packets are sent by a switch:

- START—sent when a new user session starts
- INTERIM—sent during an existing session for updates
- STOP—sent when a session terminates

You can view the AV pairs that are being sent by the switch by entering the debug radius accounting privileged EXEC command. For more information about this command, see the Cisco IOS Debug Command Reference, Release 12.4.

This table lists the AV pairs and when they are sent are sent by the switch.

Table 73: Accounting AV Pairs

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>AV Pair Name</th>
<th>START</th>
<th>INTERIM</th>
<th>STOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute[1]</td>
<td>User-Name</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[4]</td>
<td>NAS-IP-Address</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[5]</td>
<td>NAS-Port</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[8]</td>
<td>Framed-IP-Address</td>
<td>Never</td>
<td>Sometimes$^{16}$</td>
<td>Sometimes</td>
</tr>
<tr>
<td>Attribute[25]</td>
<td>Class</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[30]</td>
<td>Called-Station-ID</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
</tbody>
</table>
The Framed-IP-Address AV pair is sent when a valid static IP address is configured or when a Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.

### 802.1x Readiness Check

The 802.1x readiness check monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable. You use an alternate authentication such as MAC authentication bypass or web authentication for the devices that do not support 802.1x functionality.

This feature only works if the supplicant on the client supports a query with the NOTIFY EAP notification packet. The client must respond within the 802.1x timeout value.

### Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by their hostname or IP address, hostname and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order that they were configured.

### 802.1x Authentication with VLAN Assignment

The switch supports 802.1x authentication with VLAN assignment. After successful 802.1x authentication of a port, the RADIUS server sends the VLAN assignment to configure the switch port. The RADIUS server

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>AV Pair Name</th>
<th>START</th>
<th>INTERIM</th>
<th>STOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute[31]</td>
<td>Calling-Station-ID</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[40]</td>
<td>Acct-Status-Type</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[41]</td>
<td>Acct-Delay-Time</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[42]</td>
<td>Acct-Input-Octets</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[43]</td>
<td>Acct-Output-Octets</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[47]</td>
<td>Acct-Input-Packets</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[48]</td>
<td>Acct-Output-Packets</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[44]</td>
<td>Acct-Session-ID</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[45]</td>
<td>Acct-Authentic</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[46]</td>
<td>Acct-Session-Time</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[49]</td>
<td>Acct-Terminate-Cause</td>
<td>Never</td>
<td>Never</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[61]</td>
<td>NAS-Port-Type</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
</tbody>
</table>

16 The Framed-IP-Address AV pair is sent when a valid static IP address is configured or when a Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.
database maintains the username-to-VLAN mappings, assigning the VLAN based on the username of the client connected to the switch port. You can use this feature to limit network access for certain users.

Voice device authentication is supported with multidomain host mode in Cisco IOS Release 12.2(37)SE. In Cisco IOS Release 12.2(40)SE and later, when a voice device is authorized and the RADIUS server returned an authorized VLAN, the voice VLAN on the port is configured to send and receive packets on the assigned voice VLAN. Voice VLAN assignment behaves the same as data VLAN assignment on multidomain authentication (MDA)-enabled ports.

When configured on the switch and the RADIUS server, 802.1x authentication with VLAN assignment has these characteristics:

- If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port is configured in its access VLAN after successful authentication. Recall that an access VLAN is a VLAN assigned to an access port. All packets sent from or received on this port belong to this VLAN.

- If 802.1x authentication is enabled but the VLAN information from the RADIUS server is not valid, authorization fails and configured VLAN remains in use. This prevents ports from appearing unexpectedly in an inappropriate VLAN because of a configuration error.

Configuration errors could include specifying a VLAN for a routed port, a malformed VLAN ID, a nonexistent or internal (routed port) VLAN ID, an RSPAN VLAN, a shut down or suspended VLAN.

In the case of a multidomain host port, configuration errors can also be due to an attempted assignment of a data VLAN that matches the configured or assigned voice VLAN ID (or the reverse).

- If 802.1x authentication is enabled and all information from the RADIUS server is valid, the authorized device is placed in the specified VLAN after authentication.

- If the multiple-hosts mode is enabled on an 802.1x port, all hosts are placed in the same VLAN (specified by the RADIUS server) as the first authenticated host.

- Enabling port security does not impact the RADIUS server-assigned VLAN behavior.

- If 802.1x authentication is disabled on the port, it is returned to the configured access VLAN and configured voice VLAN.

- If an 802.1x port is authenticated and put in the RADIUS server-assigned VLAN, any change to the port access VLAN configuration does not take effect. In the case of a multidomain host, the same applies to voice devices when the port is fully authorized with these exceptions:
  - If the VLAN configuration change of one device results in matching the other device configured or assigned VLAN, then authorization of all devices on the port is terminated and multidomain host mode is disabled until a valid configuration is restored where data and voice device configured VLANs no longer match.
  - If a voice device is authorized and is using a downloaded voice VLAN, the removal of the voice VLAN configuration, or modifying the configuration value to dot1p or untagged results in voice device un-authorization and the disablement of multi-domain host mode.

When the port is in the force authorized, force unauthorized, unauthorized, or shutdown state, it is put into the configured access VLAN.

If an 802.1x port is authenticated and put in the RADIUS server-assigned VLAN, any change to the port access VLAN configuration does not take effect. In the case of a multidomain host, the same applies to voice devices when the port is fully authorized with these exceptions:

- If the VLAN configuration change of one device results in matching the other device configured or assigned VLAN, authorization of all devices on the port is terminated and multidomain host mode is
disabled until a valid configuration is restored where data and voice device configured VLANs no longer match.

- If a voice device is authorized and is using a downloaded voice VLAN, the removal of the voice VLAN configuration, or modifying the configuration value to *dot1p* or *untagged* results in voice device un-authorization and the disablement of multi-domain host mode.

When the port is in the force authorized, force unauthorized, unauthorized, or shutdown state, it is put into the configured access VLAN.

The 802.1x authentication with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN Membership Policy Server (VMPS).

To configure VLAN assignment you need to perform these tasks:

- Enable AAA authorization by using the `network` keyword to allow interface configuration from the RADIUS server.
- Enable 802.1x authentication. (The VLAN assignment feature is automatically enabled when you configure 802.1x authentication on an access port).
- Assign vendor-specific tunnel attributes in the RADIUS server. The RADIUS server must return these attributes to the switch:
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN name or VLAN ID
  - [83] Tunnel-Preference

Attributes [64] must contain the value *VLAN* (type 13). Attribute [65] must contain the value *802* (type 6). Attribute [81] specifies the *VLAN name or VLAN ID* assigned to the IEEE 802.1x-authenticated user.

### 802.1x Authentication with Per-User ACLs

You can enable per-user access control lists (ACLs) to provide different levels of network access and service to an 802.1x-authenticated user. When the RADIUS server authenticates a user connected to an 802.1x port, it retrieves the ACL attributes based on the user identity and sends them to the switch. The switch applies the attributes to the 802.1x port for the duration of the user session. The switch removes the per-user ACL configuration when the session is over, if authentication fails, or if a link-down condition occurs. The switch does not save RADIUS-specified ACLs in the running configuration. When the port is unauthorized, the switch removes the ACL from the port.

You can configure router ACLs and input port ACLs on the same switch. However, a port ACL takes precedence over a router ACL. If you apply input port ACL to an interface that belongs to a VLAN, the port ACL takes precedence over an input router ACL applied to the VLAN interface. Incoming packets received on the port, to which a port ACL is applied, are filtered by the port ACL. Incoming routed packets received on other ports are filtered by the router ACL. Outgoing routed packets are filtered by the router ACL. To avoid configuration conflicts, you should carefully plan the user profiles stored on the RADIUS server.

RADIUS supports per-user attributes, including vendor-specific attributes. These vendor-specific attributes (VSAs) are in octet-string format and are passed to the switch during the authentication process. The VSAs used for per-user ACLs are `inac1#<n>` for the ingress direction and `outac1#<n>` for the egress direction. MAC
ACLS are supported only in the ingress direction. The switch supports VSAs only in the ingress direction. It does not support port ACLs in the egress direction on Layer 2 ports.

Use only the extended ACL syntax style to define the per-user configuration stored on the RADIUS server. When the definitions are passed from the RADIUS server, they are created by using the extended naming convention. However, if you use the Filter-Id attribute, it can point to a standard ACL.

You can use the Filter-Id attribute to specify an inbound or outbound ACL that is already configured on the switch. The attribute contains the ACL number followed by .in for ingress filtering or .out for egress filtering. If the RADIUS server does not allow the .in or .out syntax, the access list is applied to the outbound ACL by default. The user is marked unauthorized if the Filter-Id sent from the RADIUS server is not configured on the device. Because of limited support of Cisco IOS access lists on the switch, the Filter-Id attribute is supported only for IP ACLs numbered in the range of 1 to 199 (IP standard ACLs) and 1300 to 2699 (IP extended ACLs).

The maximum size of the per-user ACL is 4000 ASCII characters but is limited by the maximum size of RADIUS-server per-user ACLs.

You must meet the following prerequisites to configure per-user ACLs:

- Enable AAA authentication.
- Enable AAA authorization by using the network keyword to allow interface configuration from the RADIUS server.
- Enable 802.1x authentication.
- Configure the user profile and VSAs on the RADIUS server.
- Configure the 802.1x port for single-host mode.

---

**Note**

Per-user ACLs are supported only in single-host mode.

---

### 802.1x Authentication with Downloadable ACLs and Redirect URLs

You can download ACLs and redirect URLs from a RADIUS server to the switch during 802.1x authentication or MAC authentication bypass of the host. You can also download ACLs during web authentication.

---

**Note**

A downloadable ACL is also referred to as a *dACL*.

---

If more than one host is authenticated and the host is in single-host, MDA, or multiple-authentication mode, the switch changes the source address of the ACL to the host IP address.

You can apply the ACLs and redirect URLs to all the devices connected to the 802.1x-enabled port.

If no ACLs are downloaded during 802.1x authentication, the switch applies the static default ACL on the port to the host. On a voice VLAN port configured in multi-auth or MDA mode, the switch applies the ACL only to the phone as part of the authorization policies.
The limit for dACL with stacking is 64 ACEs per dACL per port. The limit without stacking is the number of available TCAM entries which varies based on the other ACL features that are active.

Beginning with Cisco IOS Release 12.2(55)SE, if there is no static ACL on a port, a dynamic auth-default ACL is created, and policies are enforced before dACLs are downloaded and applied.

The auth-default-ACL does not appear in the running configuration.

The auth-default ACL is created when at least one host with an authorization policy is detected on the port. The auth-default ACL is removed from the port when the last authenticated session ends. You can configure the auth-default ACL by using the `ip access-list extended auth-default-acl` global configuration command.

The auth-default-ACL does not support Cisco Discovery Protocol (CDP) bypass in the single host mode. You must configure a static ACL on the interface to support CDP bypass.

The 802.1x and MAB authentication methods support two authentication modes, `open` and `closed`. If there is no static ACL on a port in `closed` authentication mode:

- An auth-default-ACL is created.
- The auth-default-ACL allows only DHCP traffic until policies are enforced.
- When the first host authenticates, the authorization policy is applied without IP address insertion.
- When a second host is detected, the policies for the first host are refreshed, and policies for the first and subsequent sessions are enforced with IP address insertion.

If there is no static ACL on a port in `open` authentication mode:

- An auth-default-ACL-OPEN is created and allows all traffic.
- Policies are enforced with IP address insertion to prevent security breaches.
- Web authentication is subject to the auth-default-ACL-OPEN.

To control access for hosts with no authorization policy, you can configure a directive. The supported values for the directive are `open` and `default`. When you configure the `open` directive, all traffic is allowed. The `default` directive subjects traffic to the access provided by the port. You can configure the directive either in the user profile on the AAA server or on the switch. To configure the directive on the AAA server, use the `authz-directive =<open/default>` global command. To configure the directive on the switch, use the `epm access-control open` global configuration command.

The default value of the directive is `default`.

If a host falls back to web authentication on a port without a configured ACL:

- If the port is in open authentication mode, the auth-default-ACL-OPEN is created.
• If the port is in closed authentication mode, the auth-default-ACL is created.

The access control entries (ACEs) in the fallback ACL are converted to per-user entries. If the configured fallback profile does not include a fallback ACL, the host is subject to the auth-default-ACL associated with the port.

---

**Note**

If you use a custom logo with web authentication and it is stored on an external server, the port ACL must allow access to the external server before authentication. You must either configure a static port ACL or change the auth-default-ACL to provide appropriate access to the external server.

---

### Cisco Secure ACS and Attribute-Value Pairs for the Redirect URL

The switch uses these `cisco-av-pair` VSAs:

- `url-redirect` is the HTTP or HTTPS URL.
- `url-redirect-acl` is the switch ACL name or number.

The switch uses the CiscoSecure-defined-ACL attribute value pair to intercept an HTTP or HTTPS request from the end point. The switch then forwards the client web browser to the specified redirect address. The `url-redirect` AV pair on the Cisco Secure ACS contains the URL to which the web browser is redirected. The `url-redirect-acl` attribute value pair contains the name or number of an ACL that specifies the HTTP or HTTPS traffic to redirect.

---

**Note**

- Traffic that matches a permit ACE in the ACL is redirected.
- An ACE that matches permit rule of the `url-redirect-acl` gets the client redirected to `url-redirect` page. The client traffic is allowed when a deny rule is matched.
- Define the URL redirect ACL and the default port ACL on the switch.

---

If a redirect URL is configured for a client on the authentication server, a default port ACL on the connected client switch port must also be configured.

When security ACL/dACL and punt/redirect ACLs are applied together to the session, the `url-redirect-acl` has the higher priority.

For more information about using redirect ACLs, refer the document [here](#).

### Cisco Secure ACS and Attribute-Value Pairs for Downloadable ACLs

You can set the CiscoSecure-Defined-ACL Attribute-Value (AV) pair on the Cisco Secure ACS with the RADIUS `cisco-av-pair` vendor-specific attributes (VSAs). This pair specifies the names of the downloadable ACLs on the Cisco Secure ACS with the `#ACL#-IP-name-number` attribute.

- The `name` is the ACL name.
- The `number` is the version number (for example, 3f783768).
If a downloadable ACL is configured for a client on the authentication server, a default port ACL on the connected client switch port must also be configured.

If the default ACL is configured on the switch and the Cisco Secure ACS sends a host-access-policy to the switch, it applies the policy to traffic from the host connected to a switch port. If the policy does not apply, the switch applies the default ACL. If the Cisco Secure ACS sends the switch a downloadable ACL, this ACL takes precedence over the default ACL that is configured on the switch port. However, if the switch receives an host access policy from the Cisco Secure ACS but the default ACL is not configured, the authorization failure is declared.

**VLAN ID-based MAC Authentication**

You can use VLAN ID-based MAC authentication if you wish to authenticate hosts based on a static VLAN ID instead of a downloadable VLAN. When you have a static VLAN policy configured on your switch, VLAN information is sent to an IAS (Microsoft) RADIUS server along with the MAC address of each host for authentication. The VLAN ID configured on the connected port is used for MAC authentication. By using VLAN ID-based MAC authentication with an IAS server, you can have a fixed number of VLANs in the network.

The feature also limits the number of VLANs monitored and handled by STP. The network can be managed as a fixed VLAN.

**Note**

This feature is not supported on Cisco ACS Server. (The ACS server ignores the sent VLAN-IDs for new hosts and only authenticates based on the MAC address.)

**802.1x Authentication with Guest VLAN**

You can configure a guest VLAN for each 802.1x port on the switch to provide limited services to clients, such as downloading the 802.1x client. These clients might be upgrading their system for 802.1x authentication, and some hosts, such as Windows 98 systems, might not be IEEE 802.1x-capable.

When you enable a guest VLAN on an 802.1x port, the switch assigns clients to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.

The switch maintains the EAPOL packet history. If an EAPOL packet is detected on the interface during the lifetime of the link, the switch determines that the device connected to that interface is an IEEE 802.1x-capable supplicant, and the interface does not change to the guest VLAN state. EAPOL history is cleared if the interface link status goes down. If no EAPOL packet is detected on the interface, the interface changes to the guest VLAN state.

If the switch is trying to authorize an 802.1x-capable voice device and the AAA server is unavailable, the authorization attempt fails, but the detection of the EAPOL packet is saved in the EAPOL history. When the AAA server becomes available, the switch authorizes the voice device. However, the switch no longer allows other devices access to the guest VLAN. To prevent this situation, use one of these command sequences:

- Enter the `authentication event no-response action authorize vlan vlan-id` interface configuration command to allow access to the guest VLAN.

- Enter the `shutdown` interface configuration command followed by the `no shutdown` interface configuration command to restart the port.
If devices send EAPOL packets to the switch during the lifetime of the link, the switch no longer allows clients that fail authentication access to the guest VLAN.

---

**Note**

If an EAPOL packet is detected after the interface has changed to the guest VLAN, the interface reverts to an unauthorized state, and 802.1x authentication restarts.

Any number of 802.1x-incapable clients are allowed access when the switch port is moved to the guest VLAN. If an 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on 802.1x ports in single host, multiple host, multi-auth and multi-domain modes.

You can configure any active VLAN except an RSPAN VLAN, a private VLAN, or a voice VLAN as an 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

The switch supports **MAC authentication bypass**. When MAC authentication bypass is enabled on an 802.1x port, the switch can authorize clients based on the client MAC address when IEEE 802.1x authentication times out while waiting for an EAPOL message exchange. After detecting a client on an 802.1x port, the switch waits for an Ethernet packet from the client. The switch sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the switch grants the client access to the network. If authorization fails, the switch assigns the port to the guest VLAN if one is specified.

---

**802.1x Authentication with Restricted VLAN**

You can configure a restricted VLAN (also referred to as an authentication failed VLAN) for each IEEE 802.1x port on a switch stack or a switch to provide limited services to clients that cannot access the guest VLAN. These clients are 802.1x-compliant and cannot access another VLAN because they fail the authentication process. A restricted VLAN allows users without valid credentials in an authentication server (typically, visitors to an enterprise) to access a limited set of services. The administrator can control the services available to the restricted VLAN.

---

**Note**

You can configure a VLAN to be both the guest VLAN and the restricted VLAN if you want to provide the same services to both types of users.

Without this feature, the client attempts and fails authentication indefinitely, and the switch port remains in the spanning-tree blocking state. With this feature, you can configure the switch port to be in the restricted VLAN after a specified number of authentication attempts (the default value is 3 attempts).

The authenticator counts the failed authentication attempts for the client. When this count exceeds the configured maximum number of authentication attempts, the port moves to the restricted VLAN. The failed attempt count increments when the RADIUS server replies with either an EAP failure or an empty response without an EAP packet. When the port moves into the restricted VLAN, the failed attempt counter resets.

Users who fail authentication remain in the restricted VLAN until the next re-authentication attempt. A port in the restricted VLAN tries to re-authenticate at configured intervals (the default is 60 seconds). If re-authentication fails, the port remains in the restricted VLAN. If re-authentication is successful, the port moves either to the configured VLAN or to a VLAN sent by the RADIUS server. You can disable
re-authentication. If you do this, the only way to restart the authentication process is for the port to receive a link down or EAP logoff event. We recommend that you keep re-authentication enabled if a client might connect through a hub. When a client disconnects from the hub, the port might not receive the link down or EAP logoff event.

After a port moves to the restricted VLAN, a simulated EAP success message is sent to the client. This prevents clients from indefinitely attempting authentication. Some clients (for example, devices running Windows XP) cannot implement DHCP without EAP success.

Restricted VLANs are supported on 802.1x ports in all host modes and on Layer 2 ports.

You can configure any active VLAN except an RSPAN VLAN, a primary private VLAN, or a voice VLAN as an 802.1x restricted VLAN. The restricted VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

Other security port features such as dynamic ARP Inspection, DHCP snooping, and IP source guard can be configured independently on a restricted VLAN.

### 802.1x Authentication with Inaccessible Authentication Bypass

Use the inaccessible authentication bypass feature, also referred to as critical authentication or the AAA fail policy, when the switch cannot reach the configured RADIUS servers and new hosts cannot be authenticated. You can configure the switch to connect those hosts to critical ports.

When a new host tries to connect to the critical port, that host is moved to a user-specified access VLAN, the critical VLAN. The administrator gives limited authentication to the hosts.

When the switch tries to authenticate a host connected to a critical port, the switch checks the status of the configured RADIUS server. If a server is available, the switch can authenticate the host. However, if all the RADIUS servers are unavailable, the switch grants network access to the host and puts the port in the critical-authentication state, which is a special case of the authentication state.

---

**Note**

If critical authentication is configured on interface, then vlan used for critical authorization (critical vlan) should be active on the switch. If the critical vlan is inactive (or) down, critical authentication session will keep trying to enable inactive vlan and fail repeatedly. This can lead to large amount of memory holding.

### Inaccessible Authentication Bypass Support on Multiple-Authentication Ports

When a port is configured on any host mode and the AAA server is unavailable, the port is then configured to multi-host mode and moved to the critical VLAN. To support this inaccessible bypass on multiple-authentication (multauth) ports, use the `authentication event server dead action reinitialize vlan vlan-id` command. When a new host tries to connect to the critical port, that port is reinitialized and all the connected hosts are moved to the user-specified access VLAN.

This command is supported on all host modes.

### Inaccessible Authentication Bypass Authentication Results

The behavior of the inaccessible authentication bypass feature depends on the authorization state of the port:

- If the port is unauthorized when a host connected to a critical port tries to authenticate and all servers are unavailable, the switch puts the port in the critical-authentication state in the RADIUS-configured or user-specified access VLAN.
• If the port is already authorized and reauthentication occurs, the switch puts the critical port in the critical-authentication state in the current VLAN, which might be the one previously assigned by the RADIUS server.

• If the RADIUS server becomes unavailable during an authentication exchange, the current exchange times out, and the switch puts the critical port in the critical-authentication state during the next authentication attempt.

You can configure the critical port to reinitialize hosts and move them out of the critical VLAN when the RADIUS server is again available. When this is configured, all critical ports in the critical-authentication state are automatically re-authenticated.

**Inaccessible Authentication Bypass Feature Interactions**

Inaccessible authentication bypass interacts with these features:

• Guest VLAN—Inaccessible authentication bypass is compatible with guest VLAN. When a guest VLAN is enabled on 8021.x port, the features interact as follows:
  • If at least one RADIUS server is available, the switch assigns a client to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.
  • If all the RADIUS servers are not available and the client is connected to a critical port, the switch authenticates the client and puts the critical port in the critical-authentication state in the RADIUS-configured or user-specified access VLAN.
  • If all the RADIUS servers are not available and the client is not connected to a critical port, the switch might not assign clients to the guest VLAN if one is configured.
  • If all the RADIUS servers are not available and if a client is connected to a critical port and was previously assigned to a guest VLAN, the switch keeps the port in the guest VLAN.

• Restricted VLAN—If the port is already authorized in a restricted VLAN and the RADIUS servers are unavailable, the switch puts the critical port in the critical-authentication state in the restricted VLAN.

• 802.1x accounting—Accounting is not affected if the RADIUS servers are unavailable.

• Private VLAN—You can configure inaccessible authentication bypass on a private VLAN host port. The access VLAN must be a secondary private VLAN.

• Voice VLAN—Inaccessible authentication bypass is compatible with voice VLAN, but the RADIUS-configured or user-specified access VLAN and the voice VLAN must be different.

• Remote Switched Port Analyzer (RSPAN)—Do not configure an RSPAN VLAN as the RADIUS-configured or user-specified access VLAN for inaccessible authentication bypass.

In a switch stack:

• The stack master checks the status of the RADIUS servers by sending keepalive packets. When the status of a RADIUS server changes, the stack master sends the information to the stack members. The stack members can then check the status of RADIUS servers when re-authenticating critical ports.

• If the new stack master is elected, the link between the switch stack and RADIUS server might change, and the new stack immediately sends keepalive packets to update the status of the RADIUS servers. If
the server status changes from *dead* to *alive*, the switch re-authenticates all switch ports in the critical-authentication state.

When a member is added to the stack, the stack master sends the member the server status.

### 802.1x Critical Voice VLAN

When an IP phone connected to a port is authenticated by the access control server (ACS), the phone is put into the voice domain. If the ACS is not reachable, the switch cannot determine if the device is a voice device. If the server is unavailable, the phone cannot access the voice network and therefore cannot operate.

For data traffic, you can configure inaccessible authentication bypass, or critical authentication, to allow traffic to pass through on the native VLAN when the server is not available. If the RADIUS authentication server is unavailable (down) and inaccessible authentication bypass is enabled, the switch grants the client access to the network and puts the port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN. When the switch cannot reach the configured RADIUS servers and new hosts cannot be authenticated, the switch connects those hosts to critical ports. A new host trying to connect to the critical port is moved to a user-specified access VLAN, the critical VLAN, and granted limited authentication.

You can enter the `authentication event server dead action authorize voice` interface configuration command to configure the critical voice VLAN feature. When the ACS does not respond, the port goes into critical authentication mode. When traffic coming from the host is tagged with the voice VLAN, the connected device (the phone) is put in the configured voice VLAN for the port. The IP phones learn the voice VLAN identification through CDP (Cisco devices) or through LLDP or DHCP.

You can configure the voice VLAN for a port by entering the `switchport voice vlan vlan-id` interface configuration command.

This feature is supported in multidomain and multi-auth host modes. Although you can enter the command when the switch in single-host or multi-host mode, the command has no effect unless the device changes to multidomain or multi-auth host mode.

### 802.1x User Distribution

You can configure 802.1x user distribution to load-balance users with the same group name across multiple different VLANs.

The VLANs are either supplied by the RADIUS server or configured through the switch CLI under a VLAN group name.

- Configure the RADIUS server to send more than one VLAN name for a user. The multiple VLAN names can be sent as part of the response to the user. The 802.1x user distribution tracks all the users in a particular VLAN and achieves load balancing by moving the authorized user to the least populated VLAN.

- Configure the RADIUS server to send a VLAN group name for a user. The VLAN group name can be sent as part of the response to the user. You can search for the selected VLAN group name among the VLAN group names that you configured by using the switch CLI. If the VLAN group name is found, the corresponding VLANs under this VLAN group name are searched to find the least populated VLAN. Load balancing is achieved by moving the corresponding authorized user to that VLAN.
The RADIUS server can send the VLAN information in any combination of VLAN-IDs, VLAN names, or VLAN groups.

802.1x User Distribution Configuration Guidelines

- Confirm that at least one VLAN is mapped to the VLAN group.
- You can map more than one VLAN to a VLAN group.
- You can modify the VLAN group by adding or deleting a VLAN.
- When you clear an existing VLAN from the VLAN group name, none of the authenticated ports in the VLAN are cleared, but the mappings are removed from the existing VLAN group.
- If you clear the last VLAN from the VLAN group name, the VLAN group is cleared.
- You can clear a VLAN group even when the active VLANs are mapped to the group. When you clear a VLAN group, none of the ports or users that are in the authenticated state in any VLAN within the group are cleared, but the VLAN mappings to the VLAN group are cleared.

IEEE 802.1x Authentication with Voice VLAN Ports

A voice VLAN port is a special access port associated with two VLAN identifiers:

- VVID to carry voice traffic to and from the IP phone. The VVID is used to configure the IP phone connected to the port.
- PVID to carry the data traffic to and from the workstation connected to the switch through the IP phone. The PVID is the native VLAN of the port.

The IP phone uses the VVID for its voice traffic, regardless of the authorization state of the port. This allows the phone to work independently of IEEE 802.1x authentication.

In single-host mode, only the IP phone is allowed on the voice VLAN. In multiple-hosts mode, additional clients can send traffic on the voice VLAN after a supplicant is authenticated on the PVID. When multiple-hosts mode is enabled, the supplicant authentication affects both the PVID and the VVID.

A voice VLAN port becomes active when there is a link, and the device MAC address appears after the first CDP message from the IP phone. Cisco IP phones do not relay CDP messages from other devices. As a result, if several IP phones are connected in series, the switch recognizes only the one directly connected to it. When IEEE 802.1x authentication is enabled on a voice VLAN port, the switch drops packets from unrecognized IP phones more than one hop away.

When IEEE 802.1x authentication is enabled on a switch port, you can configure an access port VLAN that is also a voice VLAN.

When IP phones are connected to an 802.1x-enabled switch port that is in single host mode, the switch grants the phones network access without authenticating them. We recommend that you use multidomain authentication (MDA) on the port to authenticate both a data device and a voice device, such as an IP phone.
If you enable IEEE 802.1x authentication on an access port on which a voice VLAN is configured and to which a Cisco IP Phone is connected, the Cisco IP phone loses connectivity to the switch for up to 30 seconds.

IEEE 802.1x Authentication with Port Security

In general, Cisco does not recommend enabling port security when IEEE 802.1x is enabled. Since IEEE 802.1x enforces a single MAC address per port (or per VLAN when MDA is configured for IP telephony), port security is redundant and in some cases may interfere with expected IEEE 802.1x operations.

IEEE 802.1x Authentication with Wake-on-LAN

The IEEE 802.1x authentication with wake-on-LAN (WoL) feature allows dormant PCs to be powered when the switch receives a specific Ethernet frame, known as the magic packet. You can use this feature in environments where administrators need to connect to systems that have been powered down.

When a host that uses WoL is attached through an IEEE 802.1x port and the host powers off, the IEEE 802.1x port becomes unauthorized. The port can only receive and send EAPOL packets, and WoL magic packets cannot reach the host. When the PC is powered off, it is not authorized, and the switch port is not opened.

When the switch uses IEEE 802.1x authentication with WoL, the switch forwards traffic to unauthorized IEEE 802.1x ports, including magic packets. While the port is unauthorized, the switch continues to block ingress traffic other than EAPOL packets. The host can receive packets but cannot send packets to other devices in the network.

If PortFast is not enabled on the port, the port is forced to the bidirectional state.

When you configure a port as unidirectional by using the authentication control-direction in interface configuration command, the port changes to the spanning-tree forwarding state. The port can send packets to the host but cannot receive packets from the host.

When you configure a port as bidirectional by using the authentication control-direction both interface configuration command, the port is access-controlled in both directions. The port does not receive packets from or send packets to the host.

IEEE 802.1x Authentication with MAC Authentication Bypass

You can configure the switch to authorize clients based on the client MAC address by using the MAC authentication bypass feature. For example, you can enable this feature on IEEE 802.1x ports connected to devices such as printers.

If IEEE 802.1x authentication times out while waiting for an EAPOL response from the client, the switch tries to authorize the client by using MAC authentication bypass.

When the MAC authentication bypass feature is enabled on an IEEE 802.1x port, the switch uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed network access. After detecting a client on an IEEE 802.1x port, the switch waits for an Ethernet packet from the client. The switch sends the authentication server a RADIUS-access/request frame with a username and
password based on the MAC address. If authorization succeeds, the switch grants the client access to the network. If authorization fails, the switch assigns the port to the guest VLAN if one is configured. This process works for most client devices; however, it does not work for clients that use an alternate MAC address format. You can configure how MAB authentication is performed for clients with MAC addresses that deviate from the standard format or where the RADIUS configuration requires the user name and password to differ.

If an EAPOL packet is detected on the interface during the lifetime of the link, the switch determines that the device connected to that interface is an 802.1x-capable supplicant and uses 802.1x authentication (not MAC authentication bypass) to authorize the interface. EAPOL history is cleared if the interface link status goes down.

If the switch already authorized a port by using MAC authentication bypass and detects an IEEE 802.1x supplicant, the switch does not unauthorize the client connected to the port. When re-authentication occurs, the switch uses the authentication or re-authentication methods configured on the port, if the previous session ended because the Termination-Action RADIUS attribute value is DEFAULT.

Clients that were authorized with MAC authentication bypass can be re-authenticated. The re-authentication process is the same as that for clients that were authenticated with IEEE 802.1x. During re-authentication, the port remains in the previously assigned VLAN. If re-authentication is successful, the switch keeps the port in the same VLAN. If re-authentication fails, the switch assigns the port to the guest VLAN, if one is configured.

If re-authentication is based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]) and if the Termination-Action RADIUS attribute (Attribute [29]) action is Initialize (the attribute value is DEFAULT), the MAC authentication bypass session ends, and connectivity is lost during re-authentication. If MAC authentication bypass is enabled and the IEEE 802.1x authentication times out, the switch uses the MAC authentication bypass feature to initiate re-authorization. For more information about these AV pairs, see RFC 3580, “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines.”

MAC authentication bypass interacts with the features:

- IEEE 802.1x authentication—You can enable MAC authentication bypass only if 802.1x authentication is enabled on the port.
- Guest VLAN—If a client has an invalid MAC address identity, the switch assigns the client to a guest VLAN if one is configured.
- Restricted VLAN—This feature is not supported when the client connected to an IEEE 802.1x port is authenticated with MAC authentication bypass.
- Port security
- Voice VLAN
- Private VLAN—You can assign a client to a private VLAN.
- Network Edge Access Topology (NEAT)—MAB and NEAT are mutually exclusive. You cannot enable MAB when NEAT is enabled on an interface, and you should not enable NEAT when MAB is enabled on an interface.

Cisco IOS Release 12.2(55)SE and later supports filtering of verbose MAB system messages.
Network Admission Control Layer 2 IEEE 802.1x Validation

The switch supports the Network Admission Control (NAC) Layer 2 IEEE 802.1x validation, which checks the antivirus condition or posture of endpoint systems or clients before granting the devices network access. With NAC Layer 2 IEEE 802.1x validation, you can do these tasks:

- Download the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute[29]) from the authentication server.
- Set the number of seconds between re-authentication attempts as the value of the Session-Timeout RADIUS attribute (Attribute[27]) and get an access policy against the client from the RADIUS server.
- Set the action to be taken when the switch tries to re-authenticate the client by using the Termination-Action RADIUS attribute (Attribute[29]). If the value is the DEFAULT or is not set, the session ends. If the value is RADIUS-Request, the re-authentication process starts.
- Set the list of VLAN number or name or VLAN group name as the value of the Tunnel Group Private ID (Attribute[81]) and the preference for the VLAN number or name or VLAN group name as the value of the Tunnel Preference (Attribute[83]). If you do not configure the Tunnel Preference, the first Tunnel Group Private ID (Attribute[81]) attribute is picked up from the list.
- View the NAC posture token, which shows the posture of the client, by using the `show authentication` privileged EXEC command.
- Configure secondary private VLANs as guest VLANs.

Configuring NAC Layer 2 IEEE 802.1x validation is similar to configuring IEEE 802.1x port-based authentication except that you must configure a posture token on the RADIUS server.

Flexible Authentication Ordering

You can use flexible authentication ordering to configure the order of methods that a port uses to authenticate a new host. The IEEE 802.1X Flexible Authentication feature supports three authentication methods:

- dot1X—IEEE 802.1X authentication is a Layer 2 authentication method.
- mab—MAC-Authentication Bypass is a Layer 2 authentication method.
- webauth—Web authentication is a Layer 3 authentication method.

Using this feature, you can control which ports use which authentication methods, and you can control the failover sequencing of methods on those ports. For example, MAC authentication bypass and 802.1x can be the primary or secondary authentication methods, and web authentication can be the fallback method if either or both of those authentication attempts fail.

The IEEE 802.1X Flexible Authentication feature supports the following host modes:

- multi-auth—Multiauthentication allows one authentication on a voice VLAN and multiple authentications on the data VLAN.
- multi-domain—Multidomain authentication allows two authentications: one on the voice VLAN and one on the data VLAN.
Open1x Authentication

Open1x authentication allows a device access to a port before that device is authenticated. When open authentication is configured, a new host can pass traffic according to the access control list (ACL) defined on the port. After the host is authenticated, the policies configured on the RADIUS server are applied to that host.

You can configure open authentication with these scenarios:

• Single-host mode with open authentication–Only one user is allowed network access before and after authentication.
• MDA mode with open authentication–Only one user in the voice domain and one user in the data domain are allowed.
• Multiple-hosts mode with open authentication–Any host can access the network.
• Multiple-authentication mode with open authentication–Similar to MDA, except multiple hosts can be authenticated.

If open authentication is configured, it takes precedence over other authentication controls. This means that if you use the `authentication open` interface configuration command, the port will grant access to the host irrespective of the `authentication port-control` interface configuration command.

Note

Multidomain Authentication

The switch supports multidomain authentication (MDA), which allows both a data device and voice device, such as an IP phone (Cisco or non-Cisco), to authenticate on the same switch port. The port is divided into a data domain and a voice domain.

For all host modes, the line protocol stays up before authorization when port-based authentication is configured.

MDA does not enforce the order of device authentication. However, for best results, we recommend that a voice device is authenticated before a data device on an MDA-enabled port.

Follow these guidelines for configuring MDA:

• You must configure a switch port for MDA.
• You must configure the voice VLAN for the IP phone when the host mode is set to multidomain.
• Voice VLAN assignment on an MDA-enabled port is supported Cisco IOS Release 12.2(40)SE and later.
• To authorize a voice device, the AAA server must be configured to send a Cisco Attribute-Value (AV) pair attribute with a value of `device-traffic-class=voice`. Without this value, the switch treats the voice device as a data device.
• The guest VLAN and restricted VLAN features only apply to the data devices on an MDA-enabled port. The switch treats a voice device that fails authorization as a data device.
• If more than one device attempts authorization on either the voice or the data domain of a port, it is error
disabled.

• Until a device is authorized, the port drops its traffic. Non-Cisco IP phones or voice devices are allowed
into both the data and voice VLANs. The data VLAN allows the voice device to contact a DHCP server
to obtain an IP address and acquire the voice VLAN information. After the voice device starts sending
on the voice VLAN, its access to the data VLAN is blocked.

• A voice device MAC address that is binding on the data VLAN is not counted towards the port security
MAC address limit.

• MDA can use MAC authentication bypass as a fallback mechanism to allow the switch port to connect
to devices that do not support IEEE 802.1x authentication.

• When a data or a voice device is detected on a port, its MAC address is blocked until authorization
succeeds. If the authorization fails, the MAC address remains blocked for 5 minutes.

• If more than five devices are detected on the data VLAN or more than one voice device is detected on
the voice VLAN while a port is unauthorized, the port is error disabled.

• When a port host mode is changed from single- or multihost to multidomain mode, an authorized data
device remains authorized on the port. However, a Cisco IP phone that has been allowed on the port
voice VLAN is automatically removed and must be reauthenticated on that port.

• Active fallback mechanisms such as guest VLAN and restricted VLAN remain configured after a port
changes from single- or multihost mode to multidomain mode.

• Switching a port host mode from multidomain to single- or multihost mode removes all authorized devices
from the port.

• If a data domain is authorized first and placed in the guest VLAN, non-IEEE 802.1x-capable voice
devices need to tag their packets on the voice VLAN to trigger authentication.

• We do not recommend per-user ACLs with an MDA-enabled port. An authorized device with a per-user
ACL policy might impact traffic on both the voice and data VLANs of the port. If used, only one device
on the port should enforce per-user ACLs.

**Limiting Login for Users**

The Limiting Login feature helps Network administrators to limit the login attempt of users to a network. When a user fails to successfully login to a network within a configurable number of attempts within a configurable time limit, the user can be blocked. This feature is enabled only for local users and not for remote users. You need to configure the `aaa authentication rejected` command in global configuration mode to enable this feature.

**802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT)**

The Network Edge Access Topology (NEAT) feature extends identity to areas outside the wiring closet (such as conference rooms). This allows any type of device to authenticate on the port.

• 802.1x switch supplicant: You can configure a switch to act as a supplicant to another switch by using
the 802.1x supplicant feature. This configuration is helpful in a scenario, where, for example, a switch
is outside a wiring closet and is connected to an upstream switch through a trunk port. A switch configured with the 802.1x switch supplicant feature authenticates with the upstream switch for secure connectivity. Once the supplicant switch authenticates successfully the port mode changes from access to trunk in an authenticator switch. In a supplicant switch you must manually configure trunk when enabling CISP.

- If the access VLAN is configured on the authenticator switch, it becomes the native VLAN for the trunk port after successful authentication.

In the default state, when you connect a supplicant switch to an authenticator switch that has BPDU guard enabled, the authenticator port could be error-disabled if it receives a Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets before the supplicant switch has authenticated. Beginning with Cisco IOS Release 15.0(1)SE, you can control traffic exiting the supplicant port during the authentication period. Entering the \texttt{dot1x supplicant controlled transient} global configuration command temporarily blocks the supplicant port during authentication to ensure that the authenticator port does not shut down before authentication completes. If authentication fails, the supplicant port opens. Entering the \texttt{no dot1x supplicant controlled transient} global configuration command opens the supplicant port during the authentication period. This is the default behavior.

We strongly recommend using the \texttt{dot1x supplicant controlled transient} command on a supplicant switch when BPDU guard is enabled on the authenticator switch port with the \texttt{spanning-tree bpduguard enable} interface configuration command.

\underline{Note}

If you globally enable BPDU guard on the authenticator switch by using the \texttt{spanning-tree portfast bpduguard default} global configuration command, entering the \texttt{dot1x supplicant controlled transient} command does not prevent the BPDU violation.

You can enable MDA or multiauth mode on the authenticator switch interface that connects to one more supplicant switches. Multihost mode is not supported on the authenticator switch interface.

When you reboot an authenticator switch with single-host mode enabled on the interface, the interface may move to err-disabled state before authentication. To recover from err-disabled state, flap the authenticator port to activate the interface again and initiate authentication.

Use the \texttt{dot1x supplicant force-multicast} global configuration command on the supplicant switch for Network Edge Access Topology (NEAT) to work in all host modes.

- Host Authorization: Ensures that only traffic from authorized hosts (connecting to the switch with supplicant) is allowed on the network. The switches use Client Information Signalling Protocol (CISP) to send the MAC addresses connecting to the supplicant switch to the authenticator switch.

- Auto enablement: Automatically enables trunk configuration on the authenticator switch, allowing user traffic from multiple VLANs coming from supplicant switches. Configure the cisco-av-pair as \texttt{device-traffic-class=switch} at the ACS. (You can configure this under the \texttt{group} or the \texttt{user} settings.)
The `switchport nonegotiate` command is not supported on supplicant and authenticator switches with NEAT. This command should not be configured at the supplicant side of the topology. If configured on the authenticator side, the internal macros will automatically remove this command from the port.

**Voice Aware 802.1x Security**

To use voice aware IEEE 802.1x authentication, the switch must be running the LAN base image.

You use the voice aware 802.1x security feature to configure the switch to disable only the VLAN on which a security violation occurs, whether it is a data or voice VLAN. In previous releases, when an attempt to authenticate the data client caused a security violation, the entire port shut down, resulting in a complete loss of connectivity.

You can use this feature in IP phone deployments where a PC is connected to the IP phone. A security violation found on the data VLAN results in the shutdown of only the data VLAN. The traffic on the voice VLAN flows through the switch without interruption.

**Common Session ID**

Authentication manager uses a single session ID (referred to as a common session ID) for a client no matter which authentication method is used. This ID is used for all reporting purposes, such as the show commands and MIBs. The session ID appears with all per-session syslog messages.

The session ID includes:
- The IP address of the Network Access Device (NAD)
- A monotonically increasing unique 32 bit integer
- The session start time stamp (a 32 bit integer)

This example shows how the session ID appears in the output of the show authentication command. The session ID in this example is 160000050000000B288508E5:

```
Switch# show authentication sessions
Interface  MAC Address  Method  Domain  Status  Session ID
Fa4/0/4    0000.0000.0203  mab  DATA  Authz Success  160000050000000B288508E5
```

This is an example of how the session ID appears in the syslog output. The session ID in this example is also 160000050000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client (0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

The session ID is used by the NAD, the AAA server, and other report-analyzing applications to identify the client. The ID appears automatically. No configuration is required.

# How to Configure 802.1x Port-Based Authentication

## Default 802.1x Authentication Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 802.1x enable state</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Per-port 802.1x enable state</td>
<td>Disabled (force-authorized). The port sends and receives normal traffic without 802.1x-based authentication of the client.</td>
</tr>
<tr>
<td>AAA</td>
<td>Disabled.</td>
</tr>
<tr>
<td>RADIUS server</td>
<td>• None specified.</td>
</tr>
<tr>
<td></td>
<td>• 1645.</td>
</tr>
<tr>
<td></td>
<td>• 1646.</td>
</tr>
<tr>
<td></td>
<td>• Key</td>
</tr>
</tbody>
</table>

# How to Configure 802.1x Port-Based Authentication

## Default 802.1x Authentication Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 802.1x enable state</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Per-port 802.1x enable state</td>
<td>Disabled (force-authorized). The port sends and receives normal traffic without 802.1x-based authentication of the client.</td>
</tr>
<tr>
<td>AAA</td>
<td>Disabled.</td>
</tr>
<tr>
<td>RADIUS server</td>
<td>• None specified.</td>
</tr>
<tr>
<td></td>
<td>• 1645.</td>
</tr>
<tr>
<td></td>
<td>• 1646.</td>
</tr>
<tr>
<td></td>
<td>• Key</td>
</tr>
<tr>
<td>Feature</td>
<td>Default Setting</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Host mode</td>
<td>Single-host mode.</td>
</tr>
<tr>
<td>Control direction</td>
<td>Bidirectional control.</td>
</tr>
<tr>
<td>Periodic re-authentication</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Number of seconds between re-authentication attempts</td>
<td>3600 seconds.</td>
</tr>
<tr>
<td>Re-authentication number</td>
<td>2 times (number of times that the switch restarts the authentication process before the port changes to the unauthorized state).</td>
</tr>
<tr>
<td>Quiet period</td>
<td>60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client).</td>
</tr>
<tr>
<td>Retransmission time</td>
<td>30 seconds (number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before resending the request).</td>
</tr>
<tr>
<td>Maximum retransmission number</td>
<td>2 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process).</td>
</tr>
<tr>
<td>Client timeout period</td>
<td>30 seconds (when relaying a request from the authentication server to the client, the amount of time the switch waits for a response before resending the request to the client).</td>
</tr>
<tr>
<td>Authentication server timeout period</td>
<td>30 seconds (when relaying a response from the client to the authentication server, the amount of time the switch waits for a reply before resending the response to the server.) You can change this timeout period by using the dot1x timeout server-timeout interface configuration command.</td>
</tr>
<tr>
<td>Inactivity timeout</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Guest VLAN</td>
<td>None specified.</td>
</tr>
<tr>
<td>Inaccessible authentication bypass</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Restricted VLAN</td>
<td>None specified.</td>
</tr>
<tr>
<td>Authenticator (switch) mode</td>
<td>None specified.</td>
</tr>
<tr>
<td>MAC authentication bypass</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Voice-aware security</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>
802.1x Authentication Configuration Guidelines

802.1x Authentication

These are the 802.1x authentication configuration guidelines:

- When 802.1x authentication is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.

- If the VLAN to which an 802.1x-enabled port is assigned changes, this change is transparent and does not affect the switch. For example, this change occurs if a port is assigned to a RADIUS server-assigned VLAN and is then assigned to a different VLAN after re-authentication.

  If the VLAN to which an 802.1x port is assigned to shut down, disabled, or removed, the port becomes unauthorized. For example, the port is unauthorized after the access VLAN to which a port is assigned shuts down or is removed.

- The 802.1x protocol is supported on Layer 2 static-access ports, voice VLAN ports, and Layer 3 routed ports, but it is not supported on these port types:
  - Dynamic ports—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1x authentication on a dynamic port, an error message appears, and 802.1x authentication is not enabled. If you try to change the mode of an 802.1x-enabled port to dynamic, an error message appears, and the port mode is not changed.
  - EtherChannel port—Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an 802.1x port. If you try to enable 802.1x authentication on an EtherChannel port, an error message appears, and 802.1x authentication is not enabled.
  - Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable 802.1x authentication on a port that is a SPAN or RSPAN destination port. However, 802.1x authentication is disabled until the port is removed as a SPAN or RSPAN destination port. You can enable 802.1x authentication on a SPAN or RSPAN source port.

  - Before globally enabling 802.1x authentication on a switch by entering the `dot1x system-auth-control` global configuration command, remove the EtherChannel configuration from the interfaces on which 802.1x authentication and EtherChannel are configured.
  - Cisco IOS Release 12.2(55)SE and later supports filtering of system messages related to 802.1x authentication.

VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass

These are the configuration guidelines for VLAN assignment, guest VLAN, restricted VLAN, and inaccessible authentication bypass:

- When 802.1x authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.

  The 802.1x authentication with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VMPS.

  You can configure any VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.
• After you configure a guest VLAN for an 802.1x port to which a DHCP client is connected, you might need to get a host IP address from a DHCP server. You can change the settings for restarting the 802.1x authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. Decrease the settings for the 802.1x authentication process (authentication timer inactivity and authentication timer reauthentication interface configuration commands). The amount to decrease the settings depends on the connected 802.1x client type.

• When configuring the inaccessible authentication bypass feature, follow these guidelines:
  - The feature is supported on 802.1x port in single-host mode and multihost mode.
  - If the client is running Windows XP and the port to which the client is connected is in the critical-authentication state, Windows XP might report that the interface is not authenticated.
  - If the Windows XP client is configured for DHCP and has an IP address from the DHCP server, receiving an EAP-Success message on a critical port might not re-initiate the DHCP configuration process.
  - You can configure the inaccessible authentication bypass feature and the restricted VLAN on an 802.1x port. If the switch tries to re-authenticate a critical port in a restricted VLAN and all the RADIUS servers are unavailable, switch changes the port state to the critical authentication state and remains in the restricted VLAN.
  - If the CTS links are in Critical Authentication mode and the master reloads, the policy where SGT was configured on a device will not be available on the new master. This is because the internal bindings will not be synced to the standby switch in a 3750-X switch stack.

• You can configure any VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN. The restricted VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

• When wireless guest clients obtains IP from foreign client VLAN instead of anchor client VLAN, you should use the ip dhcp required command under the WLAN configuration to force clients to issue a new DHCP request. This prevents the clients from getting an incorrect IP at anchor.

• If the wired guest clients fail to get IP address after a Cisco WLC (foreign) reload, perform a shut/no shut on the ports used by the clients to reconnect them.

**MAC Authentication Bypass**

These are the MAC authentication bypass configuration guidelines:

• Unless otherwise stated, the MAC authentication bypass guidelines are the same as the 802.1x authentication guidelines.

• If you disable MAC authentication bypass from a port after the port has been authorized with its MAC address, the port state is not affected.

• If the port is in the unauthorized state and the client MAC address is not the authentication-server database, the port remains in the unauthorized state. However, if the client MAC address is added to the database, the switch can use MAC authentication bypass to re-authorize the port.

• If the port is in the authorized state, the port remains in this state until re-authorization occurs.

• You can configure a timeout period for hosts that are connected by MAC authentication bypass but are inactive. The range is 1 to 65535 seconds.
Maximum Number of Allowed Devices Per Port

This is the maximum number of devices allowed on an 802.1x-enabled port:

- In single-host mode, only one device is allowed on the access VLAN. If the port is also configured with a voice VLAN, an unlimited number of Cisco IP phones can send and receive traffic through the voice VLAN.
- In multidomain authentication (MDA) mode, one device is allowed for the access VLAN, and one IP phone is allowed for the voice VLAN.
- In multihost mode, only one 802.1x supplicant is allowed on the port, but an unlimited number of non-802.1x hosts are allowed on the access VLAN. An unlimited number of devices are allowed on the voice VLAN.

Configuring 802.1x Readiness Check

The 802.1x readiness check monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable.

The 802.1x readiness check is allowed on all ports that can be configured for 802.1x. The readiness check is not available on a port that is configured as `dot1x force-unauthorized`.

Follow these steps to enable the 802.1x readiness check on the switch:

**Before you begin**

Follow these guidelines to enable the readiness check on the switch:

- The readiness check is typically used before 802.1x is enabled on the switch.
- If you use the `dot1x test capol-capable` privileged EXEC command without specifying an interface, all the ports on the switch stack are tested.
- When you configure the `dot1x test capol-capable` command on an 802.1x-enabled port, and the link comes up, the port queries the connected client about its 802.1x capability. When the client responds with a notification packet, it is 802.1x-capable. A syslog message is generated if the client responds within the timeout period. If the client does not respond to the query, the client is not 802.1x-capable. No syslog message is generated.
- When you configure the `dot1x test capol-capable` command on an 802.1x-enabled port, and the link comes up, the port queries the connected client about its 802.1x capability. When the client responds with a notification packet, it is 802.1x-capable. A syslog message is generated if the client responds within the timeout period. If the client does not respond to the query, the client is not 802.1x-capable. No syslog message is generated.
- The readiness check can be sent on a port that handles multiple hosts (for example, a PC that is connected to an IP phone). A syslog message is generated for each of the clients that respond to the readiness check within the timer period.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dot1x test eapol-capable [interface interface-id]</td>
<td>Enables the 802.1x readiness check on the switch.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# dot1x test eapol-capable interface gigabitethernet1/0/13 DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable</td>
<td>(Optional) For <em>interface-id</em> specify the port on which to check for IEEE 802.1x readiness.</td>
</tr>
<tr>
<td><strong>Note</strong> If you omit the optional <em>interface</em> keyword, all interfaces on the switch are tested.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> dot1x test timeout timeout</td>
<td>(Optional) Configures the timeout used to wait for EAPOL response. The range is from 1 to 65535 seconds. The default is 10 seconds.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Voice Aware 802.1x Security**

*Note* To use voice aware IEEE 802.1x authentication, the switch must be running the LAN base image.
You use the voice aware 802.1x security feature on the switch to disable only the VLAN on which a security violation occurs, whether it is a data or voice VLAN. You can use this feature in IP phone deployments where a PC is connected to the IP phone. A security violation found on the data VLAN results in the shutdown of only the data VLAN. The traffic on the voice VLAN flows through the switch without interruption.

Follow these guidelines to configure voice aware 802.1x voice security on the switch:

- You enable voice aware 802.1x security by entering the `errdisable detect cause security-violation shutdown vlan` global configuration command. You disable voice aware 802.1x security by entering the `no` version of this command. This command applies to all 802.1x-configured ports in the switch.

  **Note** If you do not include the `shutdown vlan` keywords, the entire port is shut down when it enters the error-disabled state.

- If you use the `errdisable recovery cause security-violation` global configuration command to configure error-disabled recovery, the port is automatically re-enabled. If error-disabled recovery is not configured for the port, you re-enable it by using the `shutdown` and `no shutdown` interface configuration commands.

- You can re-enable individual VLANs by using the `clear errdisable interface interface-id vlan [vlan-list]` privileged EXEC command. If you do not specify a range, all VLANs on the port are enabled.

Beginning in privileged EXEC mode, follow these steps to enable voice aware 802.1x security:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 2** | `errdisable detect cause security-violation shutdown vlan` Shut down any VLAN on which a security violation error occurs.  
**Note** If the `shutdown vlan` keywords are not included, the entire port enters the error-disabled state and shuts down. |
| **Step 3** | `errdisable recovery cause security-violation` Enter global configuration mode. |
| **Step 4** | `clear errdisable interface interface-id vlan [vlan-list]` (Optional) Reenable individual VLANs that have been error disabled.  
- For `interface-id` specify the port on which to reenable individual VLANs.  
- (Optional) For `vlan-list` specify a list of VLANs to be re-enabled. If `vlan-list` is not specified, all VLANs are re-enabled. |
| **Step 5** | Enter the following:  
- `shutdown`  
- `no shutdown` (Optional) Re-enable an error-disabled VLAN, and clear all error-disable indications. |
| **Step 6** | `end` Return to privileged EXEC mode. |
### Configuring 802.1x Violation Modes

You can configure an 802.1x port so that it shuts down, generates a syslog error, or discards packets from a new device when:

- a device connects to an 802.1x-enabled port
- the maximum number of allowed about devices have been authenticated on the port

Beginning in privileged EXEC mode, follow these steps to configure the security violation actions on the switch:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:**
  
  Switch# configure terminal | |
| **Step 2** aaa new-model | Enables AAA. |
| **Example:**
  
  Switch(config)# aaa new-model | |
<p>| <strong>Step 3</strong> aaa authentication dot1x {default} method1 | Creates an 802.1x authentication method list. To create a default list that is used when a named list is <strong>not</strong> specified in the authentication command, use the <code>default</code> keyword followed |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>default group radius</td>
<td>by the method that is to be used in default situations. The default method list is automatically applied to all ports. For method1, enter the group radius keywords to use the list of all RADIUS servers for authentication.</td>
</tr>
</tbody>
</table>

**Step 4**

```
interface interface-id
```

**Example:**

```
Switch(config)# interface gigabitethernet1/0/4
```

Specifies the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.

**Step 5**

```
switchport mode access
```

**Example:**

```
Switch(config-if)# switchport mode access
```

Sets the port to access mode.

**Step 6**

```
authentication violation {shutdown | restrict | protect | replace}
```

**Example:**

```
Switch(config-if)# authentication violation restrict
```

Configures the violation mode. The keywords have these meanings:

- **shutdown**—Error disable the port.
- **restrict**—Generate a syslog error.
- **protect**—Drop packets from any new device that sends traffic to the port.
- **replace**—Removes the current session and authenticates with the new host.

**Step 7**

```
end
```

**Example:**

```
Switch(config-if)# end
```

Returns to privileged EXEC mode.

---

**Configuring 802.1x Authentication**

To allow per-user ACLs or VLAN assignment, you must enable AAA authorization to configure the switch for all network-related service requests.

This is the 802.1x AAA process:
Before you begin

To configure 802.1x port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>A user connects to a port on the switch.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Authentication is performed.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>The switch sends a start message to an accounting server.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Re-authentication is performed, as necessary.</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>The switch sends an interim accounting update to the accounting server that is based on the result of re-authentication.</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>The user disconnects from the port.</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>The switch sends a stop message to the accounting server.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring 802.1x Port-Based Authentication

Beginning in privileged EXEC mode, follow these steps to configure 802.1x port-based authentication:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa new-model</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa authentication dot1x {default} method1</td>
<td>Creates an 802.1x authentication method list.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To create a default list that is used when a named list is not specified in the</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring 802.1x Port-Based Authentication

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch(config)# aaa authentication dot1x</strong> default group radius</td>
<td><strong>authentication</strong> command, use the <strong>default</strong> keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports. For <strong>method1</strong>, enter the <strong>group radius</strong> keywords to use the list of all RADIUS servers for authentication. <strong>Note</strong> Though other keywords are visible in the command-line help string, only the <strong>group radius</strong> keywords are supported.</td>
</tr>
<tr>
<td><strong>Step 4</strong> dot1x system-auth-control</td>
<td>Enables 802.1x authentication globally on the switch.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# dot1x system-auth-control</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> aaa authorization network {default} group radius</td>
<td>(Optional) Configures the switch to use user-RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa authorization network default group radius</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> radius server <strong>server name</strong></td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# radius server rsim address ipv4 124.2.2.12</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> address {ipv4</td>
<td>ipv6} <strong>ip address</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-radius-server)# address ipv4 10.0.1.12</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> key <strong>string</strong></td>
<td>(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-radius-server)# key rad123</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Switch-to-RADIUS-Server Communication

Follow these steps to configure the RADIUS server parameters:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>ip radius source-interface vlan vlan interface number</td>
<td>Specifies that the RADIUS packets have the IP address of the indicated interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>Switch(config)# ip radius source-interface vlan 80</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>radius server server name</td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>Switch(config)# radius server rsim address ipv4 124.2.2.12</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>address {ipv4</td>
<td>ipv6} ip address</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>Switch(config-radius-server)# address ipv4 10.0.1.2 auth-port 1550 acct-port 1560</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>key string</td>
<td>(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>Switch(config-radius-server)# key rad123</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>exit</td>
<td>Exits the RADIUS server mode and enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>Switch(config-radius-server)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>radius-server dead-criteria tries num-tries</td>
<td>Specifies the number of unanswered sent messages to a RADIUS server before considering the server to be inactive. The range of num-tries is 1 to 100.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Configuring the Host Mode

Beginning in privileged EXEC mode, follow these steps to allow multiple hosts (clients) on an IEEE 802.1x-authorized port that has the `authentication port-control` interface configuration command set to `auto`. Use the `multi-domain` keyword to configure and enable multidomain authentication (MDA), which allows both a host and a voice device, such as an IP phone (Cisco or non-Cisco), on the same switch port. This procedure is optional.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>authentication host-mode [multi-auth</td>
</tr>
<tr>
<td>Example:</td>
<td>host-mode multi-host]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Example:

```
Switch(config)# radius-server
dead-criteria tries 30
```

```
Step 9
end
Example:
Switch(config)# end
```

Returns to privileged EXEC mode.
### Configuring Periodic Re-Authentication

You can enable periodic 802.1x client re-authentication and specify how often it occurs. If you do not specify a time period before enabling re-authentication, the number of seconds between attempts is 3600.

Beginning in privileged EXEC mode, follow these steps to enable periodic re-authentication of the client and to configure the number of seconds between re-authentication attempts. This procedure is optional.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface</td>
<td></td>
</tr>
<tr>
<td>gigabitethernet2/0/1</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

| Step 3 | authentication periodic  
|        | Example:  
|        | Switch(config-if)# authentication periodic |

**Purpose**

- Enables periodic re-authentication of the client, which is disabled by default.
- **Note:** The default value is 3600 seconds. To change the value of the reauthentication timer or to have the switch use a RADIUS-provided session timeout, enter the `authentication timer reauthenticate` command.

| Step 4 | authentication timer \{\{inactivity | reauthenticate | restart | unauthorized\}\} \{value\}  
|        | Example:  
|        | Switch(config-if)# authentication timer reauthenticate 180 |

**Purpose**

- Sets the number of seconds between re-authentication attempts.
- The `authentication timer` keywords have these meanings:
  - **inactivity**—Interval in seconds after which if there is no activity from the client then it is unauthorized
  - **reauthenticate**—Time in seconds after which an automatic re-authentication attempt is initiated
  - **restart value**—Interval in seconds after which an attempt is made to authenticate an unauthorized port
  - **unauthorized value**—Interval in seconds after which an unauthorized session will get deleted

**This command affects the behavior of the switch only if periodic re-authentication is enabled.**

| Step 5 | end  
|        | Example:  
|        | Switch(config-if)# end |

**Purpose**

- Returns to privileged EXEC mode.

---

### Changing the Quiet Period

When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. The `authentication timer restart` interface configuration command controls the idle period. A failed authentication of the client might occur because the client provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default.

Beginning in privileged EXEC mode, follow these steps to change the quiet period. This procedure is optional.
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config)# interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>authentication timer restart seconds</code></td>
<td>Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-if)# authentication timer restart 30</td>
<td>The range is 1 to 65535 seconds; the default is 60.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show authentication sessions interface interface-id</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch# show authentication sessions interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Changing the Switch-to-Client Retransmission Time

The client responds to the EAP-request/identity frame from the switch with an EAP-response/identity frame. If the switch does not receive this response, it waits a set period of time (known as the retransmission time) and then resends the frame.
You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to change the amount of time that the switch waits for client notification. This procedure is optional.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** interface interface-id          | Specifies the port to be configured, and enter interface configuration mode. |
| Example:                                   |                                                                         |
| Switch(config)# interface gigabitethernet2/0/1 |                                                                         |

| **Step 3** authentication timer reauthenticate seconds | Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request. The range is 1 to 65535 seconds; the default is 5. |
| Example:                                           |                                                                         |
| Switch(config-if)# authentication timer reauthenticate 60 |                                                                         |

| **Step 4** end                                 | Returns to privileged EXEC mode.                                       |
| Example:                                       |                                                                         |
| Switch(config-if)# end                        |                                                                         |

| **Step 5** show authentication sessions interface interface-id | Verifies your entries.                                                 |
| Example:                                                   |                                                                         |
| Switch# show authentication sessions interface gigabitethernet2/0/1 |                                                                         |

| **Step 6** copy running-config startup-config | (Optional) Saves your entries in the configuration file.                |
| Example:                                       |                                                                         |
| Switch# copy running-config                    |                                                                         |
Setting the Switch-to-Client Frame-Retransmission Number

In addition to changing the switch-to-client retransmission time, you can change the number of times that the switch sends an EAP-request/identity frame (assuming no response is received) to the client before restarting the authentication process.

**Note**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to set the switch-to-client frame-retransmission number. This procedure is optional.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface</td>
<td>Specifies the port to be configured, and enter interface configuration</td>
</tr>
<tr>
<td>gigabitethernet2/0/1</td>
<td>mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>dot1x max-reauth-req count</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# dot1x</td>
<td>Sets the number of times that the switch sends an EAP-request/identity</td>
</tr>
<tr>
<td>max-reauth-req 5</td>
<td>frame to the client before restarting the authentication process. The</td>
</tr>
<tr>
<td></td>
<td>range is 1 to 10; the default is 2.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Setting the Re-Authentication Number

You can also change the number of times that the switch restarts the authentication process before the port changes to the unauthorized state.

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to set the re-authentication number. This procedure is optional.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode access</td>
<td>Sets the port to access mode only if you previously configured the RADIUS server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>dot1x max-req count</td>
<td>Sets the number of times that the switch restarts the authentication process before the port changes to the unauthorized state. The range is 0 to 10; the default is 2.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# dot1x max-req 4</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

Enabling MAC Move

MAC move allows an authenticated host to move from one port on the switch to another.
Beginning in privileged EXEC mode, follow these steps to globally enable MAC move on the switch. This procedure is optional.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>authentication mac-move permit</td>
<td>Enables MAC move on the switch. Default is deny.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# authentication mac-move permit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Session Aware Networking mode, the default CLI is <strong>access-session mac-move deny</strong>. To enable Mac Move in Session Aware Networking, use the <strong>no access-session mac-move</strong> global configuration command.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In legacy mode (IBNS 1.0), default value for <strong>mac-move</strong> is <strong>deny</strong> and in C3PL mode (IBNS 2.0) default value is <strong>permit</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# show running-config</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Enabling MAC Replace**

MAC replace allows a host to replace an authenticated host on a port.

Beginning in privileged EXEC mode, follow these steps to enable MAC replace on an interface. This procedure is optional.
## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface gigabitethernet2/0/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>authentication violation {protect</td>
<td>replace</td>
</tr>
</tbody>
</table>
| Example: | Switch(config-if)# authentication violation replace | The other keywords have these effects:  
- **protect**: the port drops packets with unexpected MAC addresses without generating a system message.  
- **restrict**: violating packets are dropped by the CPU and a system message is generated.  
- **shutdown**: the port is error disabled when it receives an unexpected MAC address. |
| **Step 4** | end | Returns to privileged EXEC mode. |
| Example: | Switch(config-if)# end | |
| **Step 5** | show running-config | Verifies your entries. |
| Example: | Switch# show running-config | |
| **Step 6** | copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
| Example: | Switch# copy running-config startup-config | |
Configuring 802.1x Accounting

Enabling AAA system accounting with 802.1x accounting allows system reload events to be sent to the accounting RADIUS server for logging. The server can then infer that all active 802.1x sessions are closed. Because RADIUS uses the unreliable UDP transport protocol, accounting messages might be lost due to poor network conditions. If the switch does not receive the accounting response message from the RADIUS server after a configurable number of retransmissions of an accounting request, this system message appears:

Accounting message %s for session %s failed to receive Accounting Response.

When the stop message is not sent successfully, this message appears:

00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.

---

Note

You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and time stamps. To turn on these functions, enable logging of “Update/Watchdog packets from this AAA client” in your RADIUS server Network Configuration tab. Next, enable “CVS RADIUS Accounting” in your RADIUS server System Configuration tab.

Beginning in privileged EXEC mode, follow these steps to configure 802.1x accounting after AAA is enabled on your switch. This procedure is optional.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet1/0/3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa accounting dot1x default start-stop group radius</td>
<td>Enables 802.1x accounting using the list of all RADIUS servers.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# aaa accounting dot1x default start-stop group radius</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Guest VLAN

When you configure a guest VLAN, clients that are not 802.1x-capable are put into the guest VLAN when the server does not receive a response to its EAP request/identity frame. Clients that are 802.1x-capable but that fail authentication are not granted network access. The switch supports guest VLANs in single-host or multiple-hosts mode.

Beginning in privileged EXEC mode, follow these steps to configure a guest VLAN. This procedure is optional.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Restricted VLAN

When you configure a restricted VLAN on a switch stack or a switch, clients that are IEEE 802.1x-compliant are moved into the restricted VLAN when the authentication server does not receive a valid username and password. The switch supports restricted VLANs only in single-host mode.

Beginning in privileged EXEC mode, follow these steps to configure a restricted VLAN. This procedure is optional.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# interface gigabitethernet 2/0/2</code></td>
<td>Specifying an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode private-vlan host</code></td>
<td>You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN or a voice VLAN as an 802.1x guest VLAN.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode access</code></td>
<td></td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode private-vlan host</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

---

### Configuring a Restricted VLAN

When you configure a restricted VLAN on a switch stack or a switch, clients that are IEEE 802.1x-compliant are moved into the restricted VLAN when the authentication server does not receive a valid username and password. The switch supports restricted VLANs only in single-host mode.

Beginning in privileged EXEC mode, follow these steps to configure a restricted VLAN. This procedure is optional.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# interface gigabitethernet 2/0/2</code></td>
<td>Specifying an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode private-vlan host</code></td>
<td>You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN or a voice VLAN as an 802.1x guest VLAN.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode access</code></td>
<td></td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode private-vlan host</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

---

### Configuring a Restricted VLAN

When you configure a restricted VLAN on a switch stack or a switch, clients that are IEEE 802.1x-compliant are moved into the restricted VLAN when the authentication server does not receive a valid username and password. The switch supports restricted VLANs only in single-host mode.

Beginning in privileged EXEC mode, follow these steps to configure a restricted VLAN. This procedure is optional.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# interface gigabitethernet 2/0/2</code></td>
<td>Specifying an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode private-vlan host</code></td>
<td>You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN or a voice VLAN as an 802.1x guest VLAN.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode access</code></td>
<td></td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode private-vlan host</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring Number of Authentication Attempts on a Restricted VLAN

You can configure the maximum number of authentication attempts allowed before a user is assigned to the restricted VLAN by using the `authentication event retry retry count` interface configuration command. The range of allowable authentication attempts is 1 to 3. The default is 3 attempts.

Beginning in privileged EXEC mode, follow these steps to configure the maximum number of allowed authentication attempts. This procedure is optional.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

### PurposeCommand or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# interface gigabitethernet 2/0/2</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

Use one of the following:

- `switchport mode access`
- `switchport mode private-vlan host`

**Example:**

```
Switch(config-if)# switchport mode access
```

- Sets the port to access mode.
- Configures the Layer 2 port as a private-VLAN host port.

**Step 4**

**authentication port-control auto**

**Example:**

```
Switch(config-if)# authentication port-control auto
```

Enables 802.1x authentication on the port.

**Step 5**

**authentication event fail action authorize vlan vlan-id**

**Example:**

```
Switch(config-if)# authentication event fail action authorize vlan 2
```

Specifies an active VLAN as an 802.1x restricted VLAN. The range is 1 to 4094.

You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN.

**Step 6**

**end**

**Example:**

```
Switch(config-if)# end
```

Returns to privileged EXEC mode.
### Command or Action

- **Switch# configure terminal**

### Purpose

Specifies the port to be configured, and enter interface configuration mode.

### Step 2

- **interface interface-id**

**Example:**

Switch(config)# interface gigabitethernet 2/0/3

### Step 3

- **Example:**

  - switchport mode access
  - switchport mode private-vlan host

**Example:**

  or

Switch(config-if)# switchport mode access

### Step 4

- **authentication port-control auto**

**Example:**

Switch(config-if)# authentication port-control auto

### Step 5

- **authentication event fail action authorize vlan vlan-id**

**Example:**

Switch(config-if)# authentication event fail action authorize vlan 8

### Step 6

- **authentication event retry retry count**

**Example:**

Switch(config-if)# authentication event retry 2

### Step 7

- **end**

**Example:**

Switch(config-if)# end

 Enables 802.1x authentication on the port.

Specifies an active VLAN as an 802.1x restricted VLAN. The range is 1 to 4094.

You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN.

Specifies a number of authentication attempts to allow before a port moves to the restricted VLAN. The range is 1 to 3, and the default is 3.

Returns to privileged EXEC mode.
## Configuring 802.1x Inaccessible Authentication Bypass with Critical Voice VLAN

Beginning in privileged EXEC mode, follow these steps to configure critical voice VLAN on a port and enable the inaccessible authentication bypass feature.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;configure terminal&lt;br&gt;Example: Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;aaa new-model&lt;br&gt;Example: Switch(config)# aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;radius-server dead-criteria {time seconds} [tries number]&lt;br&gt;Example: Switch(config)# radius-server dead-criteria time 20 tries 10</td>
<td>Sets the conditions that determine when a RADIUS server is considered un-available or down (dead).&lt;br&gt;• time — 1 to 120 seconds. The switch dynamically determines a default <code>seconds</code> value between 10 and 60.&lt;br&gt;• number — 1 to 100 tries. The switch dynamically determines a default <code>tries number</code> between 10 and 100.</td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;radius-server dead-time minutes&lt;br&gt;Example: Switch(config)# radius-server dead-time 60</td>
<td>(Optional) Sets the number of minutes during which a RADIUS server is not sent requests. The range is from 0 to 1440 minutes (24 hours). The default is 0 minutes.</td>
</tr>
<tr>
<td><strong>Step 5</strong>&lt;br&gt;radius server server name&lt;br&gt;Example: Switch(config)# radius server rsim address ipv4 124.2.2.12</td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
</tr>
<tr>
<td><strong>Step 6</strong>&lt;br&gt;address {ipv4</td>
<td>ipv6} ip address auth-port port_number acct-port port_number&lt;br&gt;Example:</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Switch(config-radius-server)# address ipv4 10.0.1.2 auth-port 1550 acct-port 1560</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> key string</td>
<td>(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td>Example: Switch(config-radius-server)# key rad123</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits the RADIUS server mode and enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config-radius-server)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> dot1x critical {eapol</td>
<td>recovery delay milliseconds}</td>
</tr>
<tr>
<td>Example: Switch(config)# dot1x critical eapol (config)# dot1x critical recovery delay 2000</td>
<td>• eapol—Specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port.</td>
</tr>
<tr>
<td></td>
<td>• recovery delay milliseconds—Set the recovery delay period during which the switch waits to re-initialize a critical port when a RADIUS server that was unavailable becomes available. The range is from 1 to 10000 milliseconds. The default is 1000 milliseconds (a port can be re-initialized every second).</td>
</tr>
<tr>
<td><strong>Step 10</strong> interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 1/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> authentication event server dead action {authorize</td>
<td>reinitialize} vlan vlan-id</td>
</tr>
<tr>
<td>Example: Switch(config-if)# authentication event server dead action reinitialize vlan 20</td>
<td>• authorize—Move any new hosts trying to authenticate to the user-specified critical VLAN.</td>
</tr>
<tr>
<td></td>
<td>• reinitialize—Move all authorized hosts on the port to the user-specified critical VLAN.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>specifies the voice VLAN for the port. The voice VLAN cannot be the same as the critical data VLAN configured in Step 6.</td>
</tr>
<tr>
<td><code>switchport voice vlan vlan-id</code></td>
<td>Example: <code>Switch(config-if)# switchport voice vlan 10</code></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>Configures critical voice VLAN to move data traffic on the port to the voice VLAN if the RADIUS server is unreachable.</td>
</tr>
<tr>
<td><code>authentication event server dead action authorize voice</code></td>
<td>Example: <code>Switch(config-if)# authentication event server dead action authorize voice</code></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>(Optional) Verify your entries.</td>
</tr>
<tr>
<td><code>show authentication interface interface-id</code></td>
<td>Example: <code>Switch(config-if)# do show authentication interface gigabit 1/0/1</code></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>(Optional) Verify your entries.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>Example: <code>Switch(config-if)# do copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

**Example**

To return to the RADIUS server default settings, use the `no radius-server dead-criteria`, the `no radius-server deadtime`, and the `no radius server` global configuration commands. To disable inaccessible authentication bypass, use the `no authentication event server dead action` interface configuration command. To disable critical voice VLAN, use the `no authentication event server dead action authorize voice` interface configuration command.

**Example of Configuring Inaccessible Authentication Bypass**

This example shows how to configure the inaccessible authentication bypass feature:

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius server server1
Switch(config-radius-server)# address ipv4 172.29.36.49 acct-port 1618 auth-port 1612
Switch(config-radius-server)# key abc1234
Switch(config-radius-server)# exit
Switch(config)# dot1x critical eapol
```
Configuring 802.1x Authentication with WoL

Beginning in privileged EXEC mode, follow these steps to enable 802.1x authentication with WoL. This procedure is optional.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

Switch# configure terminal

<table>
<thead>
<tr>
<th>Step 2</th>
<th>interface interface-id</th>
<th>Specifies the port to be configured, and enter interface configuration mode.</th>
</tr>
</thead>
</table>

**Example:**

Switch(config)# interface gigabitethernet 2/0/3

| Step 3 | authentication control-direction {both | in} | Enables 802.1x authentication with WoL on the port, and use these keywords to configure the port as bidirectional or unidirectional. |
|--------|-------------------------------------------|--------------------------------------------------------------------------|

**Example:**

Switch(config-if)# authentication control-direction both

- **both**—Sets the port as bidirectional. The port cannot receive packets from or send packets to the host. By default, the port is bidirectional.
- **in**—Sets the port as unidirectional. The port can send packets to the host but cannot receive packets from the host.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>end</th>
<th>Returns to privileged EXEC mode.</th>
</tr>
</thead>
</table>

**Example:**

Switch(config-if)# end

<table>
<thead>
<tr>
<th>Step 5</th>
<th>show authentication sessions interface interface-id</th>
<th>Verifies your entries.</th>
</tr>
</thead>
</table>

**Example:**

Switch(config-if)# show authentication sessions interface 1/0/1

```
Switch(config)# dot1x critical recovery delay 2000
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```
**Configuring MAC Authentication Bypass**

Beginning in privileged EXEC mode, follow these steps to enable MAC authentication bypass. This procedure is optional.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> authentication port-control auto</td>
<td>Enables 802.1x authentication on the port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication port-control auto</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> mab [eap]</td>
<td>Enables MAC authentication bypass. (Optional) Use the eap keyword to configure the switch to use EAP for authorization.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# mab</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Configuring 802.1x User Distribution

Beginning in privileged EXEC mode, follow these steps to configure a VLAN group and to map a VLAN to it:

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> vlan group vlan-group-name vlan-list</td>
<td>Configures a VLAN group, and maps a single VLAN or a range of VLANs to it.</td>
</tr>
<tr>
<td>Example: Switch(config)# vlan group eng-dept vlan-list 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no vlan group vlan-group-name vlan-list</td>
<td>Clears the VLAN group configuration or elements of the VLAN group configuration.</td>
</tr>
<tr>
<td>Example: Switch(config)# no vlan group eng-dept vlan-list 10</td>
<td></td>
</tr>
</tbody>
</table>

Example of Configuring VLAN Groups

This example shows how to configure the VLAN groups, to map the VLANs to the groups, to and verify the VLAN group configurations and mapping to the specified VLANs:

```
Switch(config)# vlan group eng-dept vlan-list 10
Switch(config)# show vlan group group-name eng-dept
Group Name               Vlans Mapped
------------------------- -----------
eng-dept                 10
```
**Configuring NAC Layer 2 802.1x Validation**

You can configure NAC Layer 2 802.1x validation, which is also referred to as 802.1x authentication with a RADIUS server.

Beginning in privileged EXEC mode, follow these steps to configure NAC Layer 2 802.1x validation. The procedure is optional.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For more information about these commands, see the *Cisco IOS Security Command Reference*. 

---

**This example shows how to add a VLAN to an existing VLAN group and to verify that the VLAN was added:**

Switch(config)# show dot1x vlan-group all

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Vlans Mapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>eng-dept</td>
<td>10</td>
</tr>
<tr>
<td>hr-dept</td>
<td>20</td>
</tr>
</tbody>
</table>

**This example shows how to remove a VLAN from a VLAN group:**

Switch# no vlan group eng-dept vlan-list 10

**This example shows that when all the VLANs are cleared from a VLAN group, the VLAN group is cleared:**

Switch(config)# no vlan group eng-dept vlan-list 30

Vlan 30 is successfully cleared from vlan group eng-dept.

Switch(config)# show vlan group group-name eng-dept

**This example shows how to clear all the VLAN groups:**

Switch(config)# no vlan group end-dept vlan-list all

Switch(config)# show vlan-group all

Form more information about these commands, see the *Cisco IOS Security Command Reference*. 

---

**Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E**

1041
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface gigabitethernet2/0/3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switchport mode access</td>
<td>Sets the port to access mode only if you configured the RADIUS server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>authentication event no-response action authorize vlan vlan-id</td>
<td>Specifies an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN, or a voice VLAN as an 802.1x guest VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# authentication event no-response action authorize vlan 8</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>authentication periodic</td>
<td>Enables periodic re-authentication of the client, which is disabled by default.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# authentication periodic</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>authentication timer reauthenticate</td>
<td>Sets re-authentication attempt for the client (set to one hour). This command affects the behavior of the switch only if periodic re-authentication is enabled.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# authentication timer reauthenticate</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>show authentication sessions interface interface-id</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# show authentication sessions interface gigabitethernet2/0/3</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Limiting Login for Users

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa new-model</td>
<td>Enables the authentication, authorization, and accounting (AAA) access control model.</td>
</tr>
<tr>
<td>Example: Device(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa authentication login default local</td>
<td>Sets the authentication, authorization, and accounting (AAA) authentication by using the default authentication methods.</td>
</tr>
<tr>
<td>Example: Device(config)# aaa authentication login default local</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> aaa authentication rejected ( n ) in ( m ) ban ( x )</td>
<td>Configures the time period for which an user is blocked, if the user fails to successfully login within the specified time and login attempts.</td>
</tr>
<tr>
<td>Example: Device(config)# aaa authentication rejected 3 in 20 ban 300</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show aaa local user blocked</td>
<td>Displays the list of local users who were blocked.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# show aaa local user blocked</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>clear aaa local user blocked username username</td>
<td>Clears the information about the blocked local user.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# clear aaa local user blocked username user1</td>
<td></td>
</tr>
</tbody>
</table>

### Example

The following is sample output from the `show aaa local user blocked` command:

```
Device# show aaa local user blocked

Local-user          State
user1               Watched (till 11:34:42 IST Feb 5 2015)
```

### Configuring an Authenticator Switch with NEAT

Configuring this feature requires that one switch outside a wiring closet is configured as a supplicant and is connected to an authenticator switch.

---

**Note**

The `cisco-av-pairs` must be configured as `device-traffic-class=switch` on the ACS, which sets the interface as a trunk after the supplicant is successfully authenticated.

---

Beginning in privileged EXEC mode, follow these steps to configure a switch as an authenticator:

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cisp enable</td>
<td>Enables CISP.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# cisp enable</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# interface gigabitethernet 2/0/1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>switchport mode access</code></td>
<td>Sets the port mode to <code>access</code>.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode access</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>authentication port-control auto</code></td>
<td>Sets the port-authentication mode to <code>auto</code>.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# authentication port-control auto</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>dot1x pae authenticator</code></td>
<td>Configures the interface as a port access entity (PAE) authenticator.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# dot1x pae authenticator</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>spanning-tree portfast</code></td>
<td>Enables Port Fast on an access port connected to a single workstation or server.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# spanning-tree portfast trunk</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# end</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>show running-config interface interface-id</code></td>
<td>Verifies your configuration.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show running-config interface gigabitethernet 2/0/1</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Supplicant Switch with NEAT

Beginning in privileged EXEC mode, follow these steps to configure a switch as a supplicant:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enable CISP</td>
</tr>
<tr>
<td><code>cisp enable</code></td>
<td>Enables CISP</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# cisp enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Create 802.1x credentials profile.</td>
</tr>
<tr>
<td><code>dot1x credentials profile</code></td>
<td>Creates 802.1x credentials profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# dot1x credentials test</code></td>
<td>Creates 802.1x credentials profile.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Create a username</td>
</tr>
<tr>
<td><code>username suppswitch</code></td>
<td>Creates a username</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# username suppswitch</code></td>
<td>Creates a username</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Create a password for the new username.</td>
</tr>
<tr>
<td><code>password password</code></td>
<td>Creates a password for the new username.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# password myswitch</code></td>
<td>Creates a password for the new username.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>6</td>
<td>dot1x supplicant force-multicast</td>
</tr>
<tr>
<td>7</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>8</td>
<td>switchport trunk encapsulation dot1q</td>
</tr>
<tr>
<td>9</td>
<td>switchport mode trunk</td>
</tr>
<tr>
<td>10</td>
<td>dot1x pae supplicant</td>
</tr>
<tr>
<td>11</td>
<td>dot1x credentials profile-name</td>
</tr>
<tr>
<td>12</td>
<td>end</td>
</tr>
<tr>
<td>13</td>
<td>show running-config interface interface-id</td>
</tr>
</tbody>
</table>
### Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs


**Note**

You must configure a downloadable ACL on the ACS before downloading it to the switch.

After authentication on the port, you can use the `show ip access-list` privileged EXEC command to display the downloaded ACLs on the port.

### Configuring Downloadable ACLs

The policies take effect after client authentication and the client IP address addition to the IP device tracking table. The switch then applies the downloadable ACL to the port.

Beginning in privileged EXEC mode:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>ip device tracking</code></td>
<td>Sets the ip device tracking table.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>ip device tracking</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# ip device tracking</code></td>
<td>Enables AAA.</td>
</tr>
</tbody>
</table>

#### Step 3

**aaa new-model**

**Example:**

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

#### Step 4

**aaa authorization network default local group radius**

**Example:**

```
Switch(config)# aaa authorization network default local group radius
```

Sets the authorization method to local. To remove the authorization method, use the `no` command.

#### Step 5

**radius-server vsa send authentication**

**Example:**

```
Switch(config)# radius-server vsa send authentication
```

Configures the radius vsa send authentication.

#### Step 6

**interface interface-id**

**Example:**

```
Switch(config)# interface gigabitethernet2/0/4
```

Specifies the port to be configured, and enter interface configuration mode.

#### Step 7

**ip access-group acl-id in**

**Example:**

```
Switch(config-if)# ip access-group default_acl in
```

Configures the default ACL on the port in the input direction.

**Note**

The acl-id is an access list name or number.

#### Step 8

**show running-config interface interface-id**

**Example:**

```
Switch(config-if)# show running-config interface gigabitethernet2/0/4
```

Verifies your configuration.

#### Step 9

**copy running-config startup-config**

**Example:**

```
Switch# copy running-config
```

(Optional) Saves your entries in the configuration file.
### Configuring a Downloadable Policy

Beginning in privileged EXEC mode:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`access-list access-list-number { deny</td>
<td>permit } { hostname</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>access-list 1 deny any log</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>interface interface-id</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>interface</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>gigabitethernet2/0/2</td>
<td>Configure the default ACL on the port in the input direction.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**

```text
ip access-group acl-id in
```

**Example:**

```
Switch(config-if)# ip access-group default_acl in
```

**Note** The acl-id is an access list name or number.

**Step 5**

```text
exit
```

**Example:**

```
Switch(config-if)# exit
```

**Step 6**

```text
aaa new-model
```

**Example:**

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

**Step 7**

```text
aaa authorization network default group radius
```

**Example:**

```
Switch(config)# aaa authorization network default group radius
```

Sets the authorization method to local. To remove the authorization method, use the `no aaa authorization network default group radius` command.

**Step 8**

```text
ip device tracking
```

**Example:**

```
Switch(config)# ip device tracking
```

Enables the IP device tracking table.

To disable the IP device tracking table, use the `no ip device tracking` global configuration commands.

**Step 9**

```text
ip device tracking probe [count | interval | use-svi]
```

**Example:**

```
Switch(config)# ip device tracking probe count
```

(Optional) Configures the IP device tracking table:

- **count**—Sets the number of times that the switch sends the ARP probe. The range is from 1 to 5. The default is 3.
- **interval**—Sets the number of seconds that the switch waits for a response before resending the ARP probe. The range is from 30 to 300 seconds. The default is 30 seconds.
- **use-svi**—Uses the switch virtual interface (SVI) IP address as source of ARP probes.
Configuring VLAN ID-based MAC Authentication

Beginning in privileged EXEC mode, follow these steps:

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> mab request format attribute 32 vlan access-vlan</td>
<td>Enables VLAN ID-based MAC authentication.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# mab request format attribute 32 vlan access-vlan</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Flexible Authentication Ordering

The examples used in the instructions below changes the order of Flexible Authentication Ordering so that MAB is attempted before IEEE 802.1X authentication (dot1x). MAB is configured as the first authentication method, so MAB will have priority over all other authentication methods.

Beginning in privileged EXEC mode, follow these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>interface interface-id</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch(config)# interface gigabitethernet 1/0/1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>switchport mode access</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch(config-if)# switchport mode access</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**authentication order [ dot1x</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>**authentication priority [ dot1x</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>end</strong>&lt;br&gt;<strong>Example:</strong></td>
</tr>
</tbody>
</table>

(Optional) Sets the order of authentication methods used on a port.

(Optional) Adds an authentication method to the port-priority list.

Returns to privileged EXEC mode.
### Configuring Open1x

Beginning in privileged EXEC mode, follow these steps to enable manual control of the port authorization state:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>interface interface-id</code></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# <code>interface gigabitethernet 1/0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>switchport mode access</code></td>
<td>Sets the port to access mode only if you configured the RADIUS server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# <code>switchport mode access</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`authentication control-direction {both</td>
<td>in}`</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# <code>authentication control-direction both</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>authentication fallback name</code></td>
<td>(Optional) Configures a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# <code>authentication fallback profile1</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 6</td>
<td>`authentication host-mode [multi-auth</td>
<td>multi-domain</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# authentication host-mode multi-auth</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>authentication open</code></td>
<td>(Optional) Enables or disable open access on a port.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# authentication open</code></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>`authentication order [ dot1x</td>
<td>mab ]</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# authentication order dot1x webauth</code></td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td><code>authentication periodic</code></td>
<td>(Optional) Enables or disable reauthentication on a port.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# authentication periodic</code></td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>`authentication port-control {auto</td>
<td>force-authorized</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# authentication port-control auto</code></td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Disabling 802.1x Authentication on the Port**

You can disable 802.1x authentication on the port by using the `no dot1x pae` interface configuration command.

Beginning in privileged EXEC mode, follow these steps to disable 802.1x authentication on the port. This procedure is optional.
### Resetting the 802.1x Authentication Configuration to the Default Values

Beginning in privileged EXEC mode, follow these steps to reset the 802.1x authentication configuration to the default values. This procedure is optional.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> switchport mode access</td>
<td>(Optional) Sets the port to access mode only if you configured the RADIUS server.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no dot1x pae authenticator</td>
<td>Disables 802.1x authentication on the port.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# no dot1x pae authenticator</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

**Purpose**

<table>
<thead>
<tr>
<th>Step 2</th>
<th>interface interface-id</th>
<th>Enters interface configuration mode, and specify the port to be configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config)# interface gigabitethernet 1/0/2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>dot1x default</th>
<th>Resets the 802.1x parameters to the default values.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config-if)# dot1x default</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>end</th>
<th>Returns to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

---

### Monitoring 802.1x Statistics and Status

#### Table 75: Privileged EXEC show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dot1x all statistics</td>
<td>Displays 802.1x statistics for all ports</td>
</tr>
<tr>
<td>show dot1x interface interface-id statistics</td>
<td>Displays 802.1x statistics for a specific port</td>
</tr>
<tr>
<td>show dot1x all [count</td>
<td>details</td>
</tr>
<tr>
<td>show dot1x interface interface-id</td>
<td>Displays the 802.1x administrative and operational status for a specific port</td>
</tr>
</tbody>
</table>

#### Table 76: Global Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no dot1x logging verbose</td>
<td>Filters verbose 802.1x authentication messages (beginning with Cisco IOS Release 12.2(55)SE)</td>
</tr>
</tbody>
</table>

For detailed information about the fields in these displays, see the command reference for this release.
## Additional References for IEEE 802.1x Port-Based Authentication

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>

### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for 802.1x Port-Based Authentication

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td></td>
<td>Supports the use of same authorization methods on all the Catalyst switches in a</td>
</tr>
<tr>
<td></td>
<td>network.</td>
</tr>
<tr>
<td></td>
<td>Supports filtering verbose system messages from the authentication manager.</td>
</tr>
</tbody>
</table>
CHAPTER 54

Configuring MACsec Encryption

- Finding Feature Information, on page 1061
- Restriction for MACSec Encryption, on page 1061
- Information About MACsec Encryption, on page 1061
- Configuring MKA and MACsec, on page 1066
- Information About Cisco TrustSec, on page 1069
- Configuring Cisco TrustSec MACsec, on page 1071
- Configuration Examples, on page 1077

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restriction for MACSec Encryption

- While configuring MACsec MKA using EAP-TLS, MACsec secure channels encrypt counters won't increment before first Rekey.

Information About MACsec Encryption

This chapter describes how to configure Media Access Control Security (MACsec) encryption on the Catalyst switches. MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. The switch also supports MACsec link layer switch-to-switch security by using Cisco TrustSec Network Device Admission Control (NDAC) and the Security Association Protocol (SAP) key exchange. Link layer security can include both packet authentication between switches and MACsec encryption between switches (encryption is optional).
MACsec is not supported on switches running the NPE or the LAN base image.

All downlink ports on the switch can run Cisco TrustSec MACsec link layer switch-to-switch security.

### Table 77: MACsec Support on Switch Ports

<table>
<thead>
<tr>
<th>Interface</th>
<th>Connections</th>
<th>MACsec support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switchports connected to other switches</td>
<td>Switch-to-switch</td>
<td>Cisco TrustSec NDAC MACsec</td>
</tr>
</tbody>
</table>

Cisco TrustSec and Cisco SAP are meant only for switch-to-switch links and are not supported on switch ports connected to end hosts, such as PCs or IP phones. Cisco NDAC and SAP are mutually exclusive with Network Edge Access Topology (NEAT), which is used for compact switches to extend security outside the wiring closet.

## Media Access Control Security and MACsec Key Agreement

MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP-TLS) or Pre Shared Key (PSK) framework.

A switch using MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the MKA peer. MACsec frames are encrypted and protected with an integrity check value (ICV). When the switch receives frames from the MKA peer, it decrypts them and calculates the correct ICV by using session keys provided by MKA. The switch compares that ICV to the ICV within the frame. If they are not identical, the frame is dropped. The switch also encrypts and adds an ICV to any frames sent over the secured port (the access point used to provide the secure MAC service to a MKA peer) using the current session key.

The MKA Protocol manages the encryption keys used by the underlying MACsec protocol. The basic requirements of MKA are defined in 802.1x-REV. The MKA Protocol extends 802.1x to allow peer discovery with confirmation of mutual authentication and sharing of MACsec secret keys to protect data exchanged by the peers.

The EAP framework implements MKA as a newly defined EAP-over-LAN (EAPOL) packet. EAP authentication produces a master session key (MSK) shared by both partners in the data exchange. Entering the EAP session ID generates a secure connectivity association key name (CKN). The switch acts as the authenticator for both uplink and downlink; and acts as the key server for downlink. It generates a random secure association key (SAK), which is sent to the client partner. The client is never a key server and can only interact with a single MKA entity, the key server. After key derivation and generation, the switch sends periodic transports to the partner at a default interval of 2 seconds.

The packet body in an EAPOL Protocol Data Unit (PDU) is referred to as a MACsec Key Agreement PDU (MKPDU). MKA sessions and participants are deleted when the MKA lifetime (6 seconds) passes with no MKPDU received from a participant. For example, if a MKA peer disconnects, the participant on the switch continues to operate MKA until 6 seconds have elapsed after the last MKPDU is received from the MKA peer.
Integrity check value (ICV) indicator in MKPDU is optional. ICV is not optional when the traffic is encrypted.

Note

EAPoL Announcements indicate the use of the type of keying material. The announcements can be used to announce the capability of the supplicant as well as the authenticator. Based on the capability of each side, the largest common denominator of the keying material could be used.

Prior to Cisco IOS XE Fuji 16.8.1a, should-secure was supported for MKA and SAP. With should-secure enabled, if the peer is configured for MACsec, the data traffic is encrypted, otherwise it is sent in clear text. Starting with Cisco IOS XE Fuji 16.8.1a, must-secure support is enabled on both the ingress and the egress. Must-secure is supported for MKA and SAP. With must-secure enabled, only EAPoL traffic will not be encrypted. The rest of the traffic will be encrypted. Unencrypted packets are dropped.

Note

Must-secure mode is enabled by default.

MKA Policies

To enable MKA on an interface, a defined MKA policy should be applied to the interface. Removing the MKA policy disables MKA on that interface. You can configure these options:

- Policy name, not to exceed 16 ASCII characters.
- Confidentiality (encryption) offset of 0, 30, or 50 bytes for each physical interface
- Replay protection. You can configure MACsec window size, as defined by the number of out-of-order frames that are accepted. This value is used while installing the security associations in the MACsec. A value of 0 means that frames are accepted only in the correct order.

Virtual Ports

You use virtual ports for multiple secured connectivity associations on a single physical port. Each connectivity association (pair) represents a virtual port, with a maximum of two virtual ports per physical port. Only one of the two virtual ports can be part of a data VLAN; the other must externally tag its packets for the voice VLAN. You cannot simultaneously host secured and unsecured sessions in the same VLAN on the same port. Because of this limitation, 802.1x multiple authentication mode is not supported.

The exception to this limitation is in multiple-host mode when the first MACsec supplicant is successfully authenticated and connected to a hub that is connected to the switch. A non-MACsec host connected to the hub can send traffic without authentication because it is in multiple-host mode. We do not recommend using multi-host mode because after the first successful client, authentication is not required for other clients.

Virtual ports represent an arbitrary identifier for a connectivity association and have no meaning outside the MKA Protocol. A virtual port corresponds to a separate logical port ID. Valid port IDs for a virtual port are 0x0002 to 0xFFFF. Each virtual port receives a unique secure channel identifier (SCI) based on the MAC address of the physical interface concatenated with a 16-bit port ID.

MACsec and Stacking

A Switch stack master running MACsec maintains the configuration files that show which ports on a member switch support MACsec. The stack master performs these functions:
• Processes secure channel and secure association creation and deletion
• Sends secure association service requests to the stack members.
• Processes packet number and replay-window information from local or remote ports and notifies the key management protocol.
• Sends MACsec initialization requests with the globally configured options to new switches that are added to the stack.
• Sends any per-port configuration to the member switches.

A member switch performs these functions:
• Processes MACsec initialization requests from the stack master.
• Processes MACsec service requests sent by the stack master.
• Sends information about local ports to the stack master.

In case of a stack master changeover, all secured sessions are brought down and then reestablished. The authentication manager recognizes any secured sessions and initiates teardown of these sessions.

Note
If you are using 1G SFP modules for inter switch connection, change system MTU to 1550 byte to ensure support of MACsec overhead.

MACsec, MKA and 802.1x Host Modes

You can use MACsec and the MKA Protocol with 802.1x single-host mode or Multi Domain Authentication (MDA) mode. Multiple authentication mode is not supported.

Single-Host Mode

The figure shows how a single EAP authenticated session is secured by MACsec by using MKA

Figure 63: MACsec in Single-Host Mode with a Secured Data Session

MKA Statistics

Some MKA counters are aggregated globally, while others are updated both globally and per session. You can also obtain information about the status of MKA sessions.

This is an example of the `show mka statistics` command output:

```
Switch# show mka statistics
MKA Global Statistics
----------------------------
MKA Session Totals
Secured...................... 32
Reauthentication Attempts.. 31
```

Deleted (Secured)........... 1
Keepalive Timeouts......... 0

**CA Statistics**
- Pairwise CAKs Derived...... 32
- Pairwise CAK Rekeys........ 31
- Group CAKs Generated........ 0
- Group CAKs Received........ 0

**SA Statistics**
- SAKs Generated............. 32
- SAKs Rekeyed................ 31
- SAKs Received............... 0
- SAK Responses Received..... 32

**MKPDU Statistics**
- MKPDUs Validated & Rx...... 580
  "Distributed SAK"........... 0
  "Distributed CAK"........... 0
- MKPDUs Transmitted......... 597
  "Distributed SAK"........... 32
  "Distributed CAK"........... 0

**MKA Error Counter Totals**

| Error Type                    | Count
|-------------------------------|-------
| Bring-up Failures             | 0     
| Reauthentication Failures     | 0     

**SAK Failures**
- SAK Generation............... 0
- Hash Key Generation........... 0
- SAK Encryption/Wrap........... 0
- SAK Decryption/Unwrap......... 0

**CA Failures**
- Group CAK Generation......... 0
- Group CAK Encryption/Wrap..... 0
- Group CAK Decryption/Unwrap... 0
- Pairwise CAK Derivation....... 0
- ARN Derivation............... 0
- ICK Derivation............... 0
- KEK Derivation............... 0
- Invalid Peer MACsec Capability.. 2

**MACsec Failures**
- Rx SC Creation................ 0
- Tx SC Creation................ 0
- Rx SA Installation............. 0
- Tx SA Installation............. 0

**MKPDU Failures**
- MKPDU Tx....................... 0
- MKPDU Rx Validation........... 0
- MKPDU Rx Bad Peer MN........... 0
- MKPDU Rx Non-recent Peerlist MN.. 0
Configuring MKA and MACsec

Default MACsec MKA Configuration

MACsec is disabled. No MKA policies are configured.

Related Topics
- Configuring MACsec on an Interface, on page 1067
- Configuring an MKA Policy, on page 1066
- Example: Configuring MACsec on an Interface, on page 1077

Configuring an MKA Policy

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> mka policy policy name</td>
<td>Identify an MKA policy, and enter MKA policy configuration mode. The maximum policy name length is 16 characters.</td>
</tr>
<tr>
<td><strong>Step 3</strong> confidentiality-offset Offset value</td>
<td>Set the Confidentiality (encryption) offset for each physical interface</td>
</tr>
<tr>
<td></td>
<td>Note: Offset Value can be 0, 30 or 50. If you are using Anyconnect on the client, it is recommended to use Offset 0.</td>
</tr>
<tr>
<td><strong>Step 4</strong> replay-protection window-size frames</td>
<td>Enable replay protection, and configure the window size in number of frames. The range is from 0 to 4294967295. The default window size is 0.</td>
</tr>
<tr>
<td></td>
<td>Enter a window size of 0 is not the same as entering the <strong>no replay-protection command</strong>. Configuring a window size of 0 uses replay protection with a strict ordering of frames. Entering <strong>no replay-protection</strong> turns off MACsec replay-protection.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> show mka policy</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>
Example
This example configures the MKA policy `relay-policy`:

Switch(config)# mka policy replay-policy
Switch(config-mka-policy)# confidentiality-offset 0
Switch(config-mka-policy)# replay-protection window-size 300
Switch(config-mka-policy)# end

Related Topics
- Default MACsec MKA Configuration, on page 1066
- Example: Configuring MACsec on an Interface, on page 1077

Configuring MACsec on an Interface

Follow these steps to configure MACsec on an interface with one MACsec session for voice and one for data:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>interface interface-id</td>
<td>Identify the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.</td>
</tr>
<tr>
<td>4</td>
<td>switchport access vlan vlan-id</td>
<td>Configure the access VLAN for the port.</td>
</tr>
<tr>
<td>5</td>
<td>switchport mode access</td>
<td>Configure the interface as an access port.</td>
</tr>
<tr>
<td>6</td>
<td>macsec</td>
<td>Enable 802.1ae MACsec on the interface.</td>
</tr>
<tr>
<td>7</td>
<td>authentication event linksec fail action authorize vlan vlan-id</td>
<td>(Optional) Specify that the switch processes authentication link-security failures resulting from unrecognized user credentials by authorizing a restricted VLAN on the port after a failed authentication attempt.</td>
</tr>
<tr>
<td>8</td>
<td>authentication host-mode multi-domain</td>
<td>Configure authentication manager mode on the port to allow both a host and a voice device</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to be authenticated on the 802.1x-authorized port. If not configured, the default host mode is single.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>authentication linksec policy must-secure</strong> Set the LinkSec security policy to secure the session with MACsec if the peer is available. If not set, the default is <em>should secure</em>.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>authentication port-control auto</strong> Enable 802.1x authentication on the port. The port changes to the authorized or unauthorized state based on the authentication exchange between the switch and the client.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>authentication periodic</strong> Enable or Disable Reauthentication for this port.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>authentication timer reauthenticate</strong> Enter a value between 1 and 65535. Obtains re-authentication timeout value from the server.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>authentication violation protect</strong> Configure the port to drop unexpected incoming MAC addresses when a new device connects to a port or when a device connects to a port after the maximum number of devices are connected to that port. If not configured, the default is to shut down the port.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><strong>mka policy policy name</strong> Apply an existing MKA protocol policy to the interface, and enable MKA on the interface. If no MKA policy was configured (by entering the mka policy global configuration command), you must apply the MKA default policy to the interface by entering the mka default-policy interface configuration command</td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td><strong>dot1x pae authenticator</strong> Configure the port as an 802.1x port access entity (PAE) authenticator.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td><strong>spanning-tree portfast</strong> Enable spanning tree Port Fast on the interface in all its associated VLANs. When Port Fast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes</td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong></td>
<td><strong>end</strong> Returns to privileged EXEC mode.</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```
Switch(config)# end
```
### Information About Cisco TrustSec

The table below lists the TrustSec features to be eventually implemented on TrustSec-enabled Cisco switches. Successive general availability releases of TrustSec will expand the number of switches supported and the number of TrustSec features supported per switch.

<table>
<thead>
<tr>
<th>Cisco TrustSec Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1AE Tagging (MACsec)</td>
<td>Protocol for IEEE 802.1AE-based wire-rate hop-to-hop Layer 2 encryption. Between MACsec-capable devices, packets are encrypted on egress from the transmitting device, decrypted on ingress to the receiving device, and in the clear within the devices. This feature is only available between TrustSec hardware-capable devices. <strong>Note</strong>: This feature is not supported on Catalyst 3850 and Catalyst 3650 switches with Cisco IOS XE Denali 16.1.1</td>
</tr>
</tbody>
</table>
## Cisco TrustSec Feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Admission Control (EAC)</td>
<td>EAC is an authentication process for an endpoint user or a device connecting to the TrustSec domain. Usually EAC takes place at the access level switch. Successful authentication and authorization in the EAC process results in Security Group Tag assignment for the user or device. Currently EAC can be 802.1X, MAC Authentication Bypass (MAB), and Web Authentication Proxy (WebAuth).</td>
</tr>
<tr>
<td>Network Device Admission Control (NDAC)</td>
<td>NDAC is an authentication process where each network device in the TrustSec domain can verify the credentials and trustworthiness of its peer device. NDAC utilizes an authentication framework based on IEEE 802.1X port-based authentication and uses EAP-FAST as its EAP method. Successful authentication and authorization in NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.</td>
</tr>
<tr>
<td>Security Group Access Control List (SGACL)</td>
<td>A Security Group Access Control List (SGACL) associates a Security Group Tag with a policy. The policy is enforced upon SGT-tagged traffic egressing the TrustSec domain. In Cisco IOS XE Fuji 16.8.1, IPv6 support was enabled for SGACL enforcement and logging of VRF name was enabled in SGACL logs.</td>
</tr>
<tr>
<td>Security Association Protocol (SAP)</td>
<td>After NDAC authentication, the Security Association Protocol (SAP) automatically negotiates keys and the cipher suite for subsequent MACSec link encryption between TrustSec peers. SAP is defined in IEEE 802.11i. Note: This feature is not supported on Catalyst 3850 and Catalyst 3650 switches with Cisco IOS XE Denali 16.1.1</td>
</tr>
<tr>
<td>Security Group Tag (SGT)</td>
<td>An SGT is a 16-bit single label indicating the security classification of a source in the TrustSec domain. It is appended to an Ethernet frame or an IP packet. In Cisco IOS XE Fuji 16.8.1, Layer 2 Inline Tagging is supported for IPv6 multicast traffic with unicast source IPv6 addresses.</td>
</tr>
</tbody>
</table>

### Note

This feature is not supported on Catalyst 3850 and Catalyst 3650 switches with Cisco IOS XE Denali 16.1.1
Cisco TrustSec Feature | Description
---|---
SGT Exchange Protocol (SXP) | Security Group Tag Exchange Protocol (SXP). With SXP, devices that are not TrustSec-hardware-capable can receive SGT attributes for authenticated users and devices from the Cisco Identity Services Engine (ISE) or the Cisco Secure Access Control System (ACS). The devices can then forward a sourceIP-to-SGT binding to a TrustSec-hardware-capable device will tag the source traffic for SGACL enforcement.

When both ends of a link support 802.1AE MACsec, SAP negotiation occurs. An EAPOL-key exchange occurs between the supplicant and the authenticator to negotiate a cipher suite, exchange security parameters, and manage keys. Successful completion of these tasks results in the establishment of a security association (SA).

Depending on your software version and licensing and link hardware support, SAP negotiation can use one of these modes of operation:

- Galois Counter Mode (GCM)—authentication and encryption
- GCM authentication (GMAC)—GCM authentication, no encryption
- No Encapsulation—no encapsulation (clear text)
- Null—encapsulation, no authentication or encryption

Related Topics
- Configuring Cisco TrustSec MACsec, on page 1071

**Configuring Cisco TrustSec MACsec**

Related Topics
- Information About Cisco TrustSec, on page 1069

**Configuring Cisco TrustSec Credentials on the Switch**

To enable Cisco TrustSec features, you must create Cisco TrustSec credentials on the switch to use in other TrustSec configurations. Beginning in privilege EXEC mode, follow these steps to configure Cisco TrustSec credentials.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> cts credentials id device-id password cts-password</td>
<td>Specifies the Cisco TrustSec credentials for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST.</td>
</tr>
<tr>
<td>Example: Switch# cts credentials id trustsec password mypassword</td>
<td></td>
</tr>
<tr>
<td>id device-id—Specifies a Cisco TrustSec device ID for the switch. The device-id</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>argument has a maximum length of 32 characters and is case sensitive</td>
</tr>
<tr>
<td></td>
<td>• password <code>cts-password</code>—Specifies the Cisco TrustSec password for the device.</td>
</tr>
</tbody>
</table>

**Step 2**

**show cts credentials**

**Example:**

Switch# show cts credentials

(Optional) Displays Cisco TrustSec credentials configured on the switch.

**Step 3**

**copy running-config startup-config**

**Example:**

Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.

---

**Example**

To delete the Cisco TrustSec credentials, enter the `clear cts credentials` privileged EXEC command.

This example shows how to create Cisco TrustSec credentials.

Switch# `cts credentials id trustsec password mypassword`

CTS device ID and password have been inserted in the local keystore. Please make sure that the same ID and password are configured in the server database.

Switch# show cts credentials

CTS password is defined in keystore, device-id = trustsec

**What to do next**

Before you configure Cisco TrustSec MACsec authentication, you should configure Cisco TrustSec seed and non-seed devices. For 802.1x mode, you must configure at least one seed device, that device closest to the access control system (ACS). See this section in the Cisco TrustSec Configuration Guide: [http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html](http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html)

---

**Configuring Cisco TrustSec Switch-to-Switch Link Security in 802.1x Mode**

**Before you begin**

You enable Cisco TrustSec link layer switch-to-switch security on an interface that connects to another Cisco TrustSec device. When configuring Cisco TrustSec in 802.1x mode on an interface, follow these guidelines:

- To use 802.1x mode, you must globally enable 802.1x on each device. For more information 802.1x, see the Configuring IEEE 802.1x Port-Based Authentication chapter.

- If you select GCM as the SAP operating mode, you must have a MACsec encryption software license from Cisco. MACsec is supported on Catalyst 3850 and 3650 universal IP Services and IP Base licenses. It is not supported with the NPE license or with a LAN base service image.
If you select GCM without the required license, the interface is forced to a link-down state.

Beginning in privilege EXEC mode, follow these steps to configure Cisco TrustSec switch-to-switch link layer security with 802.1x:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# interface tengigabitethernet 1/1/2</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>cts dot1x</td>
<td>Configures the interface to perform NDAC authentication.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# cts dot1x</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>sap mode-list mode1 [mode2 [mode3 [mode4]]]</td>
<td>(Optional) Configures the SAP operation mode on the interface. The interface negotiates with the peer for a mutually acceptable mode. Enter the acceptable modes in your order of preference.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap</td>
<td></td>
</tr>
</tbody>
</table>

**Choices for mode** are:

- **gcm-encrypt**—Authentication and encryption

  **Note** Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption.

- **gmac**—Authentication, no encryption

- **no-encap**—No encapsulation

- **null**—Encapsulation, no authentication or encryption

**Note** If the interface is not capable of data link encryption, no-encap is the default and the only available SAP operating mode. SGT is not supported.
### Configuring Cisco TrustSec Switch-to-Switch Link Security in Manual Mode

#### Before you begin

When manually configuring Cisco TrustSec on an interface, consider these usage guidelines and restrictions:

- If no SAP parameters are defined, Cisco TrustSec encapsulation or encryption is not performed.
- If you select GCM as the SAP operating mode, you must have a MACsec Encryption software license from Cisco. If you select GCM without the required license, the interface is forced to a link-down state.

#### Example

This example shows how to enable Cisco TrustSec authentication in 802.1x mode on an interface using GCM as the preferred SAP mode:

```
Switch# configure terminal
Switch(config)# interface tengigabitethernet 1/1/2
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap

Switch(config-if-cts-dot1x)# exit
Switch(config-if)# end
```

#### Related Topics

- Cisco TrustSec Switch-to-Switch Link Security Configuration Example, on page 1080
• These protection levels are supported when you configure SAP pairwise master key (sap pmk):
  
  • SAP is not configured—no protection.

  • sap mode-list gcm-encrypt hmac no-encap—protection desirable but not mandatory.

  • sap mode-list gcm-encrypt hmac—confidentiality preferred and integrity required. The protection is selected by the supplicant according to supplicant preference.

  • sap mode-list hmac—integrity only.

  • sap mode-list gcm-encrypt—confidentiality required.

  • sap mode-list hmac gcm-encrypt—integrity required and preferred, confidentiality optional.

• When CTS is configured on an interface and the System MTU is set to a value greater than 9191, the resulting packet size is limited to 9190.

Beginning in privileged EXEC mode, follow these steps to manually configure Cisco TrustSec on an interface to another Cisco TrustSec device:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Example: | ```
Switch# configure terminal
``` | |
| Step 2 | interface interface-id | Note Enters interface configuration mode. |
| Example: | ```
Switch(config)# interface
tengigabitethernet 1/1/2
``` | |
| Step 3 | cts manual | Enters Cisco TrustSec manual configuration mode. |
| Example: | ```
Switch(config-if)# cts manual
``` | |
| Step 4 | sap pmk key [mode-list mode1 [mode2 [mode3 [mode4]]]] | (Optional) Configures the SAP pairwise master key (PMK) and operation mode. SAP is disabled by default in Cisco TrustSec manual mode. |
| Example: | ```
Switch(config-if-cts-manual)# sap pmk
1234abcdef mode-list
gcm-encrypt null no-encap
``` | • key—A hexadecimal value with an even number of characters and a maximum length of 32 characters. The SAP operation mode options:

  • gcm-encrypt—Authentication and encryption
### Configuring Cisco TrustSec Switch-to-Switch Link Security in Manual Mode

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>- gmac — Authentication, no encryption</td>
<td></td>
</tr>
<tr>
<td>- no-encap — No encapsulation</td>
<td></td>
</tr>
<tr>
<td>- null — Encapsulation, no authentication or encryption</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>- If the interface is not capable of data link encryption, <strong>no-encap</strong> is the default and the only available SAP operating mode. SGT is not supported.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>no propagate sgt</td>
<td>Use the no form of this command when the peer is incapable of processing a SGT. The no propagate sgt command prevents the interface from transmitting the SGT to the peer.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if-cts-manual)# no propagate sgt</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits Cisco TrustSec 802.1x interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if-cts-manual)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>show cts interface [interface-id</td>
<td>brief</td>
</tr>
</tbody>
</table>

### Example

This example shows how to configure Cisco TrustSec authentication in manual mode on an interface:

```plaintext
Switch# configure terminal
Switch(config)# interface tengigabitethernet 1/1/2
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# end
```

### Related Topics

- [Cisco TrustSec Switch-to-Switch Link Security Configuration Example](#), on page 1080
Configuration Examples

Example: Configuring MACsec on an Interface

Configuring MACsec on an Interface

Switch(config)# interface GigabitEthernet1/0/25
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access
Switch(config-if)# macsec
Switch(config-if)# authentication event linksec fail action authorize vlan 2
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# authentication linksec policy must-secure
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate
Switch(config-if)# mka policy replay-policy
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end

Switch# show authentication session interface gigabitethernet6/0/36

Interface MAC Address Method Domain Status Fg Session ID
----------------------------------------------------------------------
Gi6/0/36 001b.214c.a98c dot1x DATA Auth 020000D4000019440E54D478
Gi6/0/36 001b.0cdb.bdd8 mab VOICE Auth 020000D400000FB2001687B2

Key to Session Events Blocked Status Flags:

A - Applying Policy (multi-line status for details)
D - Awaiting Deletion
F - Final Removal in progress
I - Awaiting IIF ID allocation
N - Waiting for AAA to come up
P - Pushed Session
R - Removing User Profile (multi-line status for details)
U - Applying User Profile (multi-line status for details)
X - Unknown Blocker

Runnable methods list:
Handle Priority Name
16 5 dot1x
19 10 mab
23 15 webauth

Switch# show authentication session interface gigabitethernet6/0/36 details

Interface: GigabitEthernet6/0/36
IIF-ID: 0x1062E8000000AB0
MAC Address: 001b.214c.a98c
IPv6 Address: Unknown
IPv4 Address: 16.0.0.21
User-Name: D_MustSecure
Status: Authorized
Domain: DATA
Oper host mode: multi-domain
Oper control dir: both
Session timeout: 200s (local), Remaining: 187s
Timeout action: Reauthenticate
Common Session ID: 020000D4000019440E54D478
Acct Session ID: 0x000019D8
Handle: 0x86000996
Current Policy: POLICY_Gi6/0/36

Local Policies:
Idle timeout: 60 sec
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
Vlan Group: Vlan: 16
Security Policy: Must Secure
Security Status: Link Secured
SGT Value: 0

Method status list:
Method State
dot1x Authc Success

----------------------------------------
Interface: GigabitEthernet6/0/36
IIF-ID: 0x100200000000120
MAC Address: 001b.0cdb.bdd8
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: 00-1B-0C-DB-BD-D8
Status: Authorized
Domain: VOICE
Oper host mode: multi-domain
Oper control dir: both
Session timeout: 200s (local), Remaining: 177s
Timeout action: Reauthenticate
Common Session ID: 020000D400000FB2001687B2
Acct Session ID: 0x000019DB
Handle: 0xA0000006
Current Policy: POLICY_Gi6/0/36

Local Policies:
Idle timeout: 60 sec
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
Vlan Group: Vlan: 116
Security Policy: Must Not Secure
Security Status: Link Unsecure

Method status list:
Method State
dot1x Stopped
mab Authc Success

Switch# show macsec interface gigabitethernet6/0/3615
MACsec is enabled
Replay protect : enabled
Replay window : 0
Include SCI : yes
Use ES Enable : no
Use SCB Enable : no
Admin Pt2Pt MAC : forceTrue(1)
Pt2Pt MAC Operational : no
Cipher : GCM-AES-128
Confidentiality Offset : 0

Capabilities
Identifier :
Name :
ICV length : 16
Data length change supported : yes
Max. Rx SA : 16
Max. Tx SA : 16
Max. Rx SC : 8
Max. Tx SC : 8
Validate Frames : strict
PN threshold notification support : Yes
Ciphers supported : GCM-AES-128

Transmit Secure Channels
SCI : B000B43A70A40002
SC state : notInUse(2)
Elapsed time : 00:05:25
Start time : 7w0d
Current AN: 1
Previous AN: 0
Next PN: 0
SA State: notInUse(2)
Confidentiality : no
SAK Unchanged : no
SA Create time : 2d18h
SA Start time : 7w0d
SC Statistics
Auth-only Pkts : 0
Auth-only Bytes : 0
Encrypt Pkts : 308
Encrypt Bytes : 0
SA Statistics
Auth-only Pkts : 0
Encrypt Pkts : 182

Port Statistics
Receive Secure Channels
SCI : 001B214CA98C0000
SC state : notInUse(2)
Elapsed time : 00:05:25
Start time : 7w0d
Current AN: 1
Previous AN: 0
Next PN: 0
RX SA Count: 0
SA State: notInUse(2)
SAK Unchanged : no
SA Create time : 2d18h
SA Start time : 7w0d
SC Statistics
Notvalid pkts 0
Invalid pkts 0
Valid pkts 495
Valid bytes 0
Cisco TrustSec Switch-to-Switch Link Security Configuration Example

This example shows the configuration necessary for a seed and non-seed device for Cisco TrustSec switch-to-switch security. You must configure the AAA and RADIUS for link security. In this example, ACS-1 through ACS-3 can be any server names and cts-radius is the Cisco TrustSec server.

Seed Device Configuration:

```plaintext
Switch(config)# aaa new-model
Switch(config)# radius server ACS-1
Switch(config-radius-server)# address ipv4 10.5.120.12 auth-port 1812 acct-port 1813
Switch(config-radius-server)# pac key cisco123
Switch(config-radius-server)# exit
Switch(config)# radius server ACS-2
Switch(config-radius-server)# address ipv4 10.5.120.14 auth-port 1812 acct-port 1813
Switch(config-radius-server)# pac key cisco123
Switch(config-radius-server)# exit
Switch(config)# radius server ACS-3
Switch(config-radius-server)# address ipv4 10.5.120.15 auth-port 1812 acct-port 1813
Switch(config-radius-server)# pac key cisco123
Switch(config-radius-server)# exit
Switch(config)# aaa group server radius cts-radius
Switch(config-sg-radius)# server name ACS-1
Switch(config-sg-radius)# server name ACS-2
Switch(config-sg-radius)# server name ACS-3
Switch(config-sg-radius)# exit
Switch(config)# aaa authentication login default none
Switch(config)# aaa authentication dot1x default group cts-radius
Switch(config)# aaa authorization network cts-radius group cts-radius
Switch(config)# aaa session-id common
```
Switch(config)# cts authorization list cts-radius
Switch(config)# dot1x system-auth-control

Switch(config)# interface gi1/1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt gmac

Switch(config-if-cts-dot1x)# exit
Switch(config-if)# exit

Switch(config)# interface gi1/1/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt gmac
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# exit

Switch(config)# radius-server vsa send authentication
Switch(config)# exit
Switch# cts credentials id cts-36 password trustsec123

Non-Seed Device:
Switch(config)# aaa new-model
Switch(config)# aaa session-id common
Switch(config)# dot1x system-auth-control

Switch(config)# interface gi1/1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# shutdown
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# exit

Switch(config)# interface gi1/1/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# shutdown
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt gmac
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# exit

Switch(config)# radius-server vsa send authentication
Switch(config)# exit
Switch# cts credentials id cts-72 password trustsec123

Related Topics
Configuring Cisco TrustSec Switch-to-Switch Link Security in 802.1x Mode, on page 1072
Configuring Cisco TrustSec Switch-to-Switch Link Security in Manual Mode, on page 1074
Cisco TrustSec Switch-to-Switch Link Security Configuration Example
CHAPTER 55

Web-Based Authentication

This chapter describes how to configure web-based authentication on the switch. It contains these sections:

- Finding Feature Information, on page 1083
- Web-Based Authentication Overview, on page 1083
- How to Configure Web-Based Authentication, on page 1093
- Monitoring Web-Based Authentication Status, on page 1115
- Feature Information for Web-Based Authentication, on page 1116

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Web-Based Authentication Overview

Use the web-based authentication feature, known as web authentication proxy, to authenticate end users on host systems that do not run the IEEE 802.1x supplicant.

Note

You can configure web-based authentication on Layer 2 and Layer 3 interfaces.

When you initiate an HTTP session, web-based authentication intercepts ingress HTTP packets from the host and sends an HTML login page to the users. The users enter their credentials, which the web-based authentication feature sends to the authentication, authorization, and accounting (AAA) server for authentication.

If authentication succeeds, web-based authentication sends a Login-Successful HTML page to the host and applies the access policies returned by the AAA server.
If authentication fails, web-based authentication forwards a Login-Fail HTML page to the user, prompting the user to retry the login. If the user exceeds the maximum number of attempts, web-based authentication forwards a Login-Expired HTML page to the host, and the user is placed on a watch list for a waiting period.

**Note**

HTTPS traffic interception for central web authentication redirect is not supported.

**Note**

You should use global parameter-map (for method-type, custom, and redirect) only for using the same web authentication methods like consent, web consent, and webauth, for all the clients and SSIDs. This ensures that all the clients have the same web-authentication method.

If the requirement is to use Consent for one SSID and Web-authentication for another SSID, then you should use two named parameter-maps. You should configure Consent in first parameter-map and configure webauth in second parameter-map.

**Note**

The traceback that you receive when webauth client tries to do authentication does not have any performance or behavioral impact. It happens rarely when the context for which FFM replied back to EPM for ACL application is already dequeued (possibly due to timer expiry) and the session becomes ‘unauthorized’.

Based on where the web pages are hosted, the local web authentication can be categorized as follows:

- **Internal**—The internal default HTML pages (Login, Success, Fail, and Expire) in the controller are used during the local web authentication.
- **Customized**—The customized web pages (Login, Success, Fail, and Expire) are downloaded onto the controller and used during the local web authentication.
- **External**—The customized web pages are hosted on the external web server instead of using the in-built or custom web pages.

Based on the various web authentication pages, the types of web authentication are as follows:

- **Webauth**—This is a basic web authentication. Herein, the controller presents a policy page with the user name and password. You need to enter the correct credentials to access the network.
- **Consent or web-passthrough**—Herein, the controller presents a policy page with the Accept or Deny buttons. You need to click the Accept button to access the network.
- **Webconsent**—This is a combination of webauth and consent web authentication types. Herein, the controller presents a policy page with Accept or Deny buttons along with user name or password. You need to enter the correct credentials and click the Accept button to access the network.

**Note**

The Wireless web authentication feature does not support the bypass type.
Device Roles

With web-based authentication, the devices in the network have these specific roles:

- **Client**—The device (workstation) that requests access to the LAN and the services and responds to requests from the switch. The workstation must be running an HTML browser with JavaScript enabled.

- **Authentication server**—Authenticates the client. The authentication server validates the identity of the client and notifies the switch that the client is authorized to access the LAN and the switch services or that the client is denied.

- **Switch**—Controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client.

![Figure 64: Web-Based Authentication Device Roles](image)

This figure shows the roles of these devices in a network.

Host Detection

The switch maintains an IP device tracking table to store information about detected hosts.

By default, the IP device tracking feature is disabled on a switch. You must enable the IP device tracking feature to use web-based authentication.

For Layer 2 interfaces, web-based authentication detects IP hosts by using these mechanisms:

- **ARP based trigger**—ARP redirect ACL allows web-based authentication to detect hosts with a static IP address or a dynamic IP address.

- **Dynamic ARP inspection**

- **DHCP snooping**—Web-based authentication is notified when the switch creates a DHCP-binding entry for the host.

Session Creation

When web-based authentication detects a new host, it creates a session as follows:
• Reviews the exception list.
  If the host IP is included in the exception list, the policy from the exception list entry is applied, and the session is established.

• Reviews for authorization bypass
  If the host IP is not on the exception list, web-based authentication sends a nonresponsive-host (NRH) request to the server.
  If the server response is access accepted, authorization is bypassed for this host. The session is established.

• Sets up the HTTP intercept ACL
  If the server response to the NRH request is access rejected, the HTTP intercept ACL is activated, and the session waits for HTTP traffic from the host.

### Authentication Process

When you enable web-based authentication, these events occur:

• The user initiates an HTTP session.
• The HTTP traffic is intercepted, and authorization is initiated. The switch sends the login page to the user. The user enters a username and password, and the switch sends the entries to the authentication server.

• If the authentication succeeds, the switch downloads and activates the user’s access policy from the authentication server. The login success page is sent to the user.

• If the authentication fails, the switch sends the login fail page. The user retries the login. If the maximum number of attempts fails, the switch sends the login expired page, and the host is placed in a watch list. After the watch list times out, the user can retry the authentication process.

• If the authentication server does not respond to the switch, and if an AAA fail policy is configured, the switch applies the failure access policy to the host. The login success page is sent to the user.

• The switch reauthenticates a client when the host does not respond to an ARP probe on a Layer 2 interface, or when the host does not send any traffic within the idle timeout on a Layer 3 interface.

• The feature applies the downloaded timeout or the locally configured session timeout.

---

**Note**

Beginning with Cisco IOS XE Denali 16.1.1 and later, the default session timeout value for web-based authentication on WLC is 1800 seconds. The default session timeout value was infinite seconds, prior to Cisco IOS XE Denali 16.1.1.

• If the terminate action is RADIUS, the feature sends a nonresponsive host (NRH) request to the server. The terminate action is included in the response from the server.

• If the terminate action is default, the session is dismantled, and the applied policy is removed.
Local Web Authentication Banner

With Web Authentication, you can create a default and customized web-browser banners that appears when you log in to a switch.

The banner appears on both the login page and the authentication-result pop-up pages. The default banner messages are as follows:

• Authentication Successful
• Authentication Failed
• Authentication Expired

The Local Web Authentication Banner can be configured in legacy CLIs as follows:

• Legacy mode—Use the `ip admission auth-proxy-banner http` global configuration command.
• New-style mode—Use the `parameter-map type webauth global banner` global configuration command.

The default banner `Cisco Systems` and `Switch host-name Authentication` appear on the Login Page. `Cisco Systems` appears on the authentication result pop-up page.

Figure 65: Authentication Successful Banner

The banner can be customized as follows:

• Add a message, such as switch, router, or company name to the banner:
  • Legacy mode—Use the `ip admission auth-proxy-banner http banner-text`global configuration command.
  • New-style mode—Use the `parameter-map type webauth global banner` global configuration command.

• Add a logo or text file to the banner:
• Legacy mode—Use the **ip admission auth-proxy-banner** `http file-path` global configuration command.

• New-style mode—Use the **parameter-map type webauth global banner** global configuration command.

**Figure 66: Customized Web Banner**

If you do not enable a banner, only the username and password dialog boxes appear in the web authentication login screen, and no banner appears when you log into the switch.
For more information, see the Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) and the Web Authentication Enhancements - Customizing Authentication Proxy Web Pages.

### Web Authentication Customizable Web Pages

During the web-based authentication process, the switch internal HTTP server hosts four HTML pages to deliver to an authenticating client. The server uses these pages to notify you of these four-authentication process states:

- **Login**—Your credentials are requested.
- **Success**—The login was successful.
- **Fail**—The login failed.
- **Expire**—The login session has expired because of excessive login failures.

### Guidelines

- You can substitute your own HTML pages for the default internal HTML pages.
- You can use a logo or specify text in the `login`, `success`, `failure`, and `expire` web pages.
- On the banner page, you can specify text in the login page.
- The pages are in HTML.
- You must include an HTML redirect command in the success page to access a specific URL.
• The URL string must be a valid URL (for example, http://www.cisco.com). An incomplete URL might cause page not found or similar errors on a web browser.

• If you configure web pages for HTTP authentication, they must include the appropriate HTML commands (for example, to set the page time out, to set a hidden password, or to confirm that the same page is not submitted twice).

• The CLI command to redirect users to a specific URL is not available when the configured login form is enabled. The administrator should ensure that the redirection is configured in the web page.

• If the CLI command redirecting users to specific URL after authentication occurs is entered and then the command configuring web pages is entered, the CLI command redirecting users to a specific URL does not take effect.

• Configured web pages can be copied to the switch boot flash or flash.

• On stackable switches, configured pages can be accessed from the flash on the stack master or members.

• The login page can be on one flash, and the success and failure pages can be another flash (for example, the flash on the stack master or a member).

• You must configure all four pages.

• The banner page has no effect if it is configured with the web page.

• All of the logo files (image, flash, audio, video, and so on) that are stored in the system directory (for example, flash, disk0, or disk) and that must be displayed on the login page must use web_auth_<filename> as the file name.

• The configured authentication proxy feature supports both HTTP and SSL.

You can substitute your HTML pages for the default internal HTML pages. You can also specify a URL to which users are redirected after authentication occurs, which replaces the internal Success page.

Figure 68: Customizable Authentication Page
Authentication Proxy Web Page Guidelines

When configuring customized authentication proxy web pages, follow these guidelines:

- To enable the custom web pages feature, specify all four custom HTML files. If you specify fewer than four files, the internal default HTML pages are used.

- The four custom HTML files must be present on the flash memory of the switch. The maximum size of each HTML file is 8 KB.

- Any images on the custom pages must be on an accessible HTTP server. Configure an intercept ACL within the admission rule.

- Any external link from a custom page requires configuration of an intercept ACL within the admission rule.

- To access a valid DNS server, any name resolution required for external links or images requires configuration of an intercept ACL within the admission rule.

- If the custom web pages feature is enabled, a configured auth-proxy-banner is not used.

- If the custom web pages feature is enabled, the redirection URL for successful login feature is not available.

- To remove the specification of a custom file, use the `no` form of the command.

Because the custom login page is a public web form, consider these guidelines for the page:

- The login form must accept user entries for the username and password and must show them as `uname` and `pwd`.

- The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.

Related Topics

Customizing the Authentication Proxy Web Pages, on page 1101

Redirection URL for Successful Login Guidelines

When configuring a redirection URL for successful login, consider these guidelines:

- If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and is not available in the CLI. You can perform redirection in the custom-login success page.

- If the redirection URL feature is enabled, a configured auth-proxy-banner is not used

- To remove the specification of a redirection URL, use the `no` form of the command.

- If the redirection URL is required after the web-based authentication client is successfully authenticated, then the URL string must start with a valid URL (for example, `http://`) followed by the URL information. If only the URL is given without `http://`, then the redirection URL on successful authentication might cause page not found or similar errors on a web browser.

Related Topics

Specifying a Redirection URL for Successful Login, on page 1102
Custom Web Authentication Guidelines

• You cannot specify a directory path of a file when downloading a tar bundle from the controller GUI. The tar file is stored in the default flash path.

• You can provide any image name for web authentication and the image name need not be webauth.

Web-based Authentication Interactions with Other Features

Port Security

You can configure web-based authentication and port security on the same port. Web-based authentication authenticates the port, and port security manages network access for all MAC addresses, including that of the client. You can then limit the number or group of clients that can access the network through the port.

Related Topics
   Enabling and Configuring Port Security

LAN Port IP

You can configure LAN port IP (LPIP) and Layer 2 web-based authentication on the same port. The host is authenticated by using web-based authentication first, followed by LPIP posture validation. The LPIP host policy overrides the web-based authentication host policy.

If the web-based authentication idle timer expires, the NAC policy is removed. The host is authenticated, and posture is validated again.

Gateway IP

You cannot configure Gateway IP (GWIP) on a Layer 3 VLAN interface if web-based authentication is configured on any of the switch ports in the VLAN.

You can configure web-based authentication on the same Layer 3 interface as Gateway IP. The host policies for both features are applied in software. The GWIP policy overrides the web-based authentication host policy.

ACLs

If you configure a VLAN ACL or a Cisco IOS ACL on an interface, the ACL is applied to the host traffic only after the web-based authentication host policy is applied.

For Layer 2 web-based authentication, it is more secure, though not required, to configure a port ACL (PACL) as the default access policy for ingress traffic from hosts connected to the port. After authentication, the web-based authentication host policy overrides the PACL. The Policy ACL is applied to the session even if there is no ACL configured on the port.

You cannot configure a MAC ACL and web-based authentication on the same interface.

You cannot configure web-based authentication on a port whose access VLAN is configured for VACL capture.

Context-Based Access Control

Web-based authentication cannot be configured on a Layer 2 port if context-based access control (CBAC) is configured on the Layer 3 VLAN interface of the port VLAN.
You can configure web-based authentication on a Layer 2 EtherChannel interface. The web-based authentication configuration applies to all member channels.

### How to Configure Web-Based Authentication

#### Default Web-Based Authentication Configuration

The following table shows the default web-based authentication configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Disabled</td>
</tr>
<tr>
<td>RADIUS server</td>
<td></td>
</tr>
<tr>
<td>• IP address</td>
<td>• None specified</td>
</tr>
<tr>
<td>• UDP authentication port</td>
<td>• 1645</td>
</tr>
<tr>
<td>• Key</td>
<td>• None specified</td>
</tr>
<tr>
<td>Default value of inactivity timeout</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>Inactivity timeout</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

#### Web-Based Authentication Configuration Guidelines and Restrictions

- Web-based authentication is an ingress-only feature.
- You can configure web-based authentication only on access ports. Web-based authentication is not supported on trunk ports, EtherChannel member ports, or dynamic trunk ports.
- External web authentication, where the switch redirects a client to a particular host or web server for displaying login message, is not supported.
- You cannot authenticate hosts on Layer 2 interfaces with static ARP cache assignment. These hosts are not detected by the web-based authentication feature because they do not send ARP messages.
- By default, the IP device tracking feature is disabled on a switch. You must enable the IP device tracking feature to use web-based authentication.
- You must configure at least one IP address to run the switch HTTP server. You must also configure routes to reach each host IP address. The HTTP server sends the HTTP login page to the host.
- Hosts that are more than one hop away might experience traffic disruption if an STP topology change results in the host traffic arriving on a different port. This occurs because the ARP and DHCP updates might not be sent after a Layer 2 (STP) topology change.
• Web-based authentication does not support VLAN assignment as a downloadable-host policy.

• Web-based authentication supports IPv6 in Session-aware policy mode. IPv6 Web-authentication requires at least one IPv6 address configured on the switch and IPv6 Snooping configured on the switchport.

• Web-based authentication and Network Edge Access Topology (NEAT) are mutually exclusive. You cannot use web-based authentication when NEAT is enabled on an interface, and you cannot use NEAT when web-based authentication is running on an interface.

• Web-based authentication NRH (Non-Responsive Host) is not supported for voice devices.

• Only the Password Authentication Protocol (PAP) is supported for web-based RADIUS authentication on controllers. The Challenge Handshake Authentication Protocol (CHAP) is not supported for web-based RADIUS authentication on controllers.

• Identify the following RADIUS security server settings that will be used while configuring switch-to-RADIUS-server communication:
  • Host name
  • Host IP address
  • Host name and specific UDP port numbers
  • IP address and specific UDP port numbers

The combination of the IP address and UDP port number creates a unique identifier, that enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service (for example, authentication) the second host entry that is configured functions as the failover backup to the first one. The RADIUS host entries are chosen in the order that they were configured.

• When you configure the RADIUS server parameters:
  • Specify the `key string` on a separate command line.

    For `key string`, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.

  • When you specify the `key string`, use spaces within and at the end of the key. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon.

  • You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using with the `radius-server host` global configuration command. If you want to configure these options on a per-server basis, use the `radius-server timeout`, radius-server transmit, and the radius-server key global configuration commands. For more information, see the `Cisco IOS Security Configuration Guide`, Release 12.4 and the `Cisco IOS Security Command Reference`, Release 12.4.

---

**Note**

You need to configure some settings on the RADIUS server, including: the switch IP address, the key string to be shared by both the server and the switch, and the downloadable ACL (DACL). For more information, see the RADIUS server documentation.
When you upgrade from IOS XE release 3.6.x and 3.7.x, ensure that you use `radius-server attribute wireless accounting call-station-id macaddress` command to configure mac-address. This is because the accounting default call-station-id is changed from mac-address to IP address from Cisco IOS XE Denali 16.3.x onwards.

## Web-Based Authentication Configuration Task List

### Configuring the Authentication Rule and Interfaces

Examples in this section are legacy-style configurations. For new-style configurations, see the *Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Follow these steps to configure the authentication rule and interfaces:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable`          | Enables privileged EXEC mode.  
  * Example:  
  
  `Switch> enable` |
| **Step 2** | `configure terminal` | Enters global configuration mode.  
  * Example:  
  
  `Switch# configure terminal` |
| **Step 3** | `ip admission name name proxy http` | Configures an authentication rule for web-based authorization.  
  * Example:  
  
  `Switch(config)# ip admission name webauth1 proxy http` |
| **Step 4** | `interface type slot/port` | Enters interface configuration mode and specifies the ingress Layer 2 or Layer 3 interface to be enabled for web-based authentication.  
  * Example:  
  
  `Switch(config)# interface gigabitethernet 1/0/1` |
| **Step 5** | `ip access-group name` | Applies the default ACL.  
  * Example:  
  
  `Switch(config-if)# ip access-group webauthag` |
### Configuring AAA Authentication

If a method-list is configured under VTY lines, the corresponding method list must be added to the AAA configuration:

```
line vty 0 4
  authorization commands 15 abc
  aaa authorization commands 15 abc group tacacs+
```

If a method-list is not configured under VTY lines, you must add the default method list to the AAA configuration:

---

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip admission name</td>
<td>Configures an authentication rule for web-based authorization for the interface.</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip admission name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Returns to configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# exit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip device tracking</td>
<td>Enables the IP device tracking table.</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip device tracking</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip admission status</td>
<td>Displays the configuration.</td>
<td></td>
</tr>
<tr>
<td>Switch# show ip admission status</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Follow these steps to configure AAA authentication:

Use default list for AAA authorization, if you are planning to use features such as dACL.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa new-model</td>
<td>Enables AAA functionality.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>aaa authentication login default group {tacacs+</td>
<td>radius}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>named_authentication_list refers to any name that is not greater than 31 characters.</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# aaa authentication login default group tacacs+</td>
<td>AAA_group_name refers to the server group name. You need to define the server-group server_name at the beginning itself.</td>
</tr>
<tr>
<td>Step 5</td>
<td>aaa authorization auth-proxy default group {tacacs+</td>
<td>radius}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# aaa authorization auth-proxy default group tacacs+</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>tacacs server server-name</td>
<td>Specifies an AAA server.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# tacacs server yourserver</code></td>
<td>Configures the IP address for the TACACS server.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 7**

`address {ipv4 | ipv6} ip address`

**Example:**

`Switch(config-server-tacacs)# address ipv4 10.0.1.12`

**Step 8**

`key string`

**Example:**

`Switch(config-server-tacacs)# key cisco123`

**Step 9**

`exit`

**Example:**

`Switch(config-server-tacacs)# exit`

**Step 10**

`end`

**Example:**

`Switch(config)# end`

**Step 11**

`show running-config`

**Example:**

`Switch# show running-config`

**Step 12**

`copy running-config startup-config`

**Example:**

`Switch# copy running-config startup-config`

---

**Configuring Switch-to-RADIUS-Server Communication**

Follow these steps to configure the RADIUS server parameters:
### Configuring Switch-to-RADIUS-Server Communication

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ip radius source-interface vlan vlan interface number</td>
<td>Specifies that the RADIUS packets have the IP address of the indicated interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ip radius source-interface vlan 80</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>radius server server name</td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# radius server rsim address ipv4 124.2.2.12</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>address {ipv4</td>
<td>ipv6} ip address</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-radius-server)# address ipv4 10.0.1.2 auth-port 1550 acct-port 1560</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>key string</td>
<td>(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-radius-server)# key rad123</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>exit</td>
<td>Exits the RADIUS server mode and enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-radius-server)# exit</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the HTTP Server

To use web-based authentication, you must enable the HTTP server within the Switch. You can enable the server for either HTTP or HTTPS.

**Note**

The Apple pseudo-browser will not open if you configure only the `ip http secure-server` command. You should also configure the `ip http server` command.

Follow these steps to enable the server for either HTTP or HTTPS:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip http server</td>
<td>Enables the HTTP server. The web-based authentication feature uses the HTTP server to communicate with the hosts for user authentication.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip http server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip http secure-server</td>
<td>Enables HTTPS.</td>
</tr>
</tbody>
</table>
### Customizing the Authentication Proxy Web Pages

You can configure web authentication to display four substitute HTML pages to the user in place of the Switch default HTML pages during web-based authentication.

For the equivalent Session Aware Networking configuration example for this feature, see the section "Configuring a Parameter Map for Web-Based Authentication" in the chapter, "Configuring Identity Control Policies." of the book, "Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)."

Follow these steps to specify the use of your custom authentication proxy web pages:

**Before you begin**

Store your custom HTML files on the Switch flash memory.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip admission proxy http login page file device:login-filename</td>
<td>Specifies the location in the Switch memory file system of the custom HTML file to use in</td>
</tr>
</tbody>
</table>
### Specifying a Redirection URL for Successful Login

Follow these steps to specify a URL to which the user is redirected after authentication, effectively replacing the internal Success HTML page:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

---

**Related Topics**

- [Authentication Proxy Web Page Guidelines](#), on page 1091
## Configuring the Web-Based Authentication Parameters

Follow these steps to configure the maximum number of failed login attempts before the client is placed in a watch list for a waiting period:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- [Redirection URL for Successful Login Guidelines](#), on page 1091
## Configuring a Web-Based Authentication Local Banner

Follow these steps to configure a local banner on a switch that has web authentication configured.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable            | Enables privileged EXEC mode.  
  * Example: |  
  * Switch> enable |
| 2    | configure terminal | Enters global configuration mode.  
  * Example: |  
  * Switch# configure terminal |
| 3    | ip admission auth-proxy-banner http [banner-text | Enables the local banner.  
  * Example: |  
  * Switch# ip admission auth-proxy-banner http [banner-text | file-path] |
### Configuring Web-Based Authentication without SVI

You configure the web-based authentication without SVI feature to redirect the HTML login page to the client without creating an IP address in the routing table. These steps are optional.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> parameter-map type weauth global</td>
<td>Creates a parameter map and enters parameter-map weauth configuration mode. The specific configuration commands supported</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Purpose

Command or Action | Purpose
---|---
Switch (config)# parameter-map type webauth global | for a global parameter map defined with the global keyword differ from the commands supported for a named parameter map defined with the parameter-map-name argument.

Step 4 | l2-webauth-enabled

Example:
Switch (config-params-parameter-map)# l2-webauth-enabled

Enables the web-based authentication without SVI feature.

Step 5 | end

Example:
Switch(config)# end

Returns to privileged EXEC mode.

Step 6 | show running-config

Example:
Switch# show running-config

Verifies your entries.

Step 7 | copy running-config startup-config

Example:
Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.

Configuring Web-Based Authentication with VRF Aware

You configure the web-based authentication with VRF aware to redirect the HTML login page to the client. These steps are optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable

Example:
Switch> enable

Enables privileged EXEC mode.

• Enter your password if prompted.

| Step 2 | configure terminal

Example:
Switch# configure terminal

Enters global configuration mode.
Removing Web-Based Authentication Cache Entries

Follow these steps to remove web-based authentication cache entries:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> clear ip auth-proxy cache { *</td>
<td>host ip address }</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose
Command or Action | Purpose
--- | ---
Switch# clear ip auth-proxy cache 192.168.4.5 | specific IP address to delete the entry for a single host.

### Step 3
Command or Action | Purpose
--- | ---
clear ip admission cache {# | host ip address} | Delete authentication proxy entries. Use an asterisk to delete all cache entries. Enter a specific IP address to delete the entry for a single host.

**Example:**
Switch# clear ip admission cache 192.168.4.5

---

## Downloading Web Authentication Tar Bundle (CLI)

You can download a tar bundle (.tar) containing all personalized files from the FTP or TFTP server.

### Procedure

### Command or Action | Purpose
--- | ---
Step 1 | Specifies to download a tar bundle (.tar) from the FTP or TFTP server.
archive tar /xtract <transfer mode> ://<IP> /<location>/<login filename> < DIRECTORY>

**Example:**
Switch# archive tar /xtract tftp://9.1.0.100/user1/login.tar flash2
Switch# show flash:
59 4096 Jan 08 2014 13:19:33.0000000000 +00:00 flash 60 2574 Jan 08 2014 13:19:51.0000000000 +00:00 flash2/aup.html 61 4092 Jan 08 2014 13:19:51.0000000000 +00:00 flash2/login.html 62 70123 Jan 08 2014 13:19:52.0000000000 +00:00 flash2/yourlogo.jpg 63 344 Jan 08 2014 13:19:51.0000000000 +00:00 flash2/failed.html 64 1653 Jan 08 2014 13:19:52.0000000000 +00:00 flash2/logout.html 64 1653 Jan 08 2014 13:19:52.0000000000 +00:00 flash2/expired.html

**Step 2**
archive tar /xtract <transfer mode> ://<IP> /<location>/<login filename> < DIRECTORY> flash-1:

**Example:**
Switch# archive tar /xtract tftp://9.1.0.100/user1/login.tar flash-1:
### Downloading Web Authentication Tar Bundle (GUI)

**Procedure**

**Step 1** Choose **Configuration > Commands > Download File** to open the Download File to Controller page.

**Step 2** From the **File Type** drop-down list, choose Webauth Bundle.

**Step 3** From the **Transfer Mode** drop-down list, choose from the following options:

- TFTP
- FTP

**Step 4** In the **IP Address** text box, enter the IP address of the server.

**Step 5** In the **File Path** text box, enter the directory path of the software.

**Step 6** In the **File Name** text box, enter the name of the controller software file (*filename.aes*).

### Integrating Customized Web Authentication Pages into a Parameter Map (CLI)

You can configure the personalized pages into a parameter map. Using the parameter map, you can configure all the personalized pages in one shot. This minimizes the need of configuring all the four custom pages separately. Even if you want to configure only some pages, the others pages use the defaults.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>2</td>
<td><code>parameter-map type webauth name type webauth</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# parameter-map type webauth WEB type webauth</code></td>
</tr>
<tr>
<td>3</td>
<td><code>custom-page login device flash:flash2/login.html</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-params-parameter-map)# custom-page login device flash:flash2/login.html</code></td>
</tr>
<tr>
<td>4</td>
<td><code>custom-page success device flash: flash2/logout.html</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-params-parameter-map)# custom-page success device flash: flash2/logout.html</code></td>
</tr>
<tr>
<td>5</td>
<td><code>custom-page failure device flash: flash2/failed.html</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-params-parameter-map)# custom-page failure device flash: flash2/failed.html</code></td>
</tr>
<tr>
<td>6</td>
<td><code>custom-page login expired device flash: flash2/expired.html</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-params-parameter-map)# custom-page login expired device flash: flash2/expired.html</code></td>
</tr>
<tr>
<td>7</td>
<td><code>end</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# end</code></td>
</tr>
<tr>
<td>8</td>
<td><code>show parameter-map type webauth name name</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch# show parameter-map type webauth name WEB</code></td>
</tr>
<tr>
<td></td>
<td>Parameter Map Name : WEB Type : webuah Custom Page: Auth-proxy login : flash: flash2/login.html</td>
</tr>
</tbody>
</table>
## Linking Image in Custom Pages

In custom pages, you can also send back images.

In releases earlier to software release 3E, the custom page had to contain the link to the image as an entire path, in the form of: `<img src="http://<ip-address>/flash:web_auth_image.jpg" alt="name">`. The IP address is the management IP address of the controller.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Specifies to link image to the custom page. The virtual IP address is automatically used as a source. The logical link implies that you define the virtual IP address in the global parameter map.</td>
</tr>
<tr>
<td><code>&lt;img src=&quot;/flash:web_auth_image.jpg&quot; alt=&quot;name&quot;&gt;</code></td>
<td>Example:</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies to link image to the custom page. The virtual IP address is automatically used as a source. The logical link implies that you define the virtual IP address in the global parameter map.</td>
</tr>
<tr>
<td><code>&lt;img src=&quot;/flash:web_auth_image.jpg&quot; alt=&quot;name&quot;&gt;</code></td>
<td>Example:</td>
</tr>
<tr>
<td>Switch# `show run</td>
<td>sec parameter-map parameter-map type webauth global virtual-ip ipv4 192.0.2.1` Sample Webauth_login HTML</td>
</tr>
</tbody>
</table>

---

### Table

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth-proxy Init State time</td>
<td>120 sec</td>
</tr>
<tr>
<td>Auth-proxy Fin Wait time</td>
<td>3000 milliseconds</td>
</tr>
<tr>
<td>Webauth max-http connection</td>
<td>30</td>
</tr>
<tr>
<td>Webauth logout-window</td>
<td>Enabled</td>
</tr>
<tr>
<td>Consent Email</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Sample Web Authentication Login HTML

You can use the sample web authentication login page (webauth_login). If you want to modify or customize the sample page, you need to involve a developer who knows HTML, which is not covered by the Cisco Technical Assistance Center.

<HTML><HEAD>
<TITLE>Authentication Proxy Login Page</TITLE>
<script type="text/javascript">
var pxypromptwindow1;
var pxysubmitted = false;
function submitreload() {
    if (pxysubmitted == false) {
        pxypromptwindow1=window.open('', 'pxywindow1', 'resizable=no,width=350,
        height=350,scrollbars=yes');
        pxysubmitted = true;
        return true;
    } else {
        alert("This page can not be submitted twice.");
        return false;
    }
}
</script>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<style type="text/css">
body {background-color: #ffffff;}
</style>
</HEAD>
<BODY>
<H1><img src="http://192.168.2.91/flash:web_auth_logo.png" width="75" height="50"
alt="Cisco Logo" longdesc="http://www.cisco.com"></H1>
<center>
<H2>Wireless Guest Access Web Authentication</H2>
<center>
<iframe src="http://192.168.2.91/flash:web_auth_aup.html" width="950" height="250"
scrolling="auto"></iframe><BR><BR>
<FORM method=post action="/" target="pxywindow1">
    Username: <input type=text name=uname><BR><BR>
    Password: <input type=password name=pwd><BR><BR>
    <input type=submit name=ok value=OK onClick="return submitreload();">
</FORM><noscript>
    <BR>
    <H2><FONT COLOR="red">Warning!</FONT></H2>
    <p>JavaScript should be enabled in your Web browser
    for secure authentication</p>
    <LI>Follow the instructions of your Web browser to enable
    JavaScript if you would like to have JavaScript enabled
    for secure authentication</LI>
    <BR><BR><LI>Follow these steps if you want to keep JavaScript
    disabled or if your browser does not support JavaScript
    <OL><BR>
    <LI>Close this Web browser window</LI>
    <LI>Click on Reload button of the original browser window</LI>
    </OL></LI>
    </UL>
    </noscript>
</center>
</BODY></HTML>
Configuring a Parameter Map for Local Web Authentication (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>parameter-map type webauth global</td>
<td>Creates a parameter map and enters parameter-map webauth configuration mode. The specific configuration commands supported for a global parameter map defined with the global keyword differ from the commands supported for a named parameter map defined with the parameter-map-name argument.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# parameter-map type webauth global</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>virtual-ip ipv4 ip-address [virtual-host fqdn]</td>
<td>Configures the virtual IP address and redirects users to a virtual host. Optionally, you can also configure a fully qualified domain name (FQDN) for the virtual IP, along with the DNS services.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1 virtual-host host.cisco.com</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>banner {file</td>
<td>text}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-params-parameter-map)# banner</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>custom-page</td>
<td>Specifies the custom page such as login, expired, success, or failure page.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-params-parameter-map)# custom-page</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>max-http-conns</td>
<td>Specifies the maximum number of HTTP connections per clients.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-params-parameter-map)# max-http-conns</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>intercept-https-enable</td>
<td>Specifies to enable intercept of HTTPS traffic.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-params-parameter-map)# intercept-https-enable</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>8</td>
<td>ratelimit</td>
<td>Specifies to rate limit on the number of web authentication sessions.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-params-parameter-map)# ratelimit</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>redirect</td>
<td>Specifies to redirect the URL.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-params-parameter-map)# redirect</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>timeout</td>
<td>Specifies to timeout for the initial state of web authentication.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-params-parameter-map)# timeout</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>watch-list</td>
<td>Specifies the watch list of web authentication clients.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-params-parameter-map)# watch-list</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>virtual-ip ipv4 virtual -IP-address</td>
<td>(Optional) Specifies a virtual IP address for web-based authentication clients. This command is supported in the global parameter map only.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-params-parameter-map)# virtual-ip ipv4 172.16.16.16</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>exit</td>
<td>Specifies to exit from parameter-map params configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-params-parameter-map)# exit</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>no</td>
<td>Specifies to negate a command or set its defaults.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-params-parameter-map)# no</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>parameter-map type webauth name type webauth test</td>
<td>Specifies parameter map user-defined name for local web-based authentication clients. This command is supported in the global parameter map only.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# parameter-map type webauth user1 type webauth test</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>banner banner-text</td>
<td>(Optional) Displays a banner on the local web-authentication login web page.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-params-parameter-map)# banner</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>17</td>
<td>consent email</td>
<td>(Optional) Requests a user’s e-mail address on the local web-authentication login web page. This command is supported in named parameter maps only.</td>
</tr>
<tr>
<td>18</td>
<td>custom-page</td>
<td>Specifies the custom page such as login, expired, success, or failure page.</td>
</tr>
<tr>
<td>19</td>
<td>max-http-conns</td>
<td>Specifies the maximum number of HTTP connections per clients.</td>
</tr>
<tr>
<td>20</td>
<td>redirect</td>
<td>Specifies to redirect the URL.</td>
</tr>
<tr>
<td>21</td>
<td>timeout</td>
<td>Specifies to timeout for the initial state of web authentication.</td>
</tr>
<tr>
<td>22</td>
<td>type</td>
<td>(Optional) Specifies the parameter type such as web authentication or consent, or both.</td>
</tr>
<tr>
<td>23</td>
<td>exit</td>
<td>Specifies to exit from parameter-map params configuration mode.</td>
</tr>
<tr>
<td>24</td>
<td>no</td>
<td>Specifies to negate a command or set its defaults.</td>
</tr>
</tbody>
</table>

### Monitoring Web-Based Authentication Status

Use the commands in this topic to display the web-based authentication settings for all interfaces or for specific ports.
Table 79: Privileged EXEC show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show authentication sessions method webauth</td>
<td>Displays the web-based authentication settings for all interfaces for fastethernet, gigabitethernet, or tengigabitethernet</td>
</tr>
<tr>
<td>show wireless client mac-address a.a.a detail</td>
<td>Displays the session specific wireless information and wireless states.</td>
</tr>
<tr>
<td>show authentication sessions interface type slot/port[details]</td>
<td>Displays the web-based authentication settings for the specified interface for fastethernet, gigabitethernet, or tengigabitethernet. In Session Aware Networking mode, use the show access-session interface command.</td>
</tr>
</tbody>
</table>

Feature Information for Web-Based Authentication

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature is introduced.</td>
</tr>
</tbody>
</table>
Configuring Cisco TrustSec

- Information about Cisco TrustSec, on page 1117
- Finding Feature Information, on page 1118
- Feature Information for Cisco TrustSec, on page 1118

Information about Cisco TrustSec

Cisco TrustSec provides security improvements to Cisco network devices based on the capability to strongly identify users, hosts, and network devices within a network. TrustSec provides topology-independent and scalable access controls by uniquely classifying data traffic for a particular role. TrustSec ensures data confidentiality and integrity by establishing trust among authenticated peers and encrypting links with those peers.

The key component of Cisco TrustSec is the Cisco Identity Services Engine (ISE). Cisco ISE can provision switches with TrustSec Identities and Security Group ACLs (SGACLs), though these may be configured manually on the switch.

MTU Guidelines

CTS tagged packets greater than 1518 bytes may get dropped on the Cisco vWLC controller. This is due to a restriction on the size of incoming packets on the UCS server, which is hosting vWLC instances. The UCS server have a default MTU of 1500 thereby allowing packets of 1518 bytes only. Here, the additional 18 bytes includes 4 bytes of 802.1Q and 14 bytes of Ethernet header.

An Ethernet link configured for CTS tagging imposes a 8-byte encapsulation called Cisco metadata. As a result, the total size of the Ethernet packet is increased by 8 bytes to 1526 bytes (1518+8 = 1526). Hence, the MTU of the receiving interface has to be increased by 8-bytes to accommodate the additional 8 bytes in the Ethernet.

While CTS interfaces on the routers and switches (for example, Cisco ASR 1000 Series Routers, Cisco 4000 Series Integrated Services Routers, Cisco Catalyst 3000 Series Switches, Cisco Catalyst 9000 Series Switches) auto-adjusts MTU to 1508 bytes to accommodate additional 8-byte. However, other devices like UCS servers requires manual update to increase the MTU to 1508. For information on how to configure jumbo MTU on UCS, see the following link:

Finding Feature Information

To configure Cisco Trustsec on the switch, see the Cisco TrustSec Switch Configuration Guide at the following URL:


Release notes for Cisco TrustSec General Availability releases are at the following URL:


For restrictions and limitations on Catalyst 3850 and 3650, see the notes available at the following URL:


Additional information about the Cisco TrustSec solution, including overviews, datasheets, features by platform matrix, and case studies, is available at the following URL:


Feature Information for Cisco TrustSec

Table 80: Feature Information for Cisco TrustSec

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDAC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SXPv1, SXPv2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SGT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SGACL Layer2 Enforcement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface to SGT and VLAN to SGT mapping.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subnet to SGT mapping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layer 3 Port Mapping (PM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layer 3 Identity Port Mapping (IPM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Group Name Download</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SXP Loop Detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy-based CoA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td></td>
<td>These features were introduced on the Catalyst 3850 and 3650 switches.</td>
</tr>
</tbody>
</table>
CHAPTER 57

Configuring Wireless Guest Access

- Finding Feature Information, on page 1119
- Prerequisites for Guest Access, on page 1119
- Restrictions for Guess Access, on page 1120
- Information about Wireless Guest Access, on page 1120
- Fast Secure Roaming, on page 1120
- How to Configure Guest Access, on page 1121
- Configuration Examples for Guest Access, on page 1136
- Additional References for Guest Access, on page 1142
- Feature History and Information for Guest Access, on page 1143

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Guest Access

- All mobility peers should be configured for hierarchical mobility architecture.
- For Guest Controller Mobility Anchor configuration on WLAN is must on Mobility Agent and Guest Controller.
- Guest Access can be a 3 box solution or 2 box solution. The mobility tunnel link status should be up between:
  - Mobility Agent, Mobility Controller and Guest Controller.
  or
  - Mobility Agent/Mobility Controller and Guest Controller
Restrictions for Guess Access

Guest Controller functionality is not supported on the Catalyst 3850 switch whereas Catalyst 3850 can act as mobility agent.

Information about Wireless Guest Access

Ideally, the implementation of a wireless guest network uses as much of an enterprise’s existing wireless and wired infrastructure as possible to avoid the cost and complexity of building a physical overlay network. Assuming this is the case, the following additional elements and functions are needed:

- A dedicated guest WLAN/SSID—Implemented throughout the campus wireless network wherever guest access is required. A guest WLAN is identified by a WLAN with mobility anchor (Guest Controller) configured.
- Guest traffic segregation—Requires implementing Layer 2 or Layer 3 techniques across the campus network to restrict where guests are allowed to go.
- Access control—Involves using imbedded access control functionality within the campus network or implementing an external platform to control guest access to the Internet from the enterprise network.
- Guest user credential management—A process by which a sponsor or lobby administrator can create temporary credentials in behalf of a guest. This function might be resident within an access control platform or it might be a component of AAA or some other management system.

Fast Secure Roaming

Fast secure roaming can be achieved by caching the Pairwise Master Key (PMK) information for Cisco Centralized Key Management (CCKM), and 802.11i clients. Cisco Centralized Key Management (CCKM) helps to improve roaming. Only the client can initiate the roaming process, which depends on factors such as:

- Overlap between APs
- Distance between APs
- Channel, signal strength, and load on the AP
- Data rates and output power

Whenever a fast-roaming client 802.11i, [CCKM]) roams to a new device, after fast-roaming the clients go through mobility "handoff" procedure. And new AAA attributes learned through mobility "handoff" procedure get re-applied.

Full L2 authentication must be avoided during roaming if the client uses the 802.11i WPA2, CCKM, to achieve the full requirements of fast secure roaming. The PMK cache (802.11i, CCKM) is used to authenticate and derive the keys for roaming clients to avoid full L2 authentication. This requires all Mobility Anchors (MA) and Mobility Controllers (MC) in the mobility group to have the same PMK cache values.

The session timeout defines when a PMK cache will expire. A PMK cache can also be deleted when a client fails to re-authenticate or when it is manually deleted from the CLI. The deletion on the original controller or switch shall be propagated to other controllers or switches in the same mobility group.
# How to Configure Guest Access

## Creating a Lobby Administrator Account

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch # <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>user-name user-name</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch (config)# <code>user-name lobby</code></td>
<td>Creates a user account.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>type lobby-admin</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch (config-user-name)# <code>type lobby-admin</code></td>
<td>Specifies the account type as lobby admin.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>password 0 password</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch(config-user-name)# <code>password 0 lobby</code></td>
<td>Creates a password for the lobby administrator account.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch (config-user-name)# <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>`show running-config</td>
<td>section user-name<code>&lt;br&gt;</code>show running-config</td>
</tr>
</tbody>
</table>
# Configuring Guest User Accounts

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch # <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>user-name user-name</code></td>
<td>Creates a username for the lobby ambassador account.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config)# <code>user-name guest</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>password unencrypted/hidden-password password</code></td>
<td>Specifies the password for the user.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-user-name)# <code>password 0 guest</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>type network-user description description</code></td>
<td>Specifies the type of user.</td>
</tr>
<tr>
<td></td>
<td>guest-user lifetime year 0-1 month 0-11 day 0-30 hour 0-23 minute 0-59 second 0-59</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-user-name)# <code>type network-user description guest guest-user lifetime year 1 month 10 day 3 hour 1 minute 5 second 30</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-user-name)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>show aaa local netuser all</code></td>
<td>Displays the configuration details. After the lifetime, the user-name with guest type will be deleted and the client associated with the guest user-name will be de-authenticated.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch # <code>show aaa local netuser all</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>`show running-config</td>
<td>section user-name`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch # `show running-config</td>
<td>section guest`</td>
</tr>
</tbody>
</table>
# Configuring Mobility Agent (MA)

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch # configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wireless mobility controller ip mc-ipaddress public-ip mc-publicipaddress</code></td>
<td>Configures the Mobility Controller to which the MA will be associated.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch (config) # wireless mobility controller ip 27.0.0.1 public-ip 27.0.0.1</code></td>
<td></td>
</tr>
</tbody>
</table>
| Step 3 | `wlan wlan-name wlan-id ssid` | • For `wlan-name` enter, enter the profile name. The range is 1-32 characters.  
  • For `wlan-id`, enter the WLAN ID. The range is 1-512.  
  • For `ssid`, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. |
| **Example:** | `Switch (config) # wlan mywlan 34 mywlan-ssid` | |
| Step 4 | `client vlan id vlan-group name/vlan-id` | Configures the VLAN id or group of the WLAN. |
| **Example:** | `Switch (config-wlan) # client vlan VLAN0136` | |
| Step 5 | `no security wpa` | The security configuration must be the same for the WLAN created on the GC. This example is for open authentication. For other security types such as open and webauth, appropriate command should be provided. |
| **Example:** | `Switch (config-wlan) # no security wpa` | |
| Step 6 | `mobility anchor ipaddress` | Configures the Guest Controller as mobility anchor. |
| **Example:** | `Switch (config-wlan) # mobility anchor 9.3.32.2` | |
| Step 7 | `aaa-override` | (Optional) Enables AAA override. AAA override is required for non open |
**Configuring Mobility Controller**

Mobility Controller mode should be enabled using the `wireless mobility controller` command.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch (config) # configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless mobility group member ip ip-address</td>
<td>Adds all peers within the MC group. The <code>ip-address</code> should be the guest controller’s IP address.</td>
</tr>
<tr>
<td>public-ip ip-address group-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch (config) # wireless mobility group member ip</td>
<td></td>
</tr>
<tr>
<td>77.0.0.1 public-ip 23.0.0.1 group test</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> wireless mobility controller peer-group</td>
<td>Creates the switch peer group.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch # wireless mobility controller peer-group</td>
<td></td>
</tr>
<tr>
<td>mywlan</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Guest Controller

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller # <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wireless mobility group member ip ip-address public-ip ip-address group group-name</code></td>
<td>Configures the mobility group member with mobility controller's IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller (config) # <code>wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1 group test</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>wlan wlan-name wlan-id ssid</code></td>
<td>• For <code>wlan-name</code> enter, enter the profile name. The range is 1-32 characters. • For <code>wlan-id</code>, enter the WLAN ID. The range is 1-64.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller (config) # <code>wlan mywlan 34 mywlan-ssid</code></td>
<td></td>
</tr>
</tbody>
</table>

---

**Example**

**Example**

**Purpose**

**Command or Action**

<table>
<thead>
<tr>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch (config) # <code>wireless mobility controller peer-group pg</code></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>wireless mobility controller peer-group peer-group-name member ip ipaddress public-ip ipaddress</code></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config) # <code>wireless mobility controller peer-group pg member ip 9.7.136.10 public-ip 9.7.136.10</code></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config) # <code>end</code></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>show wireless mobility summary</code></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch # <code>show wireless mobility summary</code></td>
</tr>
<tr>
<td>Command or Action</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td><strong>Step 4</strong> client vlan id &lt;vlan-group name/vlan-id&gt;</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-wlan) # client vlan VLAN0136</td>
</tr>
<tr>
<td><strong>Step 5</strong> no security wpa</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller (config-wlan) # no security wpa</td>
</tr>
<tr>
<td><strong>Step 6</strong> mobility anchor self-ipaddress</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller (config-wlan) # mobility anchor 9.3.32.2</td>
</tr>
<tr>
<td><strong>Step 7</strong> aaa-override</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller (config-wlan) # aaa-override</td>
</tr>
<tr>
<td><strong>Step 8</strong> security web-auth authentication-list &lt;authentication list name&gt;</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller (config-wlan) # security web-auth authentication-list test</td>
</tr>
<tr>
<td><strong>Step 9</strong> security web-auth parameter-map &lt;parameter-map name&gt;</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller (config-wlan) # security web-auth parameter-map webparalocal</td>
</tr>
<tr>
<td><strong>Step 10</strong> no shutdown</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller (config-wlan) # no shutdown</td>
</tr>
<tr>
<td><strong>Step 11</strong> end</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller (config-wlan) # end</td>
</tr>
</tbody>
</table>
### Obtaining a Web Authentication Certificate

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example</td>
<td>Switch # <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>crypto pki import trustpoint name pkcs12 tftp: passphrase</code></td>
<td>Imports certificate.</td>
</tr>
<tr>
<td>Example</td>
<td>Switch (config)# <code>crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example</td>
<td>Switch (config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show crypto pki trustpoints cert</code></td>
<td>Displays the configuration details.</td>
</tr>
<tr>
<td>Example</td>
<td>Switch # <code>show crypto pki trustpoints cert</code></td>
<td></td>
</tr>
</tbody>
</table>
### Displaying a Web Authentication Certificate

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show crypto ca certificate verb</td>
<td>Displays the current web authentication certificate details.</td>
</tr>
<tr>
<td>Example: Switch # show crypto ca certificate verb</td>
<td></td>
</tr>
</tbody>
</table>

### Choosing the Default Web Authentication Login Page

AAA override flag should be enabled on the WLAN for web authentication using local or remote AAA server.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch # configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> parameter-map type webauth</td>
<td>Configures the web-auth parameter-map.</td>
</tr>
<tr>
<td>parameter-map name</td>
<td></td>
</tr>
<tr>
<td>Example: Switch (config) # parameter-map type webauth test</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> wlan wlan-name</td>
<td>For the wlan-name, enter the profile name. The range is 1-32 characters.</td>
</tr>
<tr>
<td>Example: Switch (config) # wlan wlan10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> shutdown</td>
<td>Disables WLAN.</td>
</tr>
<tr>
<td>Example: Switch (config) # shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> security web-auth</td>
<td>Enables web-auth on WLAN.</td>
</tr>
<tr>
<td>Example: Controller (config-wlan) # security web-auth</td>
<td></td>
</tr>
</tbody>
</table>
Purpose  
Command or Action  
Step 6 security web-auth authentication-list  
authentication list name  
Example:  
Controller (config-wlan) # security web-auth authentication-list test  
Allows you to map the authentication list name with the web-auth WLAN.  
Step 7 security web-auth parameter-map  
parameter-map name  
Example:  
Switch (config) # security web-auth parameter-map test  
Allows you to map the parameter-map name with the web-auth WLAN.  
Step 8 no shutdown  
Example:  
Switch (config) # no shutdown  
Enables the WLAN.  
Step 9 end  
Example:  
Switch (config) # end  
Returns to privileged EXEC mode.  
Step 10 show running-config | section wlan-name  
Example:  
Switch# show running-config | section mywlan  
Displays the configuration details.  
Step 11 show running-config | section parameter-map type webauth  
parameter-map  
Example:  
Switch# show running-config | section parameter-map type webauth test  
Displays the configuration details.  

Example

Choosing a Customized Web Authentication Login Page from an External Web Server

AAA override flag should be enabled on the WLAN for web authentication using local or remote AAA server.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong> &lt;br&gt;Switch # configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> parameter-map type webauth global</td>
<td>Configures a global webauth type parameter.</td>
</tr>
<tr>
<td><strong>Example:</strong> &lt;br&gt;Switch (config) # parameter-map type webauth global</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> virtual-ip {ipv4</td>
<td>ipv6} ip-address</td>
</tr>
<tr>
<td><strong>Example:</strong> &lt;br&gt;Switch (config-params-parameter-map) # virtual-ip ipv4 1.1.1.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> parameter-map type webauth parameter-map name</td>
<td>Configures the webauth type parameter.</td>
</tr>
<tr>
<td><strong>Example:</strong> &lt;br&gt;Switch (config-params-parameter-map) # parameter-map type webauth test</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> type {authbypass</td>
<td>consent</td>
</tr>
<tr>
<td><strong>Example:</strong> &lt;br&gt;Switch (config-params-parameter-map) # type webauth</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> redirect [for-login</td>
<td>on-success</td>
</tr>
<tr>
<td><strong>Example:</strong> &lt;br&gt;Switch (config-params-parameter-map) # redirect for-login <a href="http://9.1.0.100/login.html">http://9.1.0.100/login.html</a></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> redirect portal {ipv4</td>
<td>ipv6} ip-address</td>
</tr>
<tr>
<td><strong>Example:</strong> &lt;br&gt;Switch (config-params-parameter-map) # redirect portal ipv4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> &lt;br&gt;Switch (config-params-parameter-map) # end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> show running-config</td>
<td>section parameter-map</td>
</tr>
<tr>
<td><strong>Example:</strong> &lt;br&gt;Switch # show running-config</td>
<td>section parameter-map</td>
</tr>
</tbody>
</table>
### Assigning Login, Login Failure, and Logout Pages per WLAN

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `configure terminal`  
**Example:**  
Switch # configure terminal | Enters global configuration mode. |
| Step 2 | `parameter-map type webauth`  
`parameter-map-name`  
**Example:**  
Switch (config) # parameter-map type  
wwebauth test | Configures the webauth type parameter. |
| Step 3 | `custom-page login device html-filename`  
**Example:**  
Switch (config-params-parameter-map)#  
custom-page login device  
device  
flash:login.html | Allows you to specify the filename for web authentication customized login page. |
| Step 4 | `custom-page login expired html-filename`  
**Example:**  
Switch (config-params-parameter-map)#  
custom-page login expired device  
flash:loginexpired.html | Allows you to specify the filename for web authentication customized login expiry page. |
| Step 5 | `custom-page failure device html-filename`  
**Example:**  
Switch (config-params-parameter-map)#  
custom-page failure device  
flash:loginfail.html | Allows you to specify the filename for web authentication customized login failure page. |
| Step 6 | `custom-page success device html-filename`  
**Example:**  
Switch (config-params-parameter-map)#  
custom-page success device  
flash:loginsuccess.html | Allows you to specify the filename for web authentication customized login success page. |
| Step 7 | `end`  
**Example:**  
Switch (config-params-parameter-map)#  
end | Returns to privileged EXEC mode. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong></td>
<td>Displays the configuration details.</td>
</tr>
<tr>
<td>`show running-config</td>
<td>section parameter-map type webauth parameter-map`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>`Switch (config) # show running-config</td>
</tr>
</tbody>
</table>

### Configuring AAA-Override

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch # configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>For <code>wlan-name</code>, enter the profile name. The range is 1-32 characters.</td>
</tr>
<tr>
<td><code>wlan wlan-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch (config) # wlan ramban</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables AAA override on the WLAN.</td>
</tr>
<tr>
<td><code>aaa-override</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch (config-wlan) # aaa-override</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch (config-wlan) # end</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Displays the configuration details.</td>
</tr>
<tr>
<td>`show running-config</td>
<td>section wlan-name`</td>
</tr>
</tbody>
</table>
## Configuring Client Load Balancing

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `configure terminal` | Enters global configuration mode.  
Example:  
`Switch # configure terminal` |
| Step 2 | `wlan wlan-name` | For `wlan-name`, enter the profile name.  
Example:  
`Switch (config)# wlan ramban` |
| Step 3 | `shutdown` | Disables WLAN.  
Example:  
`Switch (config-wlan)# shutdown` |
| Step 4 | `mobility anchor ip-address1` | Configures a guest controller as mobility anchor.  
Example:  
`Switch (config-wlan) # mobility anchor 9.7.136.15` |
| Step 5 | `mobility anchor ip-address2` | Configures a guest controller as mobility anchor.  
Example:  
`Switch (config-wlan) # mobility anchor 9.7.136.16` |
| Step 6 | `no shutdown wlan` | Enables the WLAN.  
Example:  
`Switch (config-wlan) # no shutdown wlan` |
| Step 7 | `end` | Returns to privileged EXEC mode.  
Example:  
`Switch (config-wlan) # end` |
| Step 8 | `show running-config | section wlan-name` | Displays the configuration details.  
Example:  
`Switch # show running-config | section ramban` |
### Configuring Preauthentication ACL

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>wlan wlan-name</td>
<td>For wlan-name, enter the profile name.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config)# wlan ramban</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>shutdown</td>
<td>Disables the WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-wlan)# shutdown</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>ip access-group web preauthrule</td>
<td>Configures ACL that has to be applied before authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-wlan)# ip access-group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>web preauthrule</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>no shutdown</td>
<td>Enables the WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config)# no shutdown</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-wlan)# end</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>show wlan name wlan-name</td>
<td>Displays the configuration details.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show wlan name ramban</td>
<td></td>
</tr>
</tbody>
</table>
Configuring IOS ACL Definition

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | configure terminal  
Example:  
Switch # configure terminal | Enters global configuration mode. |
| Step 2 | ip access-list extended access-list number  
Example:  
Switch (config) # ip access-list extended 102 | Configures extended IP access-list. |
| Step 3 | permit udp any eq port number any  
Example:  
Switch (config-ext-nacl) # permit udp any eq 8080 any | Configures destination host. |
| Step 4 | end  
Example:  
Switch (config-wlan) # end | Returns to privileged EXEC mode. |
| Step 5 | show access-lists ACL number  
Example:  
Switch # show access-lists 102 | Displays the configuration details. |

Example

Configuring Webpasssthrough

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | configure terminal  
Example:  
Switch # configure terminal | Enters global configuration mode. |
### Configuration Examples for Guest Access

#### Example: Creating a Lobby Ambassador Account

This example shows how to configure a lobby ambassador account.

```bash
Switch# configure terminal
Switch(config)# user-name lobby
Switch(config)# type lobby-admin
Switch(config)# password 0 lobby
Switch(config)# end
Switch# show running-config | section lobby
    user-name lobby
    creation-time 1351118727
    password 0 lobby
    type lobby-admin
```

#### Example: Obtaining Web Authentication Certificate

This example shows how to obtain web authentication certificate.

```bash
Switch# show running-config | section parameter-map
```

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>parameter-map type webauth parameter-map name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch (config) # parameter-map type webauth webparalocal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>type consent</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch (config-params-parameter-map) # type consent</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch (config-params-parameter-map) # end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch (config) # show running-config</td>
</tr>
</tbody>
</table>
Switch# configure terminal
Switch(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco
Switch(config)# end
Switch# show crypto pki trustpoints cert
Trustpoint cert:
  Subject Name:
    e=rkannajr@cisco.com
cn=sthaliya-lnx
ou=WNBU
c=Cisco
l=SanJose
st=California
c=US
  Serial Number (hex): 00
Certificate configured.
Switch# show crypto pki certificates cert
Certificate
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: General Purpose
Issuer:
  e=rkannajr@cisco.com
cn=sthaliya-lnx
ou=WNBU
c=Cisco
l=SanJose
st=California
c=US
Subject:
  Name: ldapserver
e=rkannajr@cisco.com
cn=ldapserver
ou=WNBU
c=Cisco
st=California
c=US
Validity Date:
  start date: 07:35:23 UTC Jan 31 2012
  end date: 07:35:23 UTC Jan 28 2022
Associated Trustpoints: cert ldap12
Storage: nvram:rkannajrscisc#4.cer

CA Certificate
Status: Available
Certificate Serial Number (hex): 00
Certificate Usage: General Purpose
Issuer:
  e=rkannajr@cisco.com
cn=sthaliya-lnx
ou=WNBU
c=Cisco
l=SanJose
st=California
c=US
Subject:
  e=rkannajr@cisco.com
cn=sthaliya-lnx
ou=WNBU
c=Cisco
l=SanJose
st=California
c=US
Validity Date:
Example: Displaying a Web Authentication Certificate

This example shows how to display a web authentication certificate.

Switch# show crypto ca certificate verb
Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 2A9636AC0000000858B
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA
o=Cisco Systems
Subject:
Name: WS-C3780-6DS-S-2037064C0E80
Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
cn=WS-C3780-6DS-S-2037064C0E80
serialNumber=PID:WS-C3780-6DS-S SN:FOC1534X12Q
CRL Distribution Points:
Validity Date:
start date: 15:43:22 UTC Aug 21 2011
end date: 15:53:22 UTC Aug 21 2021
Subject Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
X509v3 extensions:
X509v3 Key Usage: F0000000
  Digital Signature
  Non Repudiation
  Key Encipherment
  Data Encipherment
X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B047F76C
Authority Info Access:
Associated Trustpoints: CISCO_IDEVID_SUDI
Key Label: CISCO_IDEVID_SUDI

Example: Configuring Guest User Accounts

This example shows how to configure a guest user account.

Switch# configure terminal
Switch(config)# user-name guest
Switch(config-user-name)# password 0 guest
Switch(config-user-name)# type network-user description guest guest-user lifetime year 1 month 10 day 3 hour 1 minute 5 second 30
Switch(config-user-name)# end
Switch# show aaa local netuser all
Example: Configuring Mobility Controller

This example shows how to configure a mobility controller.

Switch# configure terminal
Switch(config)# wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1 group test
Switch(config)# wireless mobility controller peer-group pg
Switch(config)# wireless mobility controller peer-group pg member ip 9.7.136.10 public-ip 9.7.136.10
Switch(config)# end
Switch# show wireless mobility summary

Mobility Controller Summary:

Mobility Role : Mobility Controller
Mobility Protocol Port : 16666
Mobility Group Name : default
Mobility Oracle : Enabled
DTLS Mode : Enabled

Mobility Keepalive Interval : 10
Mobility Keepalive Count : 3
Mobility Control Message DSCP Value : 7
Mobility Domain Member Count : 3

Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

<table>
<thead>
<tr>
<th>IP</th>
<th>Public IP</th>
<th>Group Name</th>
<th>Multicast IP</th>
<th>Link Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9.9.2</td>
<td>-</td>
<td>default</td>
<td>0.0.0.0</td>
<td>UP : UP</td>
</tr>
<tr>
<td>12.12.11.11</td>
<td>12.13.12.12</td>
<td>rasagna-grp</td>
<td>DOWN : DOWN</td>
<td></td>
</tr>
<tr>
<td>27.0.0.1</td>
<td>23.0.0.1</td>
<td>test</td>
<td>DOWN : DOWN</td>
<td></td>
</tr>
</tbody>
</table>

Switch Peer Group Name : spgl
Switch Peer Group Member Count : 0
Bridge Domain ID : 0
Multicast IP Address : 0.0.0.0

Switch Peer Group Name : pg
Switch Peer Group Member Count : 1
Bridge Domain ID : 0
Multicast IP Address : 0.0.0.0

<table>
<thead>
<tr>
<th>IP</th>
<th>Public IP</th>
<th>Link Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.7.136.10</td>
<td>9.7.136.10</td>
<td>DOWN : DOWN</td>
</tr>
</tbody>
</table>

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
Example: Choosing the Default Web Authentication Login Page

This example shows how to choose a default web authentication login page.

Switch# configure terminal
Switch(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their CPL control-policy equivalents. As this conversion is irreversible and will disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
Switch(config)# wlan wlan50
Switch(config-wlan)# shutdown
Switch(config-wlan)# security web-auth authentication-list test
Switch(config-wlan)# security web-auth parameter-map test
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
Switch# show running-config | section wlan50
wlan wlan50 50 wlan50
security wpa akm cckm
security wpa wpa1
security wpa wpa1 ciphers aes
security wpa wpa1 ciphers tkip
security web-auth authentication-list test
security web-auth parameter-map test
session-timeout 1800
no shutdown

Switch# show running-config | section parameter-map type webauth test
parameter-map type webauth test
  type webauth

Example: Choosing a Customized Web Authentication Login Page from an IPv4 External Web Server

This example shows how to choose a customized web authentication login page from an IPv4 external web server.

Switch# configure terminal
Switch(config)# parameter-map type webauth global
Switch(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1
Switch(config-params-parameter-map)# parameter-map type webauth test
Switch(config-params-parameter-map)# type webauth
Switch(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
Switch(config-params-parameter-map)# redirect portal ipv4 9.1.0.100
Switch(config-params-parameter-map)# end
Switch# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
Example: Assigning Login, Login Failure, and Logout Pages per WLAN

This example shows how to assign login, login failure and logout pages per WLAN.

Switch# configure terminal
Switch(config)# parameter-map type webauth test
Switch(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
Switch(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html
Switch(config-params-parameter-map)# custom-page failure device flash:loginfail.html
Switch(config-params-parameter-map)# custom-page success device flash:loginsucess.html
Switch(config-params-parameter-map)# end
Switch# show running-config | section parameter-map type webauth test
parameter-map type webauth test
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
custom-page login device flash:loginsantosh.html
custom-page success device flash:loginsucess.html
custom-page failure device flash:loginfail.html
custom-page login expired device flash:loginexpire.html

Example: Configuring AAA-Override

This example shows how to configure aaa-override.

Switch# configure terminal
Switch(config)# wlan fff
Switch(config-wlan)# aaa-override
Switch(config-wlan)# end
Switch# show running-config | section fff
wlan fff 44 fff
aaa-override
shutdown

Example: Configuring Client Load Balancing

This example shows how to configure client load balancing.

Switch# configure terminal
Switch(config)# wlan fff
Switch(config-wlan)# shutdown
Switch(config-wlan)# mobility anchor 9.7.136.15
Switch(config-wlan)# mobility anchor 9.7.136.16
Switch(config-wlan)# no shutdown wlan
Switch(config-wlan)# end
Switch# show running-config | section fff
wlan fff 44 fff
aaa-override
shutdown

Example: Configuring Preauthentication ACL

This example shows how to configure preauthentication ACL.
Example: Configuring IOS ACL Definition

This example shows how to configure IOS ACL definition.

```
Switch# configure terminal
Switch(config)# ip access-list extended 102
Switch(config-ext-nacl)# permit udp any eq 8080 any
Switch(config-ext-nacl)# end
Switch# show access-lists 102
Extended IP access list 102
  10 permit udp any eq 8080 any
```

Example: Configuring Webpassthrough

This example shows how to configure webpassthrough.

```
Switch# configure terminal
Switch(config)# parameter-map type webauth webparalocal
Switch(config-params-parameter-map)# type consent
Switch(config-params-parameter-map)# end
Switch# show running-config | section parameter-map type webauth test
parameter-map type webauth test
  redirect for-login http://9.1.0.100/login.html
  redirect portal ipv4 9.1.0.100
```

Additional References for Guest Access

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility CLI commands</td>
<td>Mobility Command Reference, Cisco IOS XE 3SE (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Mobility configuration</td>
<td>Mobility Configuration Guide, Cisco IOS XE 3SE (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Security CLI commands</td>
<td>Security Command Reference, Cisco IOS Release 3SE (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>
## Related Topic

<table>
<thead>
<tr>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired guest access configuration and commands</td>
</tr>
</tbody>
</table>

## Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>-</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

## Feature History and Information for Guest Access

<table>
<thead>
<tr>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Managing Rogue Devices

• Finding Feature Information, on page 1145
• Information About Rogue Devices, on page 1145
• How to Configure Rogue Detection, on page 1151
• Monitoring Rogue Detection, on page 1154
• Examples: Rogue Detection Configuration, on page 1154
• Additional References for Rogue Detection, on page 1155
• Feature History and Information For Performing Rogue Detection Configuration, on page 1156

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Rogue Devices

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of Clear to Send (CTS) frames. This action mimics an access point, informing a particular client to transmit, and instructing all the other clients to wait, which results in legitimate clients being unable to access network resources. Wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad hoc wireless networks without their IT department's knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to
intercept network traffic and hijack client sessions. There is an increased chance of enterprise security breach when wireless users connect to access points in the enterprise network.

The following are some guidelines to manage rogue devices:

- The containment frames are sent immediately after the authorization and associations are detected. The enhanced containment algorithm provides more effective containment of ad hoc clients.

- In a dense RF environment, where maximum rogue access points are suspected, the chances of detecting rogue access points by a local mode access point in channel 157 or channel 161 is less when compared to other channels. To mitigate this problem, we recommend that you use dedicated monitor mode access points.

- The local mode access points are designed to serve associated clients. These access points spend relatively less time performing off-channel scanning: about 50 milliseconds on each channel. If you want to perform high rogue detection, a monitor mode access point must be used. Alternatively, you can reduce the scan intervals from 180 seconds to a lesser value, for example, 120 or 60 seconds, ensuring that the radio goes off-channel more frequently, which improves the chances of rogue detection. However, the access point will still spend about 50 milliseconds on each channel.

- Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

- Client card implementations might mitigate the effectiveness of ad hoc containment.

- It is possible to classify and report rogue access points through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states.

- Each controller limits the number of rogue containment to three per radio (or six per radio for access points in the monitor mode).

- Rogue Location Discovery Protocol (RLDP) detects rogue access points that are configured for open authentication.

- RLDP detects rogue access points that use a broadcast Basic Service Set Identifier (BSSID), that is, the access point broadcasts its Service Set Identifier in beacons.

- RLDP detects only those rogue access points that are on the same network. If an access list in the network prevents the sending of RLDP traffic from the rogue access point to the controller, RLDP does not work.

- RLDP does not work on 5-GHz Dynamic Frequency Selection (DFS) channels. However, RLDP works when the managed access point is in the monitor mode on a DFS channel.

- If RLDP is enabled on mesh APs, and the APs perform RLDP tasks, the mesh APs are dissociated from the controller. The workaround is to disable RLDP on mesh APs.

- If RLDP is enabled on non-monitor APs, client connectivity outages occur when RLDP is in process.

- If the rogue is manually contained, the rogue entry is retained even after the rogue expires.

- If the rogue is contained by any other means, such as auto, rule, and AwIPS preventions, the rogue entry is deleted when it expires.

- The controller will request to AAA server for rogue client validation only once. As a result, if rogue client validation fails on the first attempt then the rogue client will not be detected as a threat any more. To avoid this, add the valid client entries in the authentication server before enabling **Validate Rogue Clients Against AAA**.
• All the valid client MAC details should be registered in the AAA authentication server with the same MAC delimiter options as set in the RADIUS configuration on the controller. For more information about configuring MAC delimiter options, see the Configuring RADIUS (GUI) section.

• In the 7.4 and earlier releases, if a rogue that was already classified by a rule was not reclassified. In the 7.5 release, this behavior is enhanced to allow reclassification of rogues based on the priority of the rogue rule. The priority is determined by using the rogue report that is received by the controller.

• All rogues that are marked as friendly or contained state (due to auto or rule or manual) are stored in the flash memory of the controller. When you reboot the controller loaded with Release 7.4, these rogues are shown as manually changed. If you wish to reboot the controller, you need to clear all rogue APs and rogue adhoc from the controller, save the configuration, and then reboot the controller.

• All rogues that are marked as friendly or contained state (only due to manual) are stored in the flash memory of the controller. If you upgrade the controller from the Release 7.4 to 7.6 or later versions, then all rogues stored in the Release 7.4 are shown as manually classified (if friendly classified) or manually contained. Hence after upgrading the controller from the Release 7.4 to 7.6 or later versions, you need to delete all rogue APs and rogue adhoc from the controller and then start configuring rogue detection.

• A FlexConnect AP (with rogue detection enabled) in the connected mode takes the containment list from the controller. If auto-contain SSID and auto contain adhoc are set in the controller, then these configurations are set to all FlexConnect APs in the connected mode and the AP stores it in its memory.

When the FlexConnect AP moves to a standalone mode, the following tasks are performed:

• The containment set by the controller continues.

• If the FlexConnect AP detects any rogue AP that has same SSID as that of infra SSID (SSID configured in the controller that the FlexConnect AP is connected to), then containment gets started if auto contain SSID was enabled from the controller before moving to the standalone mode.

• If the FlexConnect AP detects any adhoc rogue, containment gets started if auto-contain adhoc was enabled from the controller when it was in the connected mode.

When the standalone FlexConnect AP moves back to the connected mode, then the following tasks are performed:

• All containment gets cleared.

• Containment initiated from the controller will take over.

• The rogue detector AP fails to co-relate and contain the wired rogue AP on a 5Mhz channel because the MAC address of the rogue AP for WLAN, LAN, 11a radio and 11bg radio are configured with a difference of +/-1 of the rogue BSSID. In the 8.0 release, this behavior is enhanced by increasing the range of MAC address, that the rogue detector AP co-relates the wired ARP MAC and rogue BSSID, by +/-3.

• The rogue access points with open authentication can be detected on wire. The NAT wired or rogue wired detection is not supported in by WLC (both RLDP and rogue detector AP). The non-adjacent MAC address is supported by rogue detector mode of AP and not by RLDP.

• In a High Availability scenario, if the rogue detection security level is set to either High or Critical, the rogue timer on the standby Cisco WLC starts only after the rogue detection pending stabilization time, which is 300 seconds. Therefore, the active configurations on the standby Cisco WLC are reflected only after 300 seconds.
After an AP is moved from rogue detection mode to any other mode or after an AP is moved from sniffer mode to local or monitor mode, the rogue detection functionality is not retained on the AP. To enable rogue detection functionality on the AP, you have to explicitly move the AP to the rogue detection mode.

A rogue AP or client or adhoc containment configuration is not saved after the reload. You have to configure all the rogues again after the reload.

No separate command exists for controlling rogue client traps. However, you can enable or disable rogue client traps using the `config trapflags rogueap {enable | disable} ` command, which is also used for rogue APs. In GUI configuration also, you should use the rogue AP flag under Management > SNMP > TrapControl > Security > Rogue AP to control rogue clients.

**Rogue Location Discovery Protocol**

Rogue Location Discovery Protocol (RLDP) is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends de-authentication messages to all connected clients and then shuts down the radio interface. Then, it associates to the rogue AP as a client. The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature.

RLDP has 100% accuracy in rogue AP detection. It detects Open APs and NAT APs.

Use the `debug dot11 rldp enable` command in order to check if the Lightweight AP associates and receives a DHCP address from the rogue AP. This command also displays the UDP packet sent by the Lightweight AP to the controller.

A sample of a UDP (destination port 6352) packet sent by the Lightweight AP is shown here: 0020 0a 01 01 0d 0a 01 ......(.*...... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 .......x........ 0040 00 00 00 00 00 00 00 00 00 00

The first 5 bytes of the data contain the DHCP address given to the local mode AP by the rogue AP. The next 5 bytes are the IP address of the controller, followed by 6 bytes that represent the rogue AP MAC address. Then, there are 18 bytes of zeroes.

The following steps describe the functioning of RLDP:

1. Identify the closest Unified AP to the rogue using signal strength values.
2. The AP then connects to the rogue as a WLAN client, attempting three associations before timing out.
3. If association is successful, the AP then uses DHCP to obtain an IP address.
4. If an IP address was obtained, the AP (acting as a WLAN client) sends a UDP packet to each of the controller's IP addresses.
5. If the controller receives even one of the RLDP packets from the client, that rogue is marked as on-wire.

The RLDP packets are unable to reach the controller if filtering rules are placed between the controller's network and the network where the rogue device is located.

Caveats of RLDP:

- RLDP only works with open rogue APs broadcasting their SSID with authentication and encryption disabled.
- RLDP requires that the Managed AP acting as a client is able to obtain an IP address via DHCP on the rogue network.
- Manual RLDP can be used to attempt an RLDP trace on a rogue multiple number of times.
- During RLDP process, the AP is unable to serve clients. This negatively impacts performance and connectivity for local mode APs. To avoid this case, RLDP can be selectively enabled for Monitor Mode AP only.
- RLDP does not attempt to connect to a rogue AP operating in a 5GHz DFS channel.

RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS). If the automatic RLDP attempt does not detect the rogue (due to a noisy RF environment, for example), the controller does not retry. However, you can initiate RLDP manually on a rogue device.

Detecting Rogue Devices

The controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) and the rogue detector mode access point is connected to determine if the rogue is attached to your network.

Controller initiates RLDP on rogue devices that have open authenticated and configured. If RLDP uses Flexconnect or local mode access points, then clients are disconnected for that moment. After the RLDP cycle, the clients are reconnected to the access points. As and when rogue access points are seen (auto-configuration), the RLDP process is initiated.

You can configure the controller to use RLDP on all the access points or only on the access points configured for the monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded radio frequency (RF) space, allowing monitoring without creating unnecessary interference and without affecting the regular data access point functionality. If you configure the controller to use RLDP on all the access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to contain the detected rogue either manually or automatically.

RLDP detects on wire presence of the rogue access points that are configured with open authentication only once, which is the default retry configuration. Retries can be configured using the `config rogue ap rldp retries` command.
You can initiate or trigger RLDP from controller in three ways:

1. Enter the RLDP initiation command manually from the controller CLI. The equivalent GUI option for initiating RLDP is not supported.
   
   `config rogue ap rldp initiate mac-address`

2. Schedule RLDP from the controller CLI. The equivalent GUI option for scheduling RLDP is not supported.
   
   `config rogue ap rldp schedule`

3. Auto RLDP. You can configure auto RLDP on controller either from controller CLI or GUI but keep in mind the following guidelines:
   
   • The auto RLDP option can be configured only when the rogue detection security level is set to custom.
   
   • Either auto RLDP or schedule of RLDP can be enabled at a time.

A rogue access point is moved to a contained state either automatically or manually. The controller selects the best available access point for containment and pushes the information to the access point. The access point stores the list of containments per radio. For auto containment, you can configure the controller to use only the monitor mode access point. The containment operation occurs in the following two ways:

   • The container access point goes through the list of containments periodically and sends unicast containment frames. For rogue access point containment, the frames are sent only if a rogue client is associated.

   • Whenever a contained rogue activity is detected, containment frames are transmitted.

Individual rogue containment involves sending a sequence of unicast disassociation and deauthentication frames.

**Cisco Prime Infrastructure Interaction and Rogue Detection**

Cisco Prime Infrastructure supports rule-based classification and uses the classification rules configured on the controller. The controller sends traps to Cisco Prime Infrastructure after the following events:

   • If an unknown access point moves to the Friendly state for the first time, the controller sends a trap to Cisco Prime Infrastructure only if the rogue state is Alert. It does not send a trap if the rogue state is Internal or External.

   • If a rogue entry is removed after the timeout expires, the controller sends a trap to Cisco Prime Infrastructure for rogue access points categorized as Malicious (Alert, Threat) or Unclassified (Alert). The controller does not remove rogue entries with the following rogue states: Contained, Contained Pending, Internal, and External.

**Validating Rogue Devices Using MSE**

You can validate the rogue clients by utilizing the resources available in the Cisco Mobility Services Engine (MSE). Using MSE, you can dynamically list the clients joining to the switch. The list of clients joined to the switch is stored in the MSE as a centralized location, where the switch communicates with MSE and validates the client before reporting if the rogue client is a valid one or not. MSE maintains the MAC addresses of clients joined to the switch for a period of 7 days and this time period is non-configurable. After enabling rouge validation on the switch, the NSMP communication is triggered. Only after this, the switch communicates with MSE. When MSE stops responding for 60 seconds or more, the MSE validation stops, and resumes with NSMP communication.
The communication between the switch and MSE is an on-demand service as the switch requests this service from MSE.

- NMSP request messages and response messages are exchanged between the switch and MSE as an on-demand service.
- The switch passes the MAC addresses of the detected rogue clients to MSE using the NMSP request message.
- MSE validates the rogue client and passes the response back to the switch using NMSP response message.
- Upon validating the response against the configuration settings, the switch performs either one of the following actions on the rogue client: contain, alarm, or ignore.

## How to Configure Rogue Detection

### Configuring Rogue Detection (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless wps rogue detection min-rssi $rssi$ in dBm</td>
<td>Specify the minimum RSSI value that rogues should have for APs to detect and for rogue entry to be created in the switch.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# wireless wps rogue detection min-rssi 100</td>
<td>Valid range for the rssi in dBm parameter is $-128$ dBm to $-70$ dBm, and the default value is $-128$ dBm.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
<td>This feature is applicable to all the AP modes. There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>wireless wps rogue detection min-transient-time $time$ in seconds</td>
<td>Specify the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| `Switch(config)# wireless wps rogue detection min-transient-time` | Valid range for the time in sec parameter is 120 seconds to 1800 seconds, and the default value is 0.  
**Note** This feature is applicable to APs that are in monitor mode only.  
Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter the rogues based on their transient interval values.  
This feature has the following advantages:  
- Rogue reports from APs to the controller are shorter  
- Transient rogue entries are avoided in the controller  
- Unnecessary memory allocation for transient rogues are avoided |

**Step 4**  
wireless wps rogue client {aaa | mse}  
**Example:**  
Switch(config)# wireless wps rogue client aaa  
Switch(config)# wireless wps rogue client mse  
Set the AAA server or local database, or the MSE to validate if rogue clients are valid clients.

**Step 5**  
wireless wps rogue ap valid-client auto-contain  
**Example:**  
Switch(config)# wireless wps rogue ap valid-client auto-contain  
Specify to automatically contain a rogue access point to which trusted clients are associated.

**Step 6**  
end  
**Example:**  
Switch(config)# end  
Returns to privileged EXEC mode. Alternatively, you can also press `Ctrl-Z` to exit global configuration mode.
# Configuring Rogue Detection (GUI)

## Procedure

### Step 1
Make sure that rogue detection is enabled on the corresponding access points. Rogue detection is enabled by default for all access points joined to the controller (except for OfficeExtend access points). However, you can enable or disable rogue detection for individual access point by choosing **Configuration > Wireless > Access Policies > All APs** to open Edit AP page, selecting or unselecting the **Rogue Detector** check box in the General area of the Edit AP page.

### Step 2

### Step 3
Choose one of the following options from the **Rogue Location Discovery Protocol** drop-down list:
- **Disable**—Disables RLDP on all the access points. This is the default value.
- **All APs**—Enables RLDP on all the access points.
- **Monitor Mode APs**—Enables RLDP only on the access points in the monitor mode.

### Step 4
In the **Expiration Timeout for Rogue AP and Rogue Client Entries** text box, enter the number of seconds after which the rogue access point and client entries expire and are removed from the list. The valid range is 240 to 3600 seconds, and the default value is 1200 seconds.

**Note** If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.

### Step 5
To use the AAA server or local database to validate if rogue clients are valid clients, select the **Validate Rogue Clients Against AAA** check box. By default, the check box is unselected.

### Step 6
If necessary, select the **Detect and Report Adhoc Networks** check box to enable adhoc rogue detection and reporting. By default, the check box is selected.

### Step 7
In the **Rogue Detection Report Interval** text box, enter the time interval, in seconds, at which APs should send the rogue detection report to the controller. The valid range is 10 seconds to 300 seconds, and the default value is 10 seconds.

### Step 8
If you want the controller to automatically contain certain rogue devices, enable the following parameters. By default, these parameters are in disabled state.

**Caution** When you select any of the Auto Contain parameters and click **Apply**, the following message is displayed: “Using this feature may have legal consequences. Do you want to continue?” The 2.4-GHz and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party’s network could have legal consequences.

- **Auto Containment Level**—Set the auto containment level. By default, the auto containment level is set to 1.
- **Auto Containment only for Monitor mode APs**—Configure the monitor mode access points for auto-containment.
- **Rogue on Wire**—Configure the auto containment of rogues that are detected on the wired network.
• **Using Our SSID**—Configure the auto containment of rogues that are advertising your network’s SSID. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.

• **Valid Client on Rogue AP**—Configure the auto containment of a rogue access point to which trusted clients are associated. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.

• **Adhoc Rogue AP**—Configure the auto containment of adhoc networks detected by the controller. If you leave this parameter unselected, the controller only generates an alarm when such a network is detected.

---

**Step 9**
Click **Apply**.

**Step 10**
Click **Save Configuration**.

---

### Monitoring Rogue Detection

This section describes the new command for rogue detection.

The following command can be used to monitor rogue detection on the switch.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless wps rogue ap summary</code></td>
<td>Displays a list of all rogue access points detected by the switch.</td>
</tr>
<tr>
<td><code>show wireless wps rogue client detailed client-mac</code></td>
<td>Displays detailed information for a specific rogue client.</td>
</tr>
<tr>
<td><code>show wireless wps rogue client summary</code></td>
<td>Displays a list of all rogue clients detected by the switch.</td>
</tr>
<tr>
<td><code>show nmsp capability</code></td>
<td>Displays the NMSP capabilities.</td>
</tr>
</tbody>
</table>

### Table 82: Monitoring Rogue Auto-Containment Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless wps rogue auto-contain</code></td>
<td>Displays the rogue auto-containment information.</td>
</tr>
</tbody>
</table>

### Examples: Rogue Detection Configuration

This example shows how to configure the minimum RSSI that a detected rogue AP needs to be at, to have an entry created at the switch:

```
Switch# configure terminal
Switch(config)# wireless wps rogue detection min-rssi -100
```
Switch(config)# end
Switch# show wireless wps rogue client detailed/show wireless wps rogue ap summary

This example shows how to configure the classification interval:

Switch# configure terminal
Switch(config)# wireless wps rogue detection min-transient-time 500
Switch(config)# end
Switch# show wireless wps rogue client detailed/show wireless wps rogue ap summary

This example shows how to configure the MSE to validate if rogue clients are valid clients:

Switch# configure terminal
Switch(config)# wireless wps rogue client mse
Switch(config)# end
Switch# show wireless wps rogue client summary

This example shows how to automatically contain a rogue access point to which trusted clients are associated:

Switch# configure terminal
Switch(config)# wireless wps rogue ap valid-client auto-contain
Switch(config)# end
Switch# show wireless wps rogue ap summary
Switch# show nmsp capability

### Additional References for Rogue Detection

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>

#### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information For Performing Rogue Detection Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3E</td>
<td>Rogue validation against MSE.</td>
</tr>
</tbody>
</table>
Classifying Rogue Access Points

- Finding Feature Information, on page 1157
- Information About Classifying Rogue Access Points, on page 1157
- Restrictions on Classifying Rogue Access Points, on page 1160
- How to Classify Rogue Access Points, on page 1161
- Viewing and Classifying Rogue Devices (GUI), on page 1166
- Examples: Classifying Rogue Access Points, on page 1168
- Additional References for Classifying Rogue Access Points, on page 1168
- Feature History and Information For Classifying Rogue Access Points, on page 1169

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Classifying Rogue Access Points

The controller software enables you to create rules that can organize and display rogue access points as Friendly, Malicious, or Unclassified.

By default, none of the classification rules are used. You need to enable them. Therefore, all unknown access points are categorized as Unclassified. When you create or change a rule, configure conditions, and enable it, all rogue access points are then reclassified. Whenever you change a rule, it is applied to all the access points (friendly, malicious, and unclassified) in the Alert state only.

If you move any rogue or ad hoc rogue manually to unclassified and Alert state, it means that the rogue is moved to the default state. Rogue rules apply to all the rogues that are manually moved to unclassified and Alert state.
Rule-based rogue classification does not apply to ad hoc rogues and rogue clients.

You can configure up to 64 rogue classification rules per controller.

When the controller receives a rogue report from one of its managed access points, it responds as follows:

- If the unknown access point is in the friendly MAC address list, the controller classifies the access point as Friendly.

- If the unknown access point is not in the friendly MAC address list, the controller starts applying the rogue classification rules to the access point.

- If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.

- If the rogue access point matches the configured rules criteria, the controller classifies the rogue based on the classification type configured for that rule.

- If the rogue access point does not match any of the configured rules, the rogue remains unclassified.

The controller repeats the previous steps for all the rogue access points.

- If the rogue access point is detected on the same wired network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if there are no configured rules. You can then manually contain the rogue to change the rogue state to Contained. If the rogue access point is not available on the network, the controller marks the rogue state as Alert. You can then manually contain the rogue.

- If desired, you can manually move the access point to a different classification type and rogue state.

### Table 83: Classification Mapping

<table>
<thead>
<tr>
<th>Rule-Based Classification Type</th>
<th>Rogue State</th>
</tr>
</thead>
</table>
| Friendly                      | • Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you can manually configure it as Friendly, Internal. An example of this would be the access points in your lab network.  
• External—If the unknown access point is outside the network and poses no threat to WLAN security, you can manually configure it as Friendly, External. An example of this would be the access point in your neighboring coffee shop.  
• Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. |
## Rule-Based Classification Type

### Rogue State

**Malicious**
- **Alert**—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list.
- **Threat**—The unknown access point is found to be on the network and poses a threat to WLAN security.
- **Contained**—The unknown access point is contained.
- **Contained Pending**—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

**Unclassified**
- **Pending**—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point.
- **Alert**—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list.
- **Contained**—The unknown access point is contained.
- **Contained Pending**—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

The classification and state of the rogue access points are configured as follows:

- From Known to Friendly, Internal
- From Acknowledged to Friendly, External
- From Contained to Malicious, Contained

As mentioned earlier, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules. Alternatively, you can manually move the unknown access point to a different classification type and rogue state.

### Table 84: Allowable Classification Type and Rogue State Transitions

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly (Internal, External, Alert)</td>
<td>Malicious (Alert)</td>
</tr>
<tr>
<td>Friendly (Internal, External, Alert)</td>
<td>Unclassified (Alert)</td>
</tr>
<tr>
<td>Friendly (Alert)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Malicious (Alert, Threat)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Malicious (Contained, Contained Pending)</td>
<td>Malicious (Alert)</td>
</tr>
<tr>
<td>Unclassified (Alert, Threat)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Unclassified (Contained, Contained Pending)</td>
<td>Unclassified (Alert)</td>
</tr>
<tr>
<td>Unclassified (Alert)</td>
<td>Malicious (Alert)</td>
</tr>
</tbody>
</table>
Restrictions on Classifying Rogue Access Points

- Classifying Custom type rogues is tied to rogue rules. Therefore, it is not possible to manually classify a rogue as Custom. Custom class change can occur only when rogue rules are used.

- Some are sent for containment by rule and every 30 minutes for rogue classification change. For custom classification, the first trap does not contain the severity score because the trap has existed before the custom classification. The severity score is obtained from the subsequent trap that is generated after 30 minutes if the rogue is classified.

- Rogue rules are applied on every incoming new rogue report in the controller in the order of their priority.

- After a rogue satisfies a higher priority rule and is classified, it does not move down the priority list for the same report.

- Previously classified rogue gets re-classified on every new rogue report with the following restrictions:
  - Rogues which are classified as friendly by rule and whose state is set to ALERT, go through re-classification on receiving the new rogue report.
  - If a rogue is classified as friendly by the administrator manually, then the state is INTERNAL and it does not get re-classified on successive rogue reports.
  - If rogue is classified as malicious, irrespective of the state it does not get re-classified on subsequent rogue reports.

- Transition of the rogue's state from friendly to malicious is possible by multiple rogue rules if some attribute is missing in new rogue report.

- Transition of the rogue's state from malicious to any other classification is not possible by any rogue rule.

- The status change of a rogue device to contain or alert does not work when you move it between different class types until you move the class type of the rogue to unclassified.

- If a rogue AP is classified as friendly, it means that the rogue AP exists in the vicinity, is a known AP, and need not be tracked. Therefore, all the rogue clients are either deleted or not tracked if they are associated with the friendly rogue AP.

- When service set identifiers (SSIDs) are defined as part of a rogue rule, and details of the rogue rule are displayed using the `show wireless wps rogue rule detailed` command, the output differs in Cisco IOS XE Release 3.7E and prior releases and Cisco IOS XE Denali 16.1.1 and later releases.

The following is sample output from the `show wireless wps rogue rule detailed` command in Cisco IOS XE Release 3.6E and prior releases:

```
Switch# show wireless wps rogue rule detailed test

Priority : 1
Rule Name : wpstest
State : Disabled
Type : Pending
```

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.
The following is sample output from the `show wireless wps rogue rule detailed` command in Cisco IOS XE Denali 16.1.1 and later releases:

```
Switch# show wireless wps rogue rule detailed test
```

```
Priority : 1
Rule Name : wpstest
State : Disabled
Type : Pending
Match Operation : Any
Hit Count : 0
Total Conditions : 1
Condition :
  type : Ssid
  SSID Count : 2
  SSID 1 : ssid1
  SSID 2 : ssid2
```

How to Classify Rogue Access Points

Configuring Rogue Classification Rules (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless wps rogue rule rule-name priority</td>
<td>Creates or enables a rule. While creating a rule, you must enter the priority for the rule.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# wireless wps rogue rule rule_3 priority 3</td>
<td>Note: After creating a rule, you can edit the rule and change the priority only for the rogue rules that are disabled. You cannot change the priority for the rogue rules that are enabled. While editing, changing the priority for a rogue rule is optional.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>classify {friendly</td>
<td>malicious}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Configuring Rogue Classification Rules (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# wireless wps rogue rule rule_3 priority 3</td>
<td>day the following conditions to a rule, which</td>
</tr>
<tr>
<td>Switch(config-rule)# classify friendly</td>
<td>the rogue access point must meet:</td>
</tr>
<tr>
<td></td>
<td>• <strong>client-count</strong>—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, the access point could be classified as Malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point for the <code>condition_value</code> parameter. The valid range is from 1 to 10 (inclusive), and the default value is 0.</td>
</tr>
<tr>
<td>Step 4</td>
<td>• <strong>duration</strong>—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period for the <code>condition_value</code> parameter. The valid range is from 0 to 3600 seconds (inclusive), and the default value is 0 seconds.</td>
</tr>
<tr>
<td>condition {client-count <code>condition_value</code></td>
<td>• <strong>encryption</strong>—Requires that the advertised WLAN does not have encryption enabled.</td>
</tr>
<tr>
<td>duration</td>
<td>infrastructure</td>
</tr>
<tr>
<td>rssi</td>
<td>ssid</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

Switch(config)# wireless wps rogue rule rule_3 priority 3
Switch(config-rule)# condition client-count 5
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>match {all | any}</td>
</tr>
</tbody>
</table>
| Example: | Switch(config)# wireless wps rogue rule rule_3 priority 3  
| | Switch(config-rule)# match all  |
| **Step 6** | default |
| Example: | Switch(config)# wireless wps rogue rule rule_3 priority 3  
| | Switch(config-rule)# default  |
| **Step 7** | exit |
| Example: | Switch(config)# wireless wps rogue rule rule_3 priority 3  
| | Switch(config-rule)# exit  
| | Switch(config)#  |
| **Step 8** | shutdown |
| Example: | Switch(config)# wireless wps rogue rule rule_3 priority 3  
| | Switch(config-rule)# shutdown  |
| **Step 9** | end |
| Example: | Switch(config)# end  |
| **Step 10** | configure terminal |
| Example: | Switch# configure terminal  |
| **Step 11** | wireless wps rogue rule shutdown |
| Example: | Switch(config)# wireless wps rogue rule shutdown  |
| **Step 12** | end |
| Example: | Switch(config)# end  |
Configuring Rogue Classification Rules (GUI)

**Procedure**

**Step 1**

Any rules that have already been created are listed in priority order. The name, type, and status of each rule is provided.

**Note**
If you ever want to delete a rule, hover your mouse cursor over the blue drop-down arrow for that rule and click Remove.

**Step 2**
Create a new rule as follows:

a) Click Add Rule. An Add Rule section appears at the top of the page.
b) In the Rule Name text box, enter a name for the new rule. Ensure that the name does not contain any spaces.
c) From the Rule Type drop-down list, choose from the following options to classify rogue access points matching this rule as friendly or malicious:
   - Friendly
   - Malicious
d) Click Add to add this rule to the list of existing rules, or click Cancel to discard this new rule.

**Step 3**
Edit a rule as follows:

a) Click the name of the rule that you want to edit. The Rogue Rule > Edit page appears.
b) From the Type drop-down list, choose from the following options to classify rogue access points matching this rule:
   - Friendly
   - Malicious
c) From the Match Operation text box, choose one of the following:
   - All—If this rule is enabled, a detected rogue access point must meet all of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule.
   - Any—If this rule is enabled, a detected rogue access point must meet any of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule. This is the default value.
d) To enable this rule, select the Enable Rule check box. The default value is unselected.
e) To disable this particular rule, unselect the Enable Rule check box.

**Note**
You cannot disable all the rogue rule in one shot from GUI but you can disable all the rogue rules from CLI using the wireless wps rogue rule shutdown command.
f) From the Add Condition drop-down list, choose one or more of the following conditions that the rogue access point must meet and click Add Condition.
• **SSID**—Requires that the rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the User Configured SSID text box, and click **Add SSID**. The user-configured SSIDs are added and listed.

  **Note**  
  To delete an SSID, highlight the SSID and click **Remove**. The SSID applied on a WLAN cannot be applied for the rogue rule.

• **RSSI**—Requires that the rogue access point have a minimum Received Signal Strength Indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the Minimum RSSI text box. The valid range is –95 to –50 dBm (inclusive), and the default value is 0 dBm.

• **Duration**—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the Time Duration text box. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.

• **Client Count**—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the Minimum Number of Rogue Clients text box. The valid range is 1 to 10 (inclusive), and the default value is 0.

• **No Encryption**—Requires that the rogue access point’s advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option.

  **Note**  
  Cisco Prime Infrastructure refers to this option as “Open Authentication.”

• **Managed SSID**—Requires that the rogue access point’s managed SSID (the SSID configured for the WLAN) be known to the controller. No further configuration is required for this option.

  **Note**  
  The SSID and Managed SSID conditions cannot be used with the All operation because these two SSID lists are mutually exclusive. If you define a rule with Match All and have these two conditions configured, the rogue access points are never classified as friendly or malicious because one of the conditions can never be met.

  You can add up to six conditions per rule. When you add a condition, it appears under the Conditions section.

  **Note**  
  If you ever want to delete a condition from this rule, click **Remove** near the condition.

• **User configured SSID**—Requires that the rogue access point have a substring of the specific user-configured SSID. The controller searches the substring in the same occurrence pattern and returns a match if the substring is found in the whole string of an SSID.

  g) Click **Apply**.

**Step 4**  
If you want to change the priority in which rogue classification rules are applied, follow these steps:

1. Click **Change Priority** to access the Rogue Rules > Priority page.

   The rogue rules are listed in priority order in the Change Rules Priority text box.

2. Click on a specific rule for which you want to change the priority, and click **Up** to raise its priority in the list or **Down** to lower its priority in the list.
You can change priority only for the disabled rule. You cannot change priority only for the enabled rule.

3. Click Apply.

### Viewing and Classifying Rogue Devices (GUI)

#### Procedure

| Step 1 | Choose Monitor > Rogues. |
| Step 2 | Choose the following options to view the different types of rogue access points detected by the controller: |
|        | • Friendly APs |
|        | • Malicious APs |
|        | • Unclassified APs |

The respective rogue APs pages provide the following information: the MAC address of the rogue access point, the number of radios that detected the rogue access point, the number of clients connected to the rogue access point, the current status of the rogue access point, and last heard.

| Step 3 | Get more details about a rogue access point by clicking the MAC address of the access point. The Rogue AP Detail page appears. |
|        | This page provides the following information: the MAC address of the rogue device, the type of rogue device (such as an access point), whether the rogue device is on the wired network, the dates and times when the rogue device was first and last reported, and the current status of the device. |

The Class Type text box shows the current classification for this rogue access point:

• **Friendly**—An unknown access point that matches the user-defined friendly rules or an existing known and acknowledged rogue access point. Friendly access points cannot be contained.

• **Malicious**—An unknown access point that matches the user-defined malicious rules or is moved manually by the user from the Friendly or Unclassified classification type.

*Note* Once an access point is classified as Malicious, you cannot apply rules to it in the future, and it cannot be moved to another classification type. If you want to move a malicious access point to the Unclassified classification type, you must delete the access point and allow the controller to reclassify it.

• **Unclassified**—An unknown access point that does not match the user-defined friendly or malicious rules. An unclassified access point can be contained. It can also be moved to the Friendly or Malicious classification type automatically in accordance with user-defined rules or manually by the user.

| Step 4 | If you want to change the classification of this device, choose a different classification from the Class Type drop-down list. |
A rogue access point cannot be moved to another class if its current state is Contain.

**Step 5**

From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this rogue access point:

- **Internal**—The controller trusts this rogue access point. This option is available if the Class Type is set to Friendly.
- **External**—The controller acknowledges the presence of this rogue access point. This option is available if the Class Type is set to Friendly.
- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients. This option is available if the Class Type is set to Malicious or Unclassified.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action. This option is available if the Class Type is set to Malicious or Unclassified.

The bottom of the page provides information on both the access points that detected this rogue access point and any clients that are associated to it. To see more details for any of the clients, click **Edit** to open the Rogue Client Detail page.

**Step 6**

Click **Apply**.

**Step 7**

Click **Save Configuration**.

**Step 8**

See any adhoc rogues detected by the controller by choosing **Adhoc Rogues**. The Adhoc Rogues page appears.

This page shows the following information: the MAC address, BSSID, and SSID of the adhoc rogue, the number of radios that detected the adhoc rogue, and the current status of the adhoc rogue.

**Step 9**

Obtain more details about an adhoc rogue by clicking the MAC address of the rogue. The Adhoc Rogue Detail page appears.

This page provides the following information: the MAC address and BSSID of the adhoc rogue, the dates and times when the rogue was first and last reported, and the current status of the rogue.

**Step 10**

From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this adhoc rogue:

- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action.
- **Internal**—The controller trusts this rogue access point.
- **External**—The controller acknowledges the presence of this rogue access point.

**Step 11**

From the Maximum Number of APs to Contain the Rogue drop-down list, choose one of the following options to specify the maximum number of access points used to contain this adhoc rogue: **1**, **2**, **3**, or **4**.

The bottom of the page provides information on the access points that detected this adhoc rogue.

**Step 12**

Click **Apply**.

**Step 13**

Click **Save Configuration**.

**Step 14**

View any access points that have been configured to be ignored by choosing **Rogue AP Ignore-List**. The Rogue AP Ignore-List page appears.
This page shows the MAC addresses of any access points that are configured to be ignored. The rogue-ignore list contains a list of any autonomous access points that have been manually added to Cisco Prime Infrastructure maps by the users. The controller regards these autonomous access points as rogues even though the Prime Infrastructure is managing them. The rogue-ignore list allows the controller to ignore these access points. The list is updated as follows:

- When the controller receives a rogue report, it checks to see if the unknown access point is in the rogue-ignore access point list.
- If the unknown access point is in the rogue-ignore list, the controller ignores this access point and continues to process other rogue access points.
- If the unknown access point is not in the rogue-ignore list, the controller sends a trap to the Prime Infrastructure. If the Prime Infrastructure finds this access point in its autonomous access point list, the Prime Infrastructure sends a command to the controller to add this access point to the rogue-ignore list. This access point is then ignored in future rogue reports.
- If a user removes an autonomous access point from the Prime Infrastructure, the Prime Infrastructure sends a command to the controller to remove this access point from the rogue-ignore list.

Examples: Classifying Rogue Access Points

This example shows how to create a rule that can organize and display rogue access points as Friendly:

```
Switch# configure terminal
Switch(config)# wireless wps rogue rule ap1 priority 1
Switch(config-rule)# classify friendly
Switch(config-rule)# end
```

This example shows how to apply a condition that a rogue access point must meet:

```
Switch# configure terminal
Switch(config)# wireless wps rogue rule ap1 priority 1
Switch(config-rule)# condition client-count 5
Switch(config-rule)# condition duration 1000
Switch(config-rule)# end
```

Additional References for Classifying Rogue Access Points

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>
Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information For Classifying Rogue Access Points

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Feature History and Information For Classifying Rogue Access Points
Configuring wIPS

- Finding Feature Information, on page 1171
- Information About wIPS, on page 1171
- How to Configure wIPS on an Access Point, on page 1177
- Monitoring wIPS Information, on page 1178
- Examples: wIPS Configuration, on page 1178
- Additional References for Configuring wIPS, on page 1179
- Feature History for Performing wIPS Configuration, on page 1179

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About wIPS

The Cisco Adaptive Wireless Intrusion Prevention System (wIPS) uses an advanced approach to wireless threat detection and performance management. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention. With a fully infrastructure-integrated solution, you can continually monitor wireless traffic on both the wired and wireless networks and use that network intelligence to analyze attacks from many sources to accurately pinpoint and proactively prevent attacks, rather than wait until damage or exposure has occurred.

Cisco Adaptive wIPS is a part of the Cisco 3300 Series Mobility Services Engine (MSE), which centralizes the processing of intelligence collected by the continuous monitoring of Cisco Aironet APs. With Cisco Adaptive wIPS functionalities and Cisco Prime Infrastructure integration into the Cisco MSE, the wIPS can configure and monitor wIPS policies and alarms and report threats.
If your wIPS deployment consists of a Cisco WLC, access point, and Cisco MSE, you must set all the three entities to the UTC time zone.

Cisco Adaptive wIPS is not configured on the Cisco WLC. Instead, the Cisco Prime Infrastructure forwards the profile configuration to the wIPS service, which forwards the profile to the Cisco WLC. The profile is stored in flash memory on the Cisco WLC and sent to APs when they join the Cisco WLC. When an access point dissassociates and joins another Cisco WLC, it receives the wIPS profile from the new Cisco WLC.

Local-mode APs with a subset of wIPS capabilities are referred to as Enhanced Local Mode access point or ELM AP. You can configure an access point to work in the wIPS mode if the AP is in any of the following modes:

- Monitor
- Local

The regular local mode AP is extended with a subset of wIPS capabilities. This feature enables you to deploy your APs to provide protection without needing a separate overlay network.

wIPS ELM has the limited capability of detecting off-channel alarms. AN AP periodically goes off-channel, and monitors the nonserving channels for a short duration, and triggers alarms if any attack is detected on the channel. But off-channel alarm detection is best effort, and it takes a longer time to detect attacks and trigger alarms, which might cause the ELM AP to intermittently detect an alarm and clear it because it is not visible. APs in any of the above modes can periodically send alarms based on the policy profile to the wIPS service through the Cisco WLC. The wIPS service stores and processes the alarms and generates SNMP traps. Cisco Prime Infrastructure configures its IP address as a trap destination to receive SNMP traps from the Cisco MSE.

This table lists all the SNMP trap controls and their respective traps. When a trap control is enabled, all the traps of that trap control are also enabled.

The Cisco WLC uses only SNMPv2 for SNMP trap transmission.

### Table 85: SNMP Trap Controls and Their Respective Traps

<table>
<thead>
<tr>
<th>Tab Name</th>
<th>Trap Control</th>
<th>Trap</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Link (Port) Up/Down</td>
<td>linkUp, linkDown</td>
</tr>
<tr>
<td></td>
<td>Spanning Tree</td>
<td>newRoot, topologyChange,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>stpInstanceNewRootTrap, stpInstanceTopologyChangeTrap</td>
</tr>
<tr>
<td></td>
<td>Config Save</td>
<td>bsnDot11EssCreated,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bsnDot11EssDeleted,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bsnConfigSaved,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ciscoLwappScheduledResetNotif,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ciscoLwappClearResetNotif,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ciscoLwappResetFailedNotif,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ciscoLwappSysInvalidXmlConfig</td>
</tr>
<tr>
<td>Tab Name</td>
<td>Trap Control</td>
<td>Trap</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>AP</td>
<td>AP Register</td>
<td>bsnAPDisassociated, bsnAPAssociated</td>
</tr>
<tr>
<td></td>
<td>AP Interface Up/Down</td>
<td>bsnAPIfUp, bsnAPIfDown</td>
</tr>
<tr>
<td>Client Traps</td>
<td>802.11 Association</td>
<td>bsnDot11StationAssociate</td>
</tr>
<tr>
<td></td>
<td>802.11 Disassociation</td>
<td>bsnDot11StationDisassociate</td>
</tr>
<tr>
<td></td>
<td>802.11 Deauthentication</td>
<td>bsnDot11StationDeauthenticate</td>
</tr>
<tr>
<td></td>
<td>802.11 Failed Authentication</td>
<td>bsnDot11StationAuthenticateFail</td>
</tr>
<tr>
<td></td>
<td>802.11 Failed Association</td>
<td>bsnDot11StationAssociateFail</td>
</tr>
<tr>
<td></td>
<td>Exclusion</td>
<td>bsnDot11StationBlacklisted</td>
</tr>
<tr>
<td>NAC Alert</td>
<td></td>
<td>cldecClientWlanProfileName, cldecClientIPAddress, cldecApMacAddress, cldecClientQuarantineVLAN, cldecClientAccessVLAN</td>
</tr>
<tr>
<td>Security Traps</td>
<td>User Authentication</td>
<td>bsnTooManyUnsuccessLoginAttempts, cLWAGuestUserLoggedIn, cLWAGuestUserLoggedOut</td>
</tr>
<tr>
<td></td>
<td>RADIUS Servers Not Responding</td>
<td>bsnRADIUSServerNotResponding, ciscoLwappAAARadiusReqTimedOut</td>
</tr>
<tr>
<td></td>
<td>WEP Decrypt Error</td>
<td>bsnWepKeyDecryptError</td>
</tr>
<tr>
<td></td>
<td>SNMP Authentication</td>
<td>agentSnmpAuthenticationTrapFlag</td>
</tr>
<tr>
<td></td>
<td>Multiple Users</td>
<td>multipleUsersTrap</td>
</tr>
<tr>
<td>Tab Name</td>
<td>Trap Control</td>
<td>Trap</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Auto RF Profile Traps</td>
<td>Load Profile</td>
<td>bsnAPLoadProfileFailed</td>
</tr>
<tr>
<td></td>
<td>Noise Profile</td>
<td>bsnAPNoiseProfileFailed</td>
</tr>
<tr>
<td></td>
<td>Interference Profile</td>
<td>bsnAPIInterferenceProfileFailed</td>
</tr>
<tr>
<td></td>
<td>Coverage Profile</td>
<td>bsnAPCoverageProfileFailed</td>
</tr>
<tr>
<td>Auto RF Update Traps</td>
<td>Channel Update</td>
<td>bsnAPCurrentChannelChanged</td>
</tr>
<tr>
<td></td>
<td>Tx Power Update</td>
<td>bsnAPCurrentTxPowerChanged</td>
</tr>
<tr>
<td>Mesh Traps</td>
<td>Child Excluded Parent</td>
<td>ciscoLwappMeshChildExcludedParent</td>
</tr>
<tr>
<td></td>
<td>Parent Change</td>
<td>ciscoLwappMeshParentChange</td>
</tr>
<tr>
<td></td>
<td>Auth failure Mesh</td>
<td>ciscoLwappMeshAuthorizationFailure</td>
</tr>
<tr>
<td></td>
<td>Child Moved</td>
<td>ciscoLwappMeshChildMoved</td>
</tr>
<tr>
<td></td>
<td>Excessive Parent Change</td>
<td>ciscoLwappMeshExcessiveParentChange</td>
</tr>
<tr>
<td></td>
<td>Excessive Children</td>
<td>ciscoLwappMeshExcessiveChildren</td>
</tr>
<tr>
<td></td>
<td>Poor SNR</td>
<td>ciscoLwappMeshAbateSNR,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ciscoLwappMeshOnsetSNR</td>
</tr>
<tr>
<td></td>
<td>Console Login</td>
<td>ciscoLwappMeshConsoleLogin</td>
</tr>
<tr>
<td></td>
<td>Excessive Association</td>
<td>ciscoLwappMeshExcessiveAssociation</td>
</tr>
<tr>
<td></td>
<td>Default Bridge Group Name</td>
<td>ciscoLwappMeshDefaultBridgeGroupName</td>
</tr>
</tbody>
</table>

The following are the trap descriptions for the traps mentioned in the **SNMP Trap Controls and Their Respective Traps** table:

- **General Traps**
  - SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated.
  
  **Note**  When a user who is configured in SNMP V3 mode tries to access the Cisco WLC with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

  - Link (Port) Up/Down—Link changes status from up or down.
  - Link (Port) Up/Down—Link changes status from up or down.
  - Multiple Users—Two users log in with the same ID.
  - Rogue AP—Whenever a rogue access point is detected, this trap is sent with its MAC address; when a rogue access point that was detected earlier no longer exists, this trap is sent.
  - Config Save—Notification that is sent when the Cisco WLC configuration is modified.
• Cisco AP Traps
  • AP Register—Notification sent when an access point associates or disassociates with the Cisco WLC.
  • AP Interface Up/Down—Notification sent when an access point interface (802.11X) status goes up or down.

• Client-Related Traps
  • 802.11 Association—Associate notification that is sent when a client sends an association frame.
  • 802.11 Disassociation—Disassociate notification that is sent when a client sends a disassociation frame.
  • 802.11 Deauthentication—Deauthenticate notification that is sent when a client sends a deauthentication frame.
  • 802.11 Failed Authentication—Authenticate failure notification that is sent when a client sends an authentication frame with a status code other than successful.
  • 802.11 Failed Association—Associate failure notification that is sent when the client sends an association frame with a status code other than successful.
  • Exclusion—Associate failure notification that is sent when a client is exclusion listed (blacklisted).

  Note  The maximum number of static blacklist entries that the APs can have is 340.

• Authentication—Authentication notification that is sent when a client is successfully authenticated.

• Max Clients Limit Reached—Notification that is sent when the maximum number of clients, defined in the Threshold field, are associated with the Cisco WLC.

• NAC Alert—Alert that is sent when a client joins an SNMP NAC-enabled WLAN.

  This notification is generated when a client on NAC-enabled SSIDs completes Layer2 authentication to inform the NAC appliance about the client’s presence. cldcClientWlanProfileName represents the profile name of the WLAN that the 802.11 wireless client is connected to, cldcClientIPAddress represents the unique IP address of the client. cldcApMacAddress represents the MAC address of the AP to which the client is associated. cldcClientQuarantineVLAN represents the quarantine VLAN for the client. cldcClientAccessVLAN represents the access VLAN for the client.

• Association with Stats—Associate notification that is sent with data statistics when a client is associated with the Cisco WLC, or roams. Data statistics include transmitted and received bytes and packets.

• Disassociation with Stats—Disassociate notification that is sent with data statistics when a client disassociates from the Cisco WLC. Data statistics include transmitted and received bytes and packets, SSID, and session ID.

  Note  When you downgrade to Release 7.4 from a later release, if a trap that was not supported in Release 7.4 (for example, NAC Alert trap) is enabled before the downgrade, all traps are disabled. After the downgrade, you must enable all the traps that were enabled before the downgrade. We recommend that you disable the new traps before the downgrade so that all the other traps are not disabled.
Security Traps

- User Auth Failure—This trap informs that a client RADIUS Authentication failure has occurred.
- RADIUS Server No Response—This trap is to indicate that no RADIUS servers are responding to authentication requests sent by the RADIUS client.
- WEP Decrypt Error—Notification sent when the Cisco WLC detects a WEP decrypting error.
- Rouge AP—Whenever a rogue access point is detected, this trap is sent with its MAC address; when a rogue access point that was detected earlier no longer exists, this trap is sent.
- SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated.

Note

When a user who is configured in SNMP V3 mode tries to access the Cisco WLC with an incorrect password, authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

- Multiple Users—Two users log in with the same ID.
- SNMP Authentication

SNMP Authentication

- Load Profile—Notification sent when the Load Profile state changes between PASS and FAIL.
- Noise Profile—Notification sent when the Noise Profile state changes between PASS and FAIL.
- Interference Profile—Notification sent when the Interference Profile state changes between PASS and FAIL.
- Coverage Profile—Notification sent when the Coverage Profile state changes between PASS and FAIL.

Auto RF Profile Traps

- Load Profile—Notification sent when the Load Profile state changes between PASS and FAIL.
- Noise Profile—Notification sent when the Noise Profile state changes between PASS and FAIL.
- Interference Profile—Notification sent when the Interference Profile state changes between PASS and FAIL.
- Coverage Profile—Notification sent when the Coverage Profile state changes between PASS and FAIL.

Auto RF Update Traps

- Channel Update—Notification sent when the access point dynamic channel algorithm is updated.
- Tx Power Update—Notification sent when the access point dynamic transmit power algorithm is updated.

Mesh Traps

- Child Excluded Parent—Notification that is sent when a defined number of failed association to the Cisco WLC occurs through a parent mesh node.
- Notification sent when a child mesh node exceeds the threshold limit of the number of discovery response timeouts. The child mesh node does not try to associate an excluded parent mesh node for the interval defined. The child mesh node remembers the excluded parent MAC address when it joins the network, and informs the Cisco WLC.
- Parent Change—Notification is sent by the agent when a child mesh node changes its parent. The child mesh node remembers previous parent and informs the Cisco WLC about the change of parent when it rejoins the network.
• Child Moved—Notification sent when a parent mesh node loses connection with its child mesh node.
• Excessive Parent Change—Notification sent when the child mesh node changes its parent frequently. Each mesh node keeps a count of the number of parent changes in a fixed time. If it exceeds the defined threshold, the child mesh node informs the Cisco WLC.
• Excessive Children—Notification sent when the child count exceeds for a RAP and a MAP.
• Poor SNR—Notification sent when the child mesh node detects a lower SNR on a backhaul link. For the other trap, a notification is sent to clear a notification when the child mesh node detects an SNR on a backhaul link that is higher then the object defined by 'clMeshSNRThresholdAbate'.
• Console Login—Notification is sent by the agent when a login on a MAP console is either successful or fail after three attempts.
• Default Bridge Group Name—Notification sent when the MAP mesh node joins its parent using the default bridge group name.

Note
The remaining traps do not have trap controls. These traps are not generated too frequently and do not require any trap control. Any other trap that is generated by the Cisco WLC cannot be turned off.

Note
In all of the above cases, the Cisco WLC functions solely as a forwarding device.

How to Configure wIPS on an Access Point

Configuring wIPS on an Access Point (CLI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>ap name name mode submode wips</td>
<td>Configure an access point for local or monitor mode and then set the submode to wIPS.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# ap name ap1 mode local wips</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>show wireless wps wips summary</td>
<td>View the wIPS configuration on the access point.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# show wireless wps wips summary</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>show wireless wps wips statistics</td>
<td>View the current state of wIPS configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch#</td>
<td></td>
</tr>
</tbody>
</table>
Configuring wIPS on an Access Point (GUI)

Procedure

Step 1
Choose Configuration > Wireless > Access Points > All APs.
The All APs page appears with a list of all access points that are associated with the switch.

Step 2
Click the name of the access point for which you want to configure wIPS.
The AP > Edit page appears.

Step 3
In the General area, set the AP Mode parameter. To configure an access point for wIPS, you must choose one of the following modes from the AP Mode drop-down list:
- Local
- Monitor

Step 4
Set the AP Sub Mode to wIPS by choosing wIPS from the AP Sub Mode drop-down list.

Step 5
Click Apply.

Step 6
Click Save.

Monitoring wIPS Information

This section describes the new command for wIPS.
The following command can be used to monitor wIPS configured on the access point.

Table 86: Monitoring wIPS Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless wps wips summary</td>
<td>Displays the wIPS configuration on the access point.</td>
</tr>
<tr>
<td>show wireless wps wips statistics</td>
<td>Displays the current state of wIPS configuration.</td>
</tr>
</tbody>
</table>

Examples: wIPS Configuration

This example shows how to configure wIPS on AP1:

```
Switch# ap name ap1 mode local submode wips
Switch# end
Switch# show wireless wps wips summary
```
Additional References for Configuring wIPS

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History for Performing wIPS Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
PART XII

System Management

- Administering the System, on page 1183
- Performing Switch Setup Configuration, on page 1215
- Configuring Right-To-Use Licenses, on page 1239
- Configuring Administrator Usernames and Passwords, on page 1253
- 802.11 parameters and Band Selection, on page 1259
- Configuring Aggressive Load Balancing, on page 1281
- Configuring Client Roaming, on page 1287
- Configuring Application Visibility and Control, on page 1299
- Configuring Voice and Video Parameters, on page 1331
- Configuring RFID Tag Tracking, on page 1353
- Configuring Location Settings, on page 1357
- Monitoring Flow Control, on page 1365
- Configuring System Message Logs, on page 1369
- Configuring Online Diagnostics, on page 1383
- Predownloading an Image to Access Points, on page 1393
- Configuring Wireless Virtual Switching System, on page 1399
- Troubleshooting the Software Configuration, on page 1405
Administering the System

- Finding Feature Information, on page 1183
- Finding Feature Information, on page 1183
- Information About Administering the Switch, on page 1184
- How to Administer the Switch, on page 1190
- Monitoring and Maintaining Administration of the Switch, on page 1209
- Configuration Examples for Switch Administration, on page 1210
- Additional References for Switch Administration, on page 1213
- Feature History and Information for Switch Administration, on page 1214

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Information About Administering the Switch

System Time and Date Management

You can manage the system time and date on your switch using automatic configuration methods (RTC and NTP), or manual configuration methods.

Note

For complete syntax and usage information for the commands used in this section, see the Cisco IOS Configuration Fundamentals Command Reference on Cisco.com.

System Clock

The basis of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time.

The system clock can then be set from these sources:

• NTP
• Manual configuration

The system clock can provide time to these services:

• User show commands
• Logging and debugging messages

The system clock keeps track of time internally based on Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone and summer time (daylight saving time) so that the time appears correctly for the local time zone.

The system clock keeps track of whether the time is authoritative or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time is available only for display purposes and is not redistributed.

Network Time Protocol

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

NTP uses the concept of a stratum to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically
chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

The communications between devices running NTP (known as associations) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

Cisco’s implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet.

The figure below shows a typical network example using NTP. Switch A is the NTP master, with the Switch B, C, and D configured in NTP server mode, in server association with Switch A. Switch E is configured as an NTP peer to the upstream and downstream Switch, Switch B and Switch F, respectively.

*Figure 69: Typical NTP Network Configuration*

If the network is isolated from the Internet, Cisco’s implementation of NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.
When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

**NTP Stratum**

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

**NTP Associations**

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

**NTP Security**

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

**NTP Implementation**

Implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet.

*Figure 70: Typical NTP Network Configuration*

The following figure shows a typical network example using NTP. Controller A is the NTP master, with the Controller B, C, and D configured in NTP server mode, in server association with Controller A. Controller E is configured as an NTP peer to the upstream and downstream controllers, Controller B and Controller F, respectively.
If the network is isolated from the Internet, NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

**NTP Version 4**

NTP version 4 is implemented on the switch. NTPv4 is an extension of NTP version 3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3.

NTPv4 provides these capabilities:

- Support for IPv6.
- Improved security compared to NTPv3. The NTPv4 protocol provides a security framework based on public key cryptography and standard X509 certificates.
- Automatic calculation of the time-distribution hierarchy for a network. Using specific multicast groups, NTPv4 automatically configures the hierarchy of the servers to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.
For details about configuring NTPv4, see the *Implementing NTPv4 in IPv6* chapter of the *Cisco IOS IPv6 Configuration Guide, Release 12.4T*.

**DNS**

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map hostnames to IP addresses. When you configure DNS on your switch, you can substitute the hostname 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 allows a device to 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 `cisco.com`. A specific device in this domain, for example, 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, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the hostnames, specify the name server that is present on your network, and enable the DNS.

**Default DNS Settings**

*Table 87: Default DNS Settings*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS enable state</td>
<td>Enabled.</td>
</tr>
<tr>
<td>DNS default domain name</td>
<td>None configured.</td>
</tr>
<tr>
<td>DNS servers</td>
<td>No name server addresses are configured.</td>
</tr>
</tbody>
</table>

**Login Banners**

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner is displayed on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

The login banner is also displayed on all connected terminals. It appears after the MOTD banner and before the login prompts.

---

**Note**

For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.4*.

**Default Banner Configuration**

The MOTD and login banners are not configured.
MAC Address Table

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- Dynamic address—A source MAC address that the switch learns and then ages when it is not in use.
- Static address—A manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address and the type (static or dynamic).

For complete syntax and usage information for the commands used in this section, see the command reference for this release.

MAC Address Table Creation

With multiple MAC addresses supported on all ports, you can connect any port on the switch to other network devices. The switch provides dynamic addressing by learning the source address of packets it receives on each port and adding the address and its associated port number to the address table. As devices are added or removed from the network, the switch updates the address table, adding new dynamic addresses and aging out those that are not in use.

The aging interval is globally configured. However, the switch maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The switch sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the switch forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded. The switch always uses the store-and-forward method: complete packets are stored and checked for errors before transmission.

MAC Addresses and VLANs

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Unicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 1 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN.

Default MAC Address Table Settings

The following table shows the default settings for the MAC address table.

Table 88: Default Settings for the MAC Address

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aging time</td>
<td>300 seconds</td>
</tr>
</tbody>
</table>
ARP Table Management

To communicate with a device (over Ethernet, for example), the software first must learn the 48-bit MAC address or the local data link address of that device. The process of learning the local data link address from an IP address is called *address resolution*.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and the VLAN ID. Using an IP address, ARP finds the associated MAC address. When a MAC address is found, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the `arpa` keyword) is enabled on the IP interface.

ARP entries added manually to the table do not age and must be manually removed.

For CLI procedures, see the Cisco IOS Release 12.4 documentation on *Cisco.com*.

### How to Administer the Switch

#### Configuring the Time and Date Manually

System time remains accurate through restarts and reboot, however, you can manually configure the time and date after the system is restarted.

We recommend that you use manual configuration only when necessary. If you have an outside source to which the switch can synchronize, you do not need to manually set the system clock.

#### Setting the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

Follow these steps to set the system clock:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
Purpose

Command or Action

Step 2
Use one of the following:

- `clock set hh:mm:ss day month year`
- `clock set hh:mm:ss month day year`

Example:

Switch# clock set 13:32:00 23 March 2013

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
</table>
| Manually set the system clock using one of these formats:
| `hh:mm:ss`—Specifies the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured timezone.
| `day`—Specifies the day by date in the month.
| `month`—Specifies the month by name.
| `year`—Specifies the year (no abbreviation). |

Configuring the Time Zone

Follow these steps to manually configure the time zone:

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.
| Example:          | • Enter your password if prompted. |
| Switch> enable    |         |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example:          |         |
| Switch# configure terminal |         |
| **Step 3** clock timezone zone hours-offset [minutes-offset] | Sets the time zone. |
| Example:          | Internal time is kept in Coordinated Universal Time (UTC), so this command is used only for display purposes and when the time is manually set. |
| Switch(config)# clock timezone AST -3 30 | • `zone`—Enters the name of the time zone to be displayed when standard time is in effect. The default is UTC.
| | • `hours-offset`—Enters the hours offset from UTC.
| | • (Optional) `minutes-offset`—Enters the minutes offset from UTC. This available |
### Configuring Summer Time (Daylight Saving Time)

To configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year, perform this task:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
   enable
   Example:
   Switch> enable | Enables privileged EXEC mode.
   • Enter your password if prompted. |
| **Step 2**
   configure terminal
   Example:
   Switch# configure terminal | Enters global configuration mode. |
| **Step 3**
   clock summer-time zone date month year hh:mm date month year hh:mm [offset]]
   Example:
   Switch(config)# clock summer-time PDT date | Configures summer time to start and end on specified days every year. |
### Configuring Summer Time (Daylight Saving Time)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 March 2013 2:00 3 November 2013 2:00</td>
<td>Configures summer time to start and end on the specified days every year. 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. Summer time is disabled by default. If you specify <code>clock summer-time zone recurring</code> without parameters, the summer time rules default to the United States rules. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.</td>
</tr>
</tbody>
</table>
| **Step 4** clock summer-time zone recurring [week day month hh:mm weekday month hh:mm [offset]] | **Example:**

```
Switch(config)# clock summer-time
PDT recurring 10 March 2013 2:00 3 November 2013 2:00
```

- `zone`—Specifies the name of the time zone (for example, PDT) to be displayed when summer time is in effect.
- (Optional) `week`—Specifies the week of the month (1 to 4, first, or last).
- (Optional) `day`—Specifies the day of the week (Sunday, Monday...).
- (Optional) `month`—Specifies the month (January, February...).
- (Optional) `hh:mm`—Specifies the time (24-hour format) in hours and minutes.
- (Optional) `offset`—Specifies the number of minutes to add during summer time. The default is 60. |
| **Step 5** end | **Example:**

```
Switch(config)# end
```

Returns to privileged EXEC mode. |
| **Step 6** show running-config | **Example:**

```
Switch# show running-config
```

Verifies your entries. |
| **Step 7** copy running-config startup-config | **Example:**

(Optional) Saves your entries in the configuration file. |
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):

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Step 1**  
**enable**  
**Example:**  
Switch> enable

**Step 2**  
**configure terminal**  
**Example:**  
Switch# configure terminal

**Step 3**  
**clock summer-time zone date [month date year hh:mm month date year hh:mm [offset]]**  
**Example:**  
Switch# clock summer-time zone date [month date year hh:mm month date year hh:mm [offset]]

**Step 4**  
**end**  
**Example:**  
Switch> end

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 to 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.
### Configuring a System Name

Follow these steps to manually configure a system name:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>hostname name</td>
<td>Configures a system name. When you set the system name, it is also used as the system prompt.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# hostname name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>remote-users</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default setting is Switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The name must follow the rules for ARPANET hostnames. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names can be up to 63 characters.</td>
</tr>
</tbody>
</table>
### Setting Up DNS

If you use the switch IP address as its hostname, the IP address is used and no DNS query occurs. If you configure a hostname that contains no periods (.), a period followed by the default domain name is appended to the hostname 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 hostname, the Cisco IOS software looks up the IP address without appending any default domain name to the hostname.

Follow these steps to set up your switch to use the DNS:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).</td>
</tr>
<tr>
<td><code>ip domain-name name</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# ip domain-name Cisco.com</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies the address of one or more name servers to use for name and address resolution. Do not include the initial period that separates an unqualified name from the domain name. At boot time, no domain name is configured; however, if the switch configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).</td>
</tr>
<tr>
<td>ip name-server server-address1 [server-address2 ... server-address6]</td>
<td>You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The switch sends DNS queries to the primary server first. If that query fails, the backup servers are queried.</td>
</tr>
</tbody>
</table>

**Example:**

| Step 5       | (Optional) Enables DNS-based hostname-to-address translation on your switch. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS). |
| ip domain-lookup [nsap | source-interface interface]      |

| Example:      | Switch(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300 |

**Step 6** | Returns to privileged EXEC mode. |
| end | Switch(config)# end |

**Step 7** | Verifies your entries. |
| show running-config | Switch# show running-config |

**Step 8** | (Optional) Saves your entries in the configuration file. |
| copy running-config startup-config | Switch# copy running-config startup-config |
Configuring a Message-of-the-Day Login Banner

You can create a single or multiline message banner that appears on the screen when someone logs in to the switch.

Follow these steps to configure a MOTD login banner:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
Example: Switch> enable |
| **Step 2** | configure terminal | Enters global configuration mode.  
Example: Switch# configure terminal |
| **Step 3** | banner motd c message c | Specifies the message of the day.  
Example: Switch(config)# banner motd #  
This is a secure site. Only authorized users are allowed. For access, contact technical support. # c—Enters the delimiting character of your choice, for example, a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.  
message—Enters a banner message up to 255 characters. You cannot use the delimiting character in the message. |
| **Step 4** | end | Returns to privileged EXEC mode.  
Example: Switch(config)# end |
| **Step 5** | show running-config | Verifies your entries.  
Example: Switch# show running-config |
| **Step 6** | copy running-config startup-config | (Optional) Saves your entries in the configuration file.  
Example: Switch# copy running-config |
You can configure a login banner to be displayed on all connected terminals. This banner appears after the MOTD banner and before the login prompt.

Follow these steps to configure a login banner:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> banner login $ message $</td>
<td>Specifies the login message.</td>
</tr>
<tr>
<td>Example:</td>
<td>c—Enters the delimiting character of your choice, for example, a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.</td>
</tr>
<tr>
<td>Switch(config)# banner login $</td>
<td>message—Enters a login message up to 255 characters. You cannot use the delimiting character in the message.</td>
</tr>
<tr>
<td>Access for authorized users only. Please enter your username and password.</td>
<td></td>
</tr>
<tr>
<td>$</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
</tbody>
</table>
Managing the MAC Address Table

Changing the Address Aging Time

Follow these steps to configure the dynamic address table aging time:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> mac address-table aging-time [0</td>
<td>10-1000000] [routed-mac</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# mac address-table aging-time 500 vlan 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring MAC Address Change Notification Traps

Follow these steps to configure the switch to send MAC address change notification traps to an NMS host:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
  Example:  
  Switch> enable |  
  • Enter your password if prompted. |
| Step 2 | configure terminal | Enters global configuration mode. |
  Example:  
  Switch# configure terminal |
| Step 3 | snmp-server host host-addr community-string notification-type { informs | traps } { version { 1 | 2c | 3 } | vrf vrf instance name} | Specifies the recipient of the trap message.  
  • host-addr—Specifies the name or address of the NMS.  
  • traps (the default)—Sends SNMP traps to the host.  
  • informs—Sends SNMP informs to the host.  
  • version—Specifies the SNMP version to support. Version 1, the default, is not available with informs.  
  • community-string—Specifies 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 |  
  Example:  
  Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification |
### Configuring MAC Address Change Notification Traps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>command before using the <code>snmp-server host</code> command.</td>
<td></td>
</tr>
<tr>
<td>• <code>notification-type</code>—Uses the <code>mac-notification</code> keyword.</td>
<td></td>
</tr>
<tr>
<td>• <code>vrf vrf instance name</code>—Specifies the VPN routing/forwarding instance for this host.</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 4

**snmp-server enable traps mac-notification change**

Example:

```
Switch(config)# snmp-server enable traps mac-notification change
```

Enables the switch to send MAC address change notification traps to the NMS.

#### Step 5

**mac address-table notification change**

Example:

```
Switch(config)# mac address-table notification change
```

Enables the MAC address change notification feature.

#### Step 6

**mac address-table notification change**

*Example:*

```
Switch(config)# mac address-table notification change interval 123
Switch(config)# mac address-table notification change history-size 100
```

Enters the trap interval time and the history table size.

- (Optional) `interval value`—Specifies the notification trap interval in seconds between each set of traps that are generated to the NMS. The range is 0 to 2147483647 seconds; the default is 1 second.

- (Optional) `history-size value`—Specifies the maximum number of entries in the MAC notification history table. The range is 0 to 500; the default is 1.

#### Step 7

**interface interface-id**

Example:

```
Switch(config)# interface gigabitethernet 1/0/2
```

Enters interface configuration mode, and specifies the Layer 2 interface on which to enable the SNMP MAC address notification trap.

#### Step 8

**snmp trap mac-notification change {added | removed}**

Example:

```
Switch(config-if)# snmp trap mac-notification change added
```

Enables the MAC address change notification trap on the interface.

- Enables the trap when a MAC address is added on this interface.
Configuring MAC Address Move Notification Traps

When you configure MAC-move notification, an SNMP notification is generated and sent to the network management system whenever a MAC address moves from one port to another within the same VLAN.

Follow these steps to configure the switch to send MAC address-move notification traps to an NMS host:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>snmp-server host host-addr {traps</td>
<td>informs} {version {1 | 2c | 3}} community-string notification-type</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• host-addr—Specifies the name or address of the NMS.</td>
</tr>
</tbody>
</table>
### Configuring MAC Address Move Notification Traps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification</code></td>
<td>• <strong>traps</strong> (the default)—Sends SNMP traps to the host.</td>
</tr>
<tr>
<td>• <strong>informs</strong>—Sends SNMP informs to the host.</td>
<td></td>
</tr>
<tr>
<td>• <strong>version</strong>—Specifies the SNMP version to support. Version 1, the default, is not available with informs.</td>
<td></td>
</tr>
<tr>
<td>• <strong>community-string</strong>—Specifies the string to send with the notification operation. Though you can set this string by using the <code>snmp-server host</code> command, we recommend that you define this string by using the <code>snmp-server community</code> command before using the <code>snmp-server host</code> command.</td>
<td></td>
</tr>
<tr>
<td>• <strong>notification-type</strong>—Uses the <code>mac-notification</code> keyword.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 4

**snmp-server enable traps mac-notification move**

**Example:**

```
Switch(config)# snmp-server enable traps
mac-notification move
```

Enables the switch to send MAC address move notification traps to the NMS.

### Step 5

**mac address-table notification mac-move**

**Example:**

```
Switch(config)# mac address-table notification mac-move
```

Enables the MAC address move notification feature.

### Step 6

**end**

**Example:**

```
Switch(config)# end
```

Returns to privileged EXEC mode.

### Step 7

**show running-config**

**Example:**

```
Switch# show running-config
```
### Configuring MAC Threshold Notification Traps

When you configure MAC threshold notification, an SNMP notification is generated and sent to the network management system when a MAC address table threshold limit is reached or exceeded.

Follow these steps to configure the switch to send MAC address table threshold notification traps to an NMS host:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  Example:  
  Switch> enable |
| **Step 2** configure terminal | Enters global configuration mode.  
  Example:  
  Switch# configure terminal |
| **Step 3** `snmp-server host host-addr {traps | informs} [version {1 | 2c | 3}] community-string notification-type` | Specifies the recipient of the trap message.  
  Example:  
  Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification  
  • `host-addr`—Specifies the name or address of the NMS.  
  • `traps` (the default)—Sends SNMP traps to the host.  
  • `informs`—Sends SNMP informs to the host. |
<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SpecifiestheSNMPversiontosupport.</td>
<td>version—</td>
</tr>
<tr>
<td></td>
<td>Specifiesthestringtosendwiththenotificationoperation.</td>
</tr>
<tr>
<td></td>
<td>Uses the</td>
</tr>
<tr>
<td>EnablesMACthresholdnotificationtraps</td>
<td>snmp-server enable traps mac-notification threshold</td>
</tr>
<tr>
<td>EnablestheMACaddressthresholdnotification</td>
<td>mac address-table notification threshold</td>
</tr>
<tr>
<td>Enters the threshold value for the MAC address</td>
<td>mac address-table notification threshold [limit\ percentage] [interval\ time]</td>
</tr>
<tr>
<td></td>
<td>(Optional) limit percentage—Specifies the percentage of the MAC address table use; valid values are from 1 to 100 percent. The default is 50 percent.</td>
</tr>
<tr>
<td></td>
<td>(Optional) interval time—Specifies the time between notifications; valid values are greater than or equal to 120 seconds. The default is 120 seconds.</td>
</tr>
<tr>
<td>Returns to privileged EXEC mode.</td>
<td>end</td>
</tr>
</tbody>
</table>

**Step 4**

```bash
Switch(config)# snmp-server enable traps mac-notification threshold
```

**Step 5**

```bash
Switch(config)# mac address-table notification threshold
```

**Step 6**

```bash
Switch(config)# mac address-table notification threshold limit 78
Switch(config)# mac address-table notification threshold interval 123
```

**Step 7**

```bash
Switch(config)# end
```
### Adding and Removing Static Address Entries

Follow these steps to add a static address:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
  | Example:  
  Switch> enable |
| Step 2 | configure terminal | Enters global configuration mode. |
  | Example:  
  Switch# configure terminal |
| Step 3 | mac address-table static mac-addr vlan  
  vlan-id interface interface-id | Adds a static address to the MAC address table.  
  • mac-addr—Specifies the destination MAC unicast address to add to the address table.  
  • vlan-id—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.  
  • interface-id—Specifies the interface to which the received packet is forwarded. Valid interfaces include physical ports or port channels. For static multicast |
  | Example:  
  Switch(config)# mac address-table  
  static c2f3.220a.12f4 vlan 4 interface  
  gigabitethernet 1/0/1 |
Configuring Unicast MAC Address Filtering

Follow these steps to configure the Switch to drop a source or destination unicast static address:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>mac address-table static mac-addr vlan vlan-id drop</code></td>
<td>Enables unicast MAC address filtering and configure the switch to drop a packet with the specified source or destination unicast static address.</td>
</tr>
</tbody>
</table>

### Example:

```
Switch> enable
```

```
Switch# configure terminal
```

```
Switch(config)# mac address-table
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| static c2f3.220a.12f4 vlan 4 drop | *mac-addr*—Specifies a source or destination unicast MAC address (48-bit). Packets with this MAC address are dropped.  
*vlan-id*—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094. |

**Step 4**  
*Example:*  
Switch(config)# end  

<table>
<thead>
<tr>
<th>Step 5</th>
<th>show running-config</th>
<th>Verifies your entries.</th>
</tr>
</thead>
</table>
| *Example:*  
Switch# show running-config | |

**Step 6**  
*Example:*  
Switch# copy running-config startup-config  

(Optional) Saves your entries in the configuration file.  

---

**Monitoring and Maintaining Administration of the Switch**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mac address-table dynamic</td>
<td>Removes all dynamic entries.</td>
</tr>
<tr>
<td>clear mac address-table dynamic address mac-address</td>
<td>Removes a specific MAC address.</td>
</tr>
<tr>
<td>clear mac address-table dynamic interface interface-id</td>
<td>Removes all addresses on the specified physical port or port channel.</td>
</tr>
<tr>
<td>clear mac address-table dynamic vlan vlan-id</td>
<td>Removes all addresses on a specified VLAN.</td>
</tr>
<tr>
<td>show clock [detail]</td>
<td>Displays the time and date configuration.</td>
</tr>
<tr>
<td>show ip igmp snooping groups</td>
<td>Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.</td>
</tr>
</tbody>
</table>
### Configuration Examples for Switch Administration

**Example: Setting the System Clock**

This example shows how to manually set the system clock:

```
Switch# clock set 13:32:00 23 July 2013
```

**Examples: Configuring Summer Time**

This example (for daylight savings time) shows how to specify that summer time starts on March 10 at 02:00 and ends on November 3 at 02:00:

```
Switch(config)# clock summer-time PDT recurring PST date
10 March 2013 2:00 3 November 2013 2:00
```

This example shows how to set summer time start and end dates:

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mac address-table address mac-address</code></td>
<td>Displays MAC address table information for the specified MAC address.</td>
</tr>
<tr>
<td><code>show mac address-table aging-time</code></td>
<td>Displays the aging time in all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td><code>show mac address-table count</code></td>
<td>Displays the number of addresses present in all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td><code>show mac address-table dynamic</code></td>
<td>Displays only dynamic MAC address table entries.</td>
</tr>
<tr>
<td><code>show mac address-table interface interface-name</code></td>
<td>Displays the MAC address table information for the specified interface.</td>
</tr>
<tr>
<td><code>show mac address-table move update</code></td>
<td>Displays the MAC address table move update information.</td>
</tr>
<tr>
<td><code>show mac address-table multicast</code></td>
<td>Displays a list of multicast MAC addresses.</td>
</tr>
<tr>
<td>`show mac address-table notification {change</td>
<td>mac-move</td>
</tr>
<tr>
<td><code>show mac address-table secure</code></td>
<td>Displays the secure MAC addresses.</td>
</tr>
<tr>
<td><code>show mac address-table static</code></td>
<td>Displays only static MAC address table entries.</td>
</tr>
<tr>
<td><code>show mac address-table vlan vlan-id</code></td>
<td>Displays the MAC address table information for the specified VLAN.</td>
</tr>
</tbody>
</table>
Switch(config)#clock summer-time PST date
20 March 2013 2:00 20 November 2013 2:00

Example: Configuring a MOTD Banner

This example shows how to configure a MOTD banner by using the pound sign (#) symbol as the beginning and ending delimiter:

Switch(config)# banner motd#
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
Switch(config)#

This example shows the banner that appears from the previous configuration:

Unix> telnet 192.0.2.15
Trying 192.0.2.15...
Connected to 192.0.2.15.
Escape character is '^]'.
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
User Access Verification
Password:

Example: Configuring a Login Banner

This example shows how to configure a login banner by using the dollar sign ($) symbol as the beginning and ending delimiter:

Switch(config)# banner login$
Access for authorized users only. Please enter your username and password.
$
Switch(config)#
Example: Configuring MAC Address Change Notification Traps

This example shows how to specify 172.20.10.10 as the NMS, enable MAC address notification traps to the NMS, enable the MAC address-change notification feature, set the interval time to 123 seconds, set the history-size to 100 entries, and enable traps whenever a MAC address is added on the specified port:

Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)# mac address-table notification change interval 123
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface gigabitethernet 1/2/1
Switch(config-if)# snmp trap mac-notification change added

Example: Configuring MAC Threshold Notification Traps

This example shows how to specify 172.20.10.10 as the NMS, enable the MAC address threshold notification feature, set the interval time to 123 seconds, and set the limit to 78 per cent:

Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification threshold
Switch(config)# mac address-table notification threshold interval 123
Switch(config)# mac address-table notification threshold limit 78

Example: Adding the Static Address to the MAC Address Table

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination address, the packet is forwarded to the specified port:

Note
You cannot associate the same static MAC address to multiple interfaces. If the command is executed again with a different interface, the static MAC address is overwritten on the new interface.

Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 1/1/1

Example: Configuring Unicast MAC Address Filtering

This example shows how to enable unicast MAC address filtering and how to configure drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
Additional References for Switch Administration

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td>System Management Command Reference (Catalyst 3850 Switches) System Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Network management configuration</td>
<td>Network Management Configuration Guide (Catalyst 3850 Switches) Network Management Configuration Guide (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Layer 2 configuration</td>
<td>Layer 2/3 Configuration Guide (Catalyst 3850 Switches) Layer 2 Configuration Guide (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>VLAN configuration</td>
<td>VLAN Configuration Guide (Catalyst 3850 Switches) VLAN Configuration Guide (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Platform-independent command references</td>
<td>Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Platform-independent configuration information</td>
<td>Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>
### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

### Feature History and Information for Switch Administration

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Performing Switch Setup Configuration

- Finding Feature Information, on page 1215
- Information About Performing Switch Setup Configuration, on page 1215
- How to Perform Switch Setup Configuration, on page 1223
- Monitoring Switch Setup Configuration, on page 1232
- Configuration Examples for Performing Switch Setup, on page 1236
- Additional References For Performing Switch Setup, on page 1237
- Feature History and Information For Performing Switch Setup Configuration, on page 1238

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Performing Switch Setup Configuration

Review the sections in this module before performing your initial switch configuration tasks that include IP address assignments and DHCP autoconfiguration.

Switch Boot Process

To start your switch, you need to follow the procedures in the hardware installation guide for installing and powering on the switch and setting up the initial switch configuration (IP address, subnet mask, default gateway, secret and Telnet passwords, and so forth).

The normal boot process involves the operation of the boot loader software and includes these activities:

- Performs low-level CPU initialization. It initializes the CPU registers, which control where physical memory is mapped, its quantity, its speed, and so forth.
- Performs power-on self-test (POST) for the CPU subsystem and tests the system DRAM.
- Initializes the file systems on the system board.
• Loads a default operating system software image into memory and boots up the switch.

The boot loader provides access to the file systems before the operating system is loaded. Normally, the boot loader is used only to load, decompress, and start the operating system. After the boot loader gives the operating system control of the CPU, the boot loader is not active until the next system reset or power-on.

The boot loader also provides trap-door access into the system if the operating system has problems serious enough that it cannot be used. The trap-door mechanism provides enough access to the system so that if it is necessary, you can reinstall the operating system software image by using the Xmodem Protocol, recover from a lost or forgotten password, and finally restart the operating system.

Before you can assign switch information, make sure you have connected a PC or terminal to the console port or a PC to the Ethernet management port, and make sure you have configured the PC or terminal-emulation software baud rate and character format to match these of the switch console port:

• Baud rate default is 9600.
• Data bits default is 8.

*Note* If the data bits option is set to 8, set the parity option to none.

• Stop bits default is 2 (minor).
• Parity settings default is none.

**Software Installer Features**

The following software installer features are supported on your switch:

• Software bundle installation on a standalone switch.
• Software rollback to a previously installed package set.
• Emergency installation in the event that no valid installed packages reside on the boot flash.

**Software Boot Modes**

Your switch supports two modes to boot the software packages:

• Installed mode
• Bundle mode

**Related Topics**

Examples: Displaying Software Bootup in Install Mode, on page 1232
Example: Emergency Installation, on page 1234

**Installed Boot Mode**

You can boot your switch in installed mode by booting the software package provisioning file that resides in flash:
Switch: `boot flash:packages.conf`

The provisioning file contains a list of software packages to boot, mount, and run. The ISO file system in each installed package is mounted to the root file system directly from flash.

---

**Note**

The packages and provisioning file used to boot in installed mode must reside in flash. Booting in installed mode from usbflash0: or tftp: is not supported.

---

**Related Topics**

- Examples: Displaying Software Bootup in Install Mode, on page 1232
- Example: Emergency Installation, on page 1234

---

### Bundle Boot Mode

You can boot your switch in bundle boot mode by booting the bundle (.bin) file:

```
controller: boot flash:ct5700-ipservicesk9.SSA.03.09.07.EMP.150-9.07.EMP.bin
```

The provisioning file contained in a bundle is used to decide which packages to boot, mount, and run. Packages are extracted from the bundle and copied to RAM. The ISO file system in each package is mounted to the root file system.

Unlike install boot mode, additional memory that is equivalent to the size of the bundle is used when booting in bundle mode.

---

**Note**

Auto install and smart install functionality is not supported in bundle boot mode.

---

**Note**

The AP image predownload feature is not supported in bundle boot mode.

---

**Related Topics**

- Examples: Displaying Software Bootup in Install Mode, on page 1232
- Example: Emergency Installation, on page 1234

---

### Switches Information Assignment

You can assign IP information through the switch setup program, through a DHCP server, or manually.

Use the switch setup program if you want to be prompted for specific IP information. With this program, you can also configure a hostname and an enable secret password.

It gives you the option of assigning a Telnet password (to provide security during remote management) and configuring your switch as a command or member switch of a cluster or as a standalone switch.

Use a DHCP server for centralized control and automatic assignment of IP information after the server is configured.
If you are using DHCP, do not respond to any of the questions in the setup program until the switch receives the dynamically assigned IP address and reads the configuration file.

If you are an experienced user familiar with the switch configuration steps, manually configure the switch. Otherwise, use the setup program described in the Boot Process section.

**DHCP-Based Autoconfiguration Overview**

DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and an operation for allocating network addresses to devices. DHCP is built on a client-server model, in which designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices. The switch can act as both a DHCP client and a DHCP server.

During DHCP-based autoconfiguration, your switch (DHCP client) is automatically configured at startup with IP address information and a configuration file.

With DHCP-based autoconfiguration, no DHCP client-side configuration is needed on your switch. However, you need to configure the DHCP server for various lease options associated with IP addresses.

If you want to use DHCP to relay the configuration file location on the network, you might also need to configure a Trivial File Transfer Protocol (TFTP) server and a Domain Name System (DNS) server.

The DHCP server for your switch can be on the same LAN or on a different LAN than the switch. If the DHCP server is running on a different LAN, you should configure a DHCP relay device between your switch and the DHCP server. A relay device forwards broadcast traffic between two directly connected LANs. A router does not forward broadcast packets, but it forwards packets based on the destination IP address in the received packet.

DHCP-based autoconfiguration replaces the BOOTP client functionality on your switch.

**DHCP Client Request Process**

When you boot up your switch, the DHCP client is invoked and requests configuration information from a DHCP server when the configuration file is not present on the switch. If the configuration file is present and the configuration includes the `ip address dhcp` interface configuration command on specific routed interfaces, the DHCP client is invoked and requests the IP address information for those interfaces.

This is the sequence of messages that are exchanged between the DHCP client and the DHCP server.

*Figure 71: DHCP Client and Server Message Exchange*

The client, Switch A, broadcasts a DHCPDISCOVER message to locate a DHCP server. The DHCP server offers configuration parameters (such as an IP address, subnet mask, gateway IP address, DNS IP address, a lease for the IP address, and so forth) to the client in a DHCPOFFER unicast message.
In a DHCPREQUEST broadcast message, the client returns a formal request for the offered configuration information to the DHCP server. The formal request is broadcast so that all other DHCP servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client.

The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client. With this message, the client and server are bound, and the client uses configuration information received from the server. The amount of information the switch receives depends on how you configure the DHCP server.

If the configuration parameters sent to the client in the DHCPOFFER unicast message are invalid (a configuration error exists), the client returns a DHCPDECLINE broadcast message to the DHCP server.

The DHCP server sends the client a DHCPNAK denial broadcast message, which means that the offered configuration parameters have not been assigned, that an error has occurred during the negotiation of the parameters, or that the client has been slow in responding to the DHCPOFFER message (the DHCP server assigned the parameters to another client).

A DHCP client might receive offers from multiple DHCP or BOOTP servers and can accept any of the offers; however, the client usually accepts the first offer it receives. The offer from the DHCP server is not a guarantee that the IP address is allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address. If the switch accepts replies from a BOOTP server and configures itself, the switch broadcasts, instead of unicasts, TFTP requests to obtain the switch configuration file.

The DHCP hostname option allows a group of switches to obtain hostnames and a standard configuration from the central management DHCP server. A client (switch) includes in its DCHPDISCOVER message an option 12 field used to request a hostname and other configuration parameters from the DHCP server. The configuration files on all clients are identical except for their DHCP-obtained hostnames.

If a client has a default hostname (the hostname name global configuration command is not configured or the no hostname global configuration command is entered to remove the hostname), the DHCP hostname option is not included in the packet when you enter the ip address dhcp interface configuration command. In this case, if the client receives the DCHP hostname option from the DHCP interaction while acquiring an IP address for an interface, the client accepts the DHCP hostname option and sets the flag to show that the system now has a hostname configured.

**DHCP Server Configuration Guidelines**

Follow these guidelines if you are configuring a device as a DHCP server:

- You should configure the DHCP server with reserved leases that are bound to each switch by the switch hardware address.
- If you want the switch to receive IP address information, you must configure the DHCP server with these lease options:
  - IP address of the client (required)
  - Subnet mask of the client (required)
  - DNS server IP address (optional)
  - Router IP address (default gateway address to be used by the switch) (required)
If you want the switch to receive the configuration file from a TFTP server, you must configure the DHCP server with these lease options:

- TFTP server name (required)
- Boot filename (the name of the configuration file that the client needs) (recommended)
- Hostname (optional)

Depending on the settings of the DHCP server, the switch can receive IP address information, the configuration file, or both.

If you do not configure the DHCP server with the lease options described previously, it replies to client requests with only those parameters that are configured. If the IP address and the subnet mask are not in the reply, the switch is not configured. If the router IP address or the TFTP server name are not found, the switch might send broadcast, instead of unicast, TFTP requests. Unavailability of other lease options does not affect autoconfiguration.

The switch can act as a DHCP server. By default, the Cisco IOS DHCP server and relay agent features are enabled on your switch but are not configured. (These features are not operational.)

Purpose of the TFTP Server

Based on the DHCP server configuration, the switch attempts to download one or more configuration files from the TFTP server. If you configured the DHCP server to respond to the switch with all the options required for IP connectivity to the TFTP server, and if you configured the DHCP server with a TFTP server name, address, and configuration filename, the switch attempts to download the specified configuration file from the specified TFTP server.

If you did not specify the configuration filename, the TFTP server, or if the configuration file could not be downloaded, the switch attempts to download a configuration file by using various combinations of filenames and TFTP server addresses. The files include the specified configuration filename (if any) and these files: network-config, cisconet.cfg, hostname.config, or hostname.cfg, where hostname is the switch’s current hostname. The TFTP server addresses used include the specified TFTP server address (if any) and the broadcast address (255.255.255.255).

For the switch to successfully download a configuration file, the TFTP server must contain one or more configuration files in its base directory. The files can include these files:

- The configuration file named in the DHCP reply (the actual switch configuration file).
- The network-config or the cisconet.cfg file (known as the default configuration files).
- The router-config or the ciscorrr.cfg file (These files contain commands common to all switches. Normally, if the DHCP and TFTP servers are properly configured, these files are not accessed.)

If you specify the TFTP server name in the DHCP server-lease database, you must also configure the TFTP server name-to-IP-address mapping in the DNS-server database.

If the TFTP server to be used is on a different LAN from the switch, or if it is to be accessed by the switch through the broadcast address (which occurs if the DHCP server response does not contain all the required information described previously), a relay must be configured to forward the TFTP packets to the TFTP server. The preferred solution is to configure the DHCP server with all the required information.
Purpose of the DNS Server

The DHCP server uses the DNS server to resolve the TFTP server name to an IP address. You must configure the TFTP server name-to-IP address map on the DNS server. The TFTP server contains the configuration files for the switch.

You can configure the IP addresses of the DNS servers in the lease database of the DHCP server from where the DHCP replies will retrieve them. You can enter up to two DNS server IP addresses in the lease database. The DNS server can be on the same LAN or on a different LAN from the switch. If it is on a different LAN, the switch must be able to access it through a router.

How to Obtain Configuration Files

Depending on the availability of the IP address and the configuration filename in the DHCP reserved lease, the switch obtains its configuration information in these ways:

- The IP address and the configuration filename is reserved for the switch and provided in the DHCP reply (one-file read method).

  The switch receives its IP address, subnet mask, TFTP server address, and the configuration filename from the DHCP server. The switch sends a unicast message to the TFTP server to retrieve the named configuration file from the base directory of the server and upon receipt, it completes its boot up process.

- The IP address and the configuration filename is reserved for the switch, but the TFTP server address is not provided in the DHCP reply (one-file read method).

  The switch receives its IP address, subnet mask, and the configuration filename from the DHCP server. The switch sends a broadcast message to a TFTP server to retrieve the named configuration file from the base directory of the server, and upon receipt, it completes its boot-up process.

- Only the IP address is reserved for the switch and provided in the DHCP reply. The configuration filename is not provided (two-file read method).

  The switch receives its IP address, subnet mask, and the TFTP server address from the DHCP server. The switch sends a unicast message to the TFTP server to retrieve the network-config or cisconet.cfg default configuration file. (If the network-config file cannot be read, the switch reads the cisconet.cfg file.)

  The default configuration file contains the hostnames-to-IP-address mapping for the switch. The switch fills its host table with the information in the file and obtains its hostname. If the hostname is not found in the file, the switch uses the hostname in the DHCP reply. If the hostname is not specified in the DHCP reply, the switch uses the default Switch as its hostname.

  After obtaining its hostname from the default configuration file or the DHCP reply, the switch reads the configuration file that has the same name as its hostname (hostname-config or hostname.cfg, depending on whether network-config or cisconet.cfg was read earlier) from the TFTP server. If the cisconet.cfg file is read, the filename of the host is truncated to eight characters.

  If the switch cannot read the network-config, cisconet.cfg, or the hostname file, it reads the router-config file. If the switch cannot read the router-config file, it reads the ciscorfr.cfg file.
The switch broadcasts TFTP server requests if the TFTP server is not obtained from the DHCP replies, if all attempts to read the configuration file through unicast transmissions fail, or if the TFTP server name cannot be resolved to an IP address.

**How to Control Environment Variables**

With a normally operating switch, you enter the boot loader mode only through the console connection configured for 9600 bps. Unplug the switch power cord, and press the **Mode** button while reconnecting the power cord. You can release the **Mode** button after all the amber system LEDs turn on and remain solid. The boot loader switch prompt then appears.

The switch boot loader software provides support for nonvolatile environment variables, which can be used to control how the boot loader, or any other software running on the system, operates. Boot loader environment variables are similar to environment variables that can be set on UNIX or DOS systems.

Environment variables that have values are stored in flash memory outside of the flash file system.

Each line in these files contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not present; it has a value if it is listed even if the value is a null string. A variable that is set to a null string (for example, “”) is a variable with a value. Many environment variables are predefined and have default values.

You can change the settings of the environment variables by accessing the boot loader or by using Cisco IOS commands. Under normal circumstances, it is not necessary to alter the setting of the environment variables.

**Scheduled Reload of the Software Image**

You can schedule a reload of the software image to occur on the switch at a later time (for example, late at night or during the weekend when the switch is used less), or you can synchronize a reload network-wide (for example, to perform a software upgrade on all switches in the network).

You have these reload options:

- Reload of the software to take affect in the specified minutes or hours and minutes. The reload must take place within approximately 24 hours. You can specify the reason for the reload in a string up to 255 characters in length.

- Reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight.

The **reload** command halts the system. If the system is not set to manually boot up, it reboots itself.

If your switch is configured for manual booting, do not reload it from a virtual terminal. This restriction prevents the switch from entering the boot loader mode and then taking it from the remote user’s control.

If you modify your configuration file, the switch prompts you to save the configuration before reloading. During the save operation, the system requests whether you want to proceed with the save if the **CONFIG_FILE** environment variable points to a startup configuration file that no longer exists. If you proceed in this situation, the system enters setup mode upon reload.
To cancel a previously scheduled reload, use the `reload cancel` privileged EXEC command.

### How to Perform Switch Setup Configuration

Using DHCP to download a new image and a new configuration to a switch requires that you configure at least two switches. One switch acts as a DHCP and TFTP server and the second switch (client) is configured to download either a new configuration file or a new configuration file and a new image file.

#### Configuring DHCP Autoconfiguration (Only Configuration File)

This task describes how to configure DHCP autoconfiguration of the TFTP and DHCP settings on an existing switch in the network so that it can support the autoconfiguration of a new switch.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><code>ip dhcp pool poolname</code></td>
<td>Creates a name for the DHCP server address pool, and enters DHCP pool configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# ip dhcp pool pool</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><code>boot filename</code></td>
<td>Specifies the name of the configuration file that is used as a boot image.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(dhcp-config)# boot config-boot.text</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td><code>network network-number mask prefix-length</code></td>
<td>Specifies the subnet network number and mask of the DHCP address pool.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(dhcp-config)# network 10.10.10.0 255.255.255.0</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td><code>default-router address</code></td>
<td>Specifies the IP address of the default router for a DHCP client.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><code>Switch(dhcp-config)# default-router 10.10.10.1</code></td>
<td>Specifies the IP address of the TFTP server.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>option 150 address</code></td>
<td>Example: <code>Switch(dhcp-config)# option 150 10.10.10.1</code></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Returns to global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> <code>tftp-server flash:filename.text</code></td>
<td>Example: <code>Switch(config)# tftp-server flash:config-boot.text</code></td>
<td></td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specifies the address of the client that will receive the configuration file.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> <code>ip address address mask</code></td>
<td>Example: <code>Switch(config-if)# ip address 10.10.10.1 255.255.255.0</code></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> <code>no switchport</code></td>
<td>Example: <code>Switch(config-if)# no switchport</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> <code>no switchport</code></td>
<td>Puts the interface into Layer 3 mode.</td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Example: <code>Switch(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
Manually Assigning IP Information to Multiple SVIs

This task describes how to manually assign IP information to multiple switched virtual interfaces (SVIs):

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>interface vlan vlan-id</td>
<td>Enters interface configuration mode, and enters the VLAN to which the IP information is assigned. The range is 1 to 4094.</td>
<td>Switch(config)# interface vlan 99</td>
</tr>
<tr>
<td>3</td>
<td>ip address ip-address subnet-mask</td>
<td>Enters the IP address and subnet mask.</td>
<td>Switch(config-vlan)# ip address 10.10.10.2 255.255.255.0</td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
<td>Switch(config-vlan)# exit</td>
</tr>
<tr>
<td>5</td>
<td>ip default-gateway ip-address</td>
<td>Enters the IP address of the next-hop router interface that is directly connected to the switch where a default gateway is being configured. The default gateway receives IP packets with unresolved destination IP addresses from the switch. Once the default gateway is configured, the switch has connectivity to the remote networks with which a host needs to communicate.</td>
<td>Switch(config)# ip default-gateway 10.10.10.1</td>
</tr>
</tbody>
</table>

**Note**

- When your switch is configured to route with IP, it does not need to have a default gateway set.
- The switch capwap relays on default-gateway configuration to support routed access point join the switch.
### Modifying the Switch Startup Configuration

#### Specifying the Filename to Read and Write the System Configuration

By default, the Cisco IOS software uses the `config.text` file to read and write a nonvolatile copy of the system configuration. However, you can specify a different filename, which will be loaded during the next boot cycle.

**Before you begin**

Use a standalone switch for this task.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>boot flash://file-url</td>
<td>Specifies the configuration file to load during the next boot cycle.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# boot flash://config.text</td>
<td>file-url—The path (directory) and the configuration filename. Filenames and directory names are case-sensitive.</td>
</tr>
</tbody>
</table>
### Booting the Switch in Installed Mode

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><em>(Optional) Copies the bin file (image.bin) from the FTP or TFTP server to USB flash.</em></td>
</tr>
<tr>
<td>cp source_file_path destination_file_path</td>
<td><em>(Optional) Copies the bin file (image.bin) from the FTP or TFTP server to USB flash.</em></td>
</tr>
<tr>
<td>Example:</td>
<td><em>(Optional) Copies the bin file (image.bin) from the FTP or TFTP server to USB flash.</em></td>
</tr>
<tr>
<td>Switch# copy tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to flash: cp tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37 EXP.bin</td>
<td><em>(Optional) Copies the bin file (image.bin) from the FTP or TFTP server to USB flash.</em></td>
</tr>
</tbody>
</table>

#### Note

Ensure that the `packages.conf` file is available in the expanded list.

Expands the bin file stored in flash, FTP, TFTP, HTTP, or HTTPS server on the booted switch.
### Command or Action

<table>
<thead>
<tr>
<th>Description</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copying package files</td>
<td>cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin</td>
<td>Finished expanding bundle</td>
</tr>
<tr>
<td>Package files copied</td>
<td>cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin</td>
<td></td>
</tr>
<tr>
<td>Package files copied</td>
<td>cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin</td>
<td></td>
</tr>
<tr>
<td>Finished expanding bundle</td>
<td>cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin</td>
<td></td>
</tr>
</tbody>
</table>

Expanding the bin file from Flash:

```
Controller# software expand file
flash:ct5700-ipservicesk9.SSA.03.09.37.EXP.150-9.37.EXP.bin
Controller#
```

Preparing expand operation ...

```
[1]: Expanding bundle
flash:ct5700-ipservicesk9.SSA.03.09.37.EXP.150-9.37.EXP.bin
[1]: Copying package files
[1]: Package files copied
[1]: Finished expanding bundle
flash:ct5700-ipservicesk9.SSA.03.09.37.EXP.150-9.37.EXP.bin
```
### Booting the Switch in Bundle Mode

There are several methods by which you can boot the switch—either by copying the bin file from the TFTP server and then boot the switch, or by booting the switch straight from flash or USB flash using the commands `boot flash:<image.bin>` or `boot usbflash0:<image.bin>`.

The following procedure explains how to boot the switch from the TFTP server in the bundle mode.
## Configuring a Scheduled Software Image Reload

This task describes how to configure your switch to reload the software image at a later time.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Sets the boot parameters.</td>
</tr>
</tbody>
</table>

**Example:**

```
switch:BOOT=<source path of .bin file>
controller:BOOT=<source path of .bin file>
```

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Boot the switch.</th>
</tr>
</thead>
</table>

**Example:**

```
switch: boot
```

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Verifies that the switch is in the BUNDLE mode.</th>
</tr>
</thead>
</table>

**Example:**

```
switch# show version
```

```
Switch Ports Model      SW
Version           SW Image      Mode
---------           ----------     ----
1 6            WS-C3850-6DS-S
03.09.40.EXP       ct3850-ipservicesk9
BUNDLE
```

```
controller# show version
```

```
Switch Ports Model      SW
Version           SW Image      Mode
---------           ----------     ----
1 6            WS-C5700-6DS-S
03.09.40.EXP       ct5700-k9
BUNDLE
```
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 2 | `copy running-config startup-config`  
  **Example:**  
  `copy running-config startup-config` | Saves your switch configuration information to the startup configuration before you use the `reload` command. |
| Step 3 | `reload in [hh:]mm [text]`  
  **Example:**  
  `Switch(config)# reload in 12`  
  System configuration has been modified.  
  Save? [yes/no]: y | Schedules a reload of the software to take affect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days. You can specify the reason for the reload in a string up to 255 characters in length. |
| Step 4 | `reload slot [stack-member-number]`  
  **Example:**  
  `Switch(config)# reload slot 6`  
  Proceed with reload? [confirm] y | Schedules a reload of the software in a switch stack. |
| Step 5 | `reload at hh: mm [month day | day month] [text]`  
  **Example:**  
  `Switch(config)# reload at 14:00` | Specifies the time in hours and minutes for the reload to occur.  
  **Note** Use the `at` keyword only if the switch system clock has been set (through Network Time Protocol (NTP), the hardware calendar, or manually). The time is relative to the configured time zone on the switch. To schedule reloads across several switches to occur simultaneously, the time on each switch must be synchronized with NTP. |
| Step 6 | `reload cancel`  
  **Example:**  
  `Switch(config)# reload cancel` | Cancels a previously scheduled reload. |
| Step 7 | `show reload`  
  **Example:**  
  `show reload` | Displays information about a previously scheduled reload or identifies if a reload has been scheduled on the switch. |
Monitoring Switch Setup Configuration

Example: Verifying the Switch Running Configuration

Switch# show running-config
Building configuration...

Current configuration: 1363 bytes

version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname Stack1
enable secret 5 $1$ej9.$DMUvAUNZ0AmvmgqBEzIxE0

interface gigabitethernet6/0/2
mvr type source

interface VLAN1
ip address 172.20.137.50 255.255.255.0
no ip directed-broadcast
ip default-gateway 172.20.137.1
snmp-server community private RW
snmp-server community public RO
snmp-server community private@es0 RW
snmp-server community public@es0 RO
snmp-server chassis-id 0x12

end

Examples: Displaying Software Bootup in Install Mode

This example displays software bootup in install mode:

switch: boot flash:packages.conf

Getting rest of image
Reading full image into memory....done
Reading full base package into memory...: done = 74596432
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042f354
Kernel Size : 0x318412/3245074
Initramfs Address : 0x60747768
Initramfs Size: 0xdc08e8/14420200
Compression Format: .mzip

Bootable image at @ ram:0x6042f354
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000, 0x90000000].

Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

All packages are Digitally Signed

Starting System Services

Nov 7 09:57:05 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_START: Switch 2 is starting stack discovery
Nov 7 09:59:07 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_DONE: Switch 2 has finished stack discovery
Nov 7 09:59:07 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-SWITCH_ADDED: Switch 2 has been added to the stack
Nov 7 09:59:14 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-ACTIVE_ELECTED: Switch 2 has been elected ACTIVE

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),

Version 03.09.12.EMD EARLY DEPLOYMENT ENGINEERING NOVA WEEKLY BUILD, synced to DSGS_P12_POSTPC_FLO_DBU7_NG3K_1105
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 04-Nov-12 22:53 by gereddy
License level to iosd is ipservices

This example displays software bootup in bundle mode:

```
```

Reading full image into memory.................................................done
Nova Bundle Image

Kernel Address: 0x6042ff38
Kernel Size: 0x318412/3245074
Initramfs Address: 0x6074834c
Initramfs Size: 0xdc08e8/14420200
Compression Format: .mzip
Example: Emergency Installation

This sample output is an example when the emergency-install boot command is initiated:

```
switch: emergency-install
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin
```

The bootflash will be erased during install operation, continue (y/n)? y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin)...
Reading full image into memory......................done
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042e5cc
Kernel Size : 0x318261/3244641
Initramfs Address : 0x60746830
Initramfs Size : 0xbdb09f/14356409
Compression Format: .mzip

Bootable image at @ ram:0x6042e5cc
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80100000, 0x90000000].

File "sda9:ct5850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

Initiating Emergency Installation of bundle

Downloading bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Validating bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Installing bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Verifying bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Package cat3k_caa-base.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-drivers.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-infra.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SSA.150-9.12.EMD.pkg is Digitally Signed
Package cat3k_caa-platform.SSA.03.09.12.EMD.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.

Booting...(use DDR clock 667 MHz)Initializing and Testing RAM +++@@@@####...++@@++@@++@
s

switch: emergency-install tftp://172.20.249.254/katana/ct5760.renum.bin

The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery (tftp://172.20.249.254/katana/ct5760.renum.bin)...
Loading "sda9:ct5760-recovery.bin"
Reading full image into memory......................done
Verifying image digital signature.
Nova Bundle Image
--------------------------------------
Kernel Address : 0x8b35b598
Kernel Size : 0x367550/3568976
Initramfs Address : 0x8b6c2ae8
Initramfs Size : 0xbfe484/12575876
Configuration Examples for Performing Switch Setup

Example: Configuring a Switch to Download Configurations from a DHCP Server

This example uses a Layer 3 SVI interface on VLAN 99 to enable DHCP-based autoconfiguration with a saved configuration:

```
Switch# configure terminal
Switch(config)# boot host dhcp
Switch(config)# boot host retry timeout 300
Switch(config)# banner config-save "Caution - Saving Configuration File to NVRAM May Cause You to No longer Automatically Download Configuration Files at Reboot"
Switch(config)# vlan 99
Switch(config-vlan)# interface vlan 99
Switch(config-if)# no shutdown
```
Switch(config-if)# end
Switch# show boot
BOOT path-list:
Config file: flash:/config.text
Private Config file: flash:/private-config.text
Enable Break: no
Manual Boot: no
HELPER path-list:
NVRAM/Config file
 buffer size: 32768
Timeout for Config
 Download: 300 seconds
Config Download via DHCP: enabled (next boot: enabled)
Switch#

Examples: Scheduling Software Image Reload

This example shows how to reload the software on the switch on the current day at 7:30 p.m:

Switch# reload at 19:30
Reload scheduled for 19:30:00 UTC Wed Jun 5 2013 (in 2 hours and 25 minutes)
Proceed with reload? [confirm]

This example shows how to reload the software on the switch at a future time:

Switch# reload at 02:00 jun 20
Reload scheduled for 02:00:00 UTC Thu Jun 20 2013 (in 344 hours and 53 minutes)
Proceed with reload? [confirm]

Additional References For Performing Switch Setup

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch setup commands</td>
<td>System Management Command Reference (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Boot loader commands</td>
<td>System Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Pre-download feature</td>
<td>System Management Configuration Guide (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>IOS XE DHCP configuration</td>
<td>IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Hardware installation</td>
<td>Catalyst 3850 Switch Hardware Installation Guide</td>
</tr>
</tbody>
</table>
## Feature History and Information For Performing Switch Setup Configuration

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 63

Configuring Right-To-Use Licenses

- Finding Feature Information, on page 1239
- Restrictions for Configuring RTU Licenses, on page 1239
- Information About Configuring RTU Licenses, on page 1240
- How to Configure RTU Licenses, on page 1243
- Monitoring and Maintaining RTU Licenses, on page 1247
- Configuration Examples for RTU Licensing, on page 1247
- Additional References for RTU Licensing, on page 1250
- Feature History and Information for RTU Licensing, on page 1251

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring RTU Licenses

The following are the restrictions for configuring and using RTU licenses.

- AP count licenses can be ordered and pre-activated on your switch.
- Imaged based licenses can be upgraded. AP count licenses can be deactivated and moved between switches and controllers.
- To activate a license, you must reboot your switch after configuring the new license level. The AP-count license does not require a reboot to activate.
- An expired evaluation license can not be reactivated after reboot.
- Stack members of a switch stack must run the same license level. If the license level is different, the switch will not join the stack until it is changed and rebooted from the active switch of the stack.
• When you downgrade the license level from an image with add-on licenses to an image without add-ons, the base license level is retained after downgrade. When you upgrade back to the image with the add-ons, the base license level is retained but the add-ons are not activated.

• Adder AP-count licenses are installed in the factory.

Related Topics
Activating an Image Based License, on page 1243
Examples: Activating RTU Image Based Licenses, on page 1247

Information About Configuring RTU Licenses

Right-To-Use Licensing

Right-to-use (RTU) licensing allows you to order and activate a specific license type and level, and then to manage license usage on your switch. The types of licenses available to order by duration are:

• Permanent licenses—For image-based licenses only. Purchased with a specific feature set with no expiration date.

• Term licenses—For add-on licenses only. Purchased with a feature set for a specific subscription period of 3, 5, or 7 years. The expiration date displays on Cisco Smart Software Manager (Cisco SSM).

• Evaluation licenses—Available with image-based and add-on licenses. Pre-installed on the switch and is valid for only a 90 day in-use period.

To activate a permanent or evaluation license, you are required to accept the End-User License Agreement (EULA).

A permanent license can be moved from one device to another. To activate a license, you must reboot your switch.

Term license expiry information is available only on Cisco SSM. To get started, create a Smart Account. Go to software.cisco.com → Administration → Request Smart Account. For more information, see: http://www.cisco.com/en/us/buy/smart-accounts/software-licensing.html

If you activate the evaluation license, it will expire in 90 days. An evaluation license is a manufacturing image on your switch and is not transferable to another switch. Once activated, this type of license cannot be deactivated until it expires. After your evaluation period expires, at the next reload your switch image will return to its default license and network operations are not impacted.

Related Topics
Activating an Image Based License, on page 1243
Examples: Activating RTU Image Based Licenses, on page 1247

Right-To-Use Image-Based Licenses

Right-to-use image licenses support a set of features based on a specific image-based license:

• LAN Base—Layer 2 features.
• IP Base—Layer 2 and Layer 3 features.
• IP Services—Layer 2, Layer 3, and IPv6 features. (Applicable only to switches and not controllers.)

Right-To-Use License States

After you configure a specific license type and level, you can manage your licenses by monitoring the license state.

<table>
<thead>
<tr>
<th>License State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active, In Use</td>
<td>EULA was accepted and the license is in use after device reboot.</td>
</tr>
<tr>
<td>Active, Not In Use</td>
<td>EULA was accepted and the switch is ready to use when the license is enabled.</td>
</tr>
<tr>
<td>Not Activated</td>
<td>EULA was not accepted.</td>
</tr>
</tbody>
</table>

Guidelines to follow when monitoring your image based license state:

• A purchased permanent license is set to Active, In Use state only after a switch reboot.

• If more than one license was purchased, a reboot will activate the license with the highest feature set. For instance, the IP Services license is activated and not the LAN Base license.

• Remaining licenses purchased after switch reboot, stay in Active, Not In Use state.

Note: For the AP count license, to change the state to Active, In Use, you must first make sure that the evaluation AP count license is deactivated.

License Activation for Switch Stacks

Right-to-use licensing is supported on switch stacks. One switch in the stack is identified as the active switch and the remaining switches are standby switches. The active switch is activated with an RTU license from its active console. The license level for the standby switches in the stack can be activated at the same time.

Note: A switch stack cannot contain mixed license levels. Also, the switches must be of the same platform.

To change the license level, you do not need to disconnected the new added stack member if the stack cables are connected. Use the active switch console to set the new member's license level same as active switch and reboot the new member to join the stack.
Mobility Controller Mode

AP-count licenses are used only when the switch is in Mobility Controller mode. The MC is the gatekeeper for tracking the AP-count licenses and allows an access point to join or not.

Management of AP-count licenses is performed by the switch in mobility controller mode configurable through the CLI.

Right-To-Use AP-Count Licensing

Right-to-use licensing (RTU) allows you to order and activate a specific license type, and then to manage license usage on your switch.

You can order your switch with support for a specific number of adder access point count licenses, but the total number of licenses ordered should not exceed 501000. You can also order your adder access point count licenses after receiving the switch.

For example, if you have ordered 50700 new adder licenses, you can add only those ordered adder licenses to the switch. The licenses can be added in increments of 1, but the total number of licenses added for the switch should not exceed 50 1000.

You can configure switch to manage the access point count licenses from the CLI and view the number of access points currently in use from both the CLI and GUI.

You can configure your switch to manage the access point count licenses and view the number of access points currently in use from the CLI.

The following are two different types of access point licenses:

1. Permanent licenses for the access points
   - Adder access point count license—You can purchase the adder license to increase the switch capacity at a later time. You can transfer the adder access point count license from one switch to another.

2. Evaluation licenses for the access points
   - You can activate these licenses to evaluate more access points before purchasing the licenses.
   - The maximum number of access points that can be evaluated is 50 1000.
   - The evaluation period for using the access point licenses is 90 days.
   - You can activate and deactivate the evaluation licenses from the CLI.

Related Topics

Activating an AP-Count License, on page 1245
Obtaining an Upgrade or Capacity Adder License, on page 1245
Rehosting a License, on page 1246

Right-to-Use AP-Count Evaluation Licenses

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license...
with a 50-access-point count and want to try an evaluation license with a 100-access-point count, you can try out the evaluation license for 90 days.

When an evaluation license is activated, the permanent AP-count licenses are ignored. The maximum supported licenses of 1000 access points are available for 90 days.

To prevent disruptions in operation, the switch does not change licenses when an evaluation license expires. A warning expiry message is displayed daily starting five days prior to the expiry date. After 90 days, the evaluation license expires with a warning message. You must disable the evaluation license and then purchase the permanent license.

When the switch reboots after the evaluation license expiry, the license defaults to a permanent license.

**Related Topics**

- Activating an AP-Count License, on page 1245
- Obtaining an Upgrade or Capacity Adder License, on page 1245
- Rehosting a License, on page 1246

**Right-To-Use Adder AP-Count Rehosting Licenses**

Revoking a license from one device and installing it on another is called rehosting. You might want to rehost a license to change the purpose of a device. For example, if you want to move your Office Extend or indoor access points to a different switch, you could transfer the adder ap-count license from one switch to another.

To rehost a license, you must deactivate the adder ap-count license from one device and activate the same license on another device.

Evaluation licenses cannot be rehosted.

**How to Configure RTU Licenses**

**Activating an Image Based License**

To activate image based licenses, complete the following task:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>license right-to-use activate {ipbase</td>
<td>Activates the license level. Activation can happen on all switches and also include the EULA acceptance.</td>
</tr>
<tr>
<td></td>
<td>ipservices</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>[slot slot-number] [acceptEULA]</td>
<td>Note</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# license right-to-use activate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ipservices all acceptEULA</td>
<td></td>
</tr>
</tbody>
</table>
Purpose

Command or Action

Reloads a specific stack member to complete the activation process for the RTU adder AP-count license.

---

**Step 2**

```bash
reload [ LINE | at | cancel | in | slot stack-member-number | standby-cpu ]
```

**Example:**

Switch# reload slot 1
Proceed with reload? [confirm] y

*Note* The reminder to accept the EULA is displayed after reload if it was not accepted earlier.

When changing license level, you are not required to save the configuration. But, it is a good practice to ensure all the configuration is stored properly before reload. Changing from a higher license level to a lower license level on reboot will remove CLIs that are not applicable. Ensure that all features in the lower license level that are actively used are not removed.

---

**Step 3**

```bash
show license right-to-use usage [ slot slot-number ]
```

**Example:**

Switch# show license right-to-use usage

<table>
<thead>
<tr>
<th>Slot#</th>
<th>License Name</th>
<th>Type</th>
<th>usage-duration(y:m:d)</th>
<th>In-Use</th>
<th>EULA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ipservices</td>
<td>Permanent</td>
<td>0:10:27</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1</td>
<td>ipservices</td>
<td>Evaluation</td>
<td>0:0:0</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>1</td>
<td>ipbase</td>
<td>Permanent</td>
<td>0:0:0:9</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1</td>
<td>ipbase</td>
<td>Evaluation</td>
<td>0:0:0</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>1</td>
<td>lanbase</td>
<td>Permanent</td>
<td>0:11:12</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

Switch#

---

Related Topics

- [Restrictions for Configuring RTU Licenses](#), on page 1239
- [Right-To-Use Licensing](#), on page 1240
- [Monitoring and Maintaining RTU Licenses](#), on page 1247
- [Examples: Activating RTU Image Based Licenses](#), on page 1247
Activating an AP-Count License

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activates one or more adder AP-count licenses and immediately accepts the EULA.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example:

Switch# license right to use activate apcount 5 slot 1 acceptEULA

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays detailed usage information.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example:

Switch# show license right-to-use usage

| Slot# | License Name | Type | usage-duration(y|m|d) | In-Use | EULA |
|-------|--------------|------|----------------------|--------|------|
| 1     | ipservices   | permanent | 0:3                 | yes    | yes  |
| 1     | ipservices   | evaluation | 0:0                 | no     | no   |
| 1     | ipbase       | permanent | 0:0                 | no     | no   |
| 1     | ipbase       | evaluation | 0:0                 | no     | no   |
| 1     | lanbase      | permanent | 0:0                 | no     | no   |
| 1     | lanbase      | evaluation | 0:0                 | no     | no   |
| 1     | lanbase      | adder | 0:0                 | no     | no   |
| 1     | lanbase      | base | 0:0                 | yes    | yes  |

Related Topics

- Monitoring and Maintaining RTU Licenses, on page 1247
- Right-To-Use AP-Count Licensing, on page 1242
- Right-to-Use AP-Count Evaluation Licenses, on page 1242

Obtaining an Upgrade or Capacity Adder License

You can use the capacity adder licenses to increase the number of access points supported by the switch.
## Rehosting a License

To rehost a license, you have to deactivate the license from one switch and then activate the same license on another switch.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>`license right-to-use [activate</td>
<td>deactivate]`</td>
</tr>
<tr>
<td>`apcount [ap-number</td>
<td>evaluation] slot slot-num [ acceptEULA]`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# <code>license right to use activate apcount 5 slot 2 acceptEULA</code></td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics
- Right-to-Use AP-Count Evaluation Licenses, on page 1242
- Right-To-Use AP-Count Licensing, on page 1242

---

## Deactivating a License

To deactivate a license, you have to deactivate the license on one switch and then activate the same license on another switch.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>`license right-to-use deactivate [license-level] apcount [ap-number</td>
<td>evaluation] slot slot-num`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# <code>license right to use deactivate apcount 1 slot 1</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# <code>license right-to-use deactivate ipbase slot 1</code></td>
<td></td>
</tr>
<tr>
<td>OR</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** |         |
| `license right-to-use activate [license-level] slot slot-num [ acceptEULA]` | Activates the license on another switch. The IP Base license level is rehosted on slot 2 in the example here. |
| Example: |         |
| Switch# `license right to use activate ipbase slot 2 acceptEULA` |         |
| Example: |         |
| Switch# `license right to-use activate ipbase slot 2 acceptEULA` |         |

### Related Topics
- Right-To-Use AP-Count Licensing, on page 1242
- Right-to-Use AP-Count Evaluation Licenses, on page 1242
Monitoring and Maintaining RTU Licenses

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show license right-to-use default</td>
<td>Displays the default license information.</td>
</tr>
<tr>
<td>show license right-to-use detail</td>
<td>Displays detailed information of all the licenses in the switch stack.</td>
</tr>
<tr>
<td>show license right-to-use eula {evaluation</td>
<td>permanent} show license right-to-use eula {evaluation</td>
</tr>
<tr>
<td>show license right-to-use mismatch</td>
<td>Displays the license information that does not match.</td>
</tr>
<tr>
<td>show license right-to-use slot slot-number</td>
<td>Displays the license information for a specific slot in a switch stack.</td>
</tr>
<tr>
<td>show license right-to-use summary</td>
<td>Displays a summary of the license information on the entire switch stack.</td>
</tr>
<tr>
<td>show license right-to-use usage [ slot slot-number ]</td>
<td>Displays detailed information about usage for all licenses in the switch stack.</td>
</tr>
<tr>
<td>show switch</td>
<td>Displays detailed information of every member in a switch stack including the state of the license.</td>
</tr>
</tbody>
</table>

Related Topics

Activating an Image Based License, on page 1243
Examples: Activating RTU Image Based Licenses, on page 1247
Activating an AP-Count License, on page 1245

Configuration Examples for RTU Licensing

Examples: Activating RTU Image Based Licenses

This example shows how to activate an IP Services image license and accept the EULA for a specific slot:

Switch# license right-to-use activate ipservices slot 1 acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level

This example shows how to activate a license for evaluation:

Switch# license right-to-use activate ipservices evaluation acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
Related Topics

- Activating an Image Based License, on page 1243
- Restrictions for Configuring RTU Licenses, on page 1239
- Right-To-Use Licensing, on page 1240
- Monitoring and Maintaining RTU Licenses, on page 1247

Examples: Displaying RTU Licensing Information

This example shows the consolidated RTU licensing information from the active switch on a switch stack. All of the members in the stack have the same license level. When the evaluation AP-count license is activated, the adder AP-count licenses are ignored. The maximum number of AP-count licenses are available when evaluation is enabled.

```
Switch# show license right-to-use summary
License Name  Type  Period left
----------------------------------------
ipservices    Permanent  Lifetime
----------------------------------------
License Level In Use: ipservices
License Level on Reboot: ipservices
```

This example shows a summary of permanent and adder licenses. The evaluation AP-count license is disabled displaying the total number of activated adder AP-count licenses in the switch stack. AP-count licenses in-use mean that they are connected.

```
Switch# show license right-to-use summary
License Name  Type  Count  Period left
---------------------------------------------------------------------
ipservices    permanent  N/A  Lifetime
apcount    base  0
apcount    adder  40  Lifetime
---------------------------------------------------------------------
License Level In Use: ipservices
License Level on Reboot: ipservices eval
Evaluation AP-Count: Disabled
Total AP Count Licenses: 40
AP Count Licenses In-use: 10
AP Count Licenses Remaining: 30
```

This example shows the RTU default licenses. Default licenses are pre-installed and cannot be removed or transferred. If no license is activated the switch uses the default license, after a reboot.

```
Switch# show license right-to-use default
Slot#  License Name  Type
-------------------------------------
1  lanbase Permanent
-------------------------------------
```
This example shows the consolidated RTU licensing information of the controller. When the evaluation ap-count license is activated, the base and adder ap-count licenses are ignored. The maximum number of ap-count licenses are available when evaluation is enabled.

This example shows the RTU default licenses. Default licenses are pre-installed and cannot be removed or transferred. If no license is activated the controller uses the default license, after a reboot.

```
controller# show license right-to-use default
Slot# License Name Type Count
----------------------------------------------------
 1     apcount     base     10
```

**Example: Displaying RTU License Details**

This example shows all the detailed information for the RTU licenses on slot 1:

```
Controller# show license right-to-use detail slot 1
Index 6: License Name: apcount
  Period left: Expired
  License Type: evaluation
  License State: Active, In use
  License Count: 1000
  License Location: Slot 1
Index 7: License Name: apcount
  Period left: Lifetime
  License Type: base
  License State: Active, Not In use
  License Count: 0
  License Location: Slot 1
Index 8: License Name: apcount
  Period left: Lifetime
  License Type: adder
  License State: Not Activated
  License Count: 0
  License Location: Slot 1
```

**Example: Displaying RTU License Mismatch**

This example shows the license information of the switches in a stack and a mismatch state of a member switch. The member must match the active.

```
Switch# show switch
```
Switch/Stack Mac Address: 1c1d.8625.7700 - Local Mac Address

<table>
<thead>
<tr>
<th>Switch#</th>
<th>Role</th>
<th>Mac Address</th>
<th>Priority</th>
<th>Version</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active</td>
<td>1c1d.8625.7700</td>
<td>15</td>
<td>V02</td>
<td>Ready</td>
</tr>
<tr>
<td>2</td>
<td>Standby</td>
<td>bc16.f55c.ab80</td>
<td>7</td>
<td>V04</td>
<td>Ready</td>
</tr>
<tr>
<td>3</td>
<td>Member</td>
<td>580a.2095.da00</td>
<td>1</td>
<td>V03</td>
<td>Lic-Mismatch</td>
</tr>
</tbody>
</table>

Note: To resolve the license mismatch, first check the RTU license summary:

Switch# show license right-to-use

Then change the license level of the mismatched switch so that it is the same license level of the active switch. This example shows that the IP Base license was activated for the member switch to match the active switch.

Switch# license right-to-use activate ipbase slot 3 acceptEULA

Example: Displaying RTU Licensing Usage

This example shows the detailed licensing usage on your controller.

Controller# show license right-to-use usage

<table>
<thead>
<tr>
<th>Slot#</th>
<th>License Name</th>
<th>Type</th>
<th>usage-duration(y:m:d)</th>
<th>In-Use</th>
<th>EULA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>apcount</td>
<td>evaluation</td>
<td>0 :3 :3</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1</td>
<td>apcount</td>
<td>base</td>
<td>0 :0 :0</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1</td>
<td>apcount</td>
<td>adder</td>
<td>0 :0 :0</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>

Additional References for RTU Licensing

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>For complete syntax and usage information for the commands used in this chapter.</td>
<td>System Management Command Reference (Catalyst 3850 Switches)System Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>RTU AP image preload feature</td>
<td>System Management Configuration Guide (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>
### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

### Feature History and Information for RTU Licensing

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>Support for add-on licensing options (DNA Essentials and DNA Advantage) were introduced.</td>
</tr>
</tbody>
</table>
Configuring Administrator Usernames and Passwords

- Finding Feature Information, on page 1253
- Information About Configuring Administrator Usernames and Passwords, on page 1253
- Configuring Administrator Usernames and Passwords, on page 1254
- Examples: Administrator Usernames and Passwords Configuration, on page 1256
- Additional References for Administrator Usernames and Passwords, on page 1257
- Feature History and Information For Performing Administrator Usernames and Passwords Configuration, on page 1257

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Administrator Usernames and Passwords

You can configure administrator usernames and passwords to prevent unauthorized users from reconfiguring the switch and viewing configuration information. This section provides instructions for initial configuration and for password recovery.

You can also set administrator usernames and passwords to manage and configure one or more access points that are associated with the switch.

Strong Passwords

You can set strong administrator passwords such as encrypted passwords with ASCII keys for the administrator user for managing access points.

Use the following guidelines while creating strong passwords:
• There should be at least three of the following categories—lowercase letters, uppercase letters, and digits, and special characters.

Note Special characters are not supported for username and password for GUI login.

• The new password should not be the same as that of the associated username and the username should not be reversed.

• The characters in the password should not be repeated more than three times consecutively.

• The password should not be \textbf{cisco}, \textbf{ocsic}, \textbf{admin}, \textbf{nimda}, or any variant obtained by changing the capitalization of letters therein, or by substituting "1" "1" or "!" for i, and/or substituting "0" for "o", and/or substituting "$" for "s".

• The maximum number of characters accepted for the username and password is 32.

\textbf{Encrypted Passwords}

You can set three types of keys for the password:

• Randomly generated key—This key is generated randomly and it is the most secure option. To export the configuration file from one system to another, the key should also be exported.

• Static key—The simplest option is to use a fixed (static) encryption key. By using a fixed key, no key management is required, but if the key is somehow discovered, the data can be decrypted by anyone with the knowledge of that key. This is not a secure option and it is called obfuscation in the CLI.

• User defined key—You can define the key by yourself. To export the configuration file from one system to another, both systems should have the same key configured.

\textbf{Note}

When you configure the \textbf{ap mgmtuser username} and \textbf{ap dot1x username} commands, the system encrypts the password automatically when password encryption aes is enabled and the encryption key is configured with the \textbf{key config-key password-encrypt} command. If an already-encrypted password is entered (that is, type 8), then it must be one that has been encrypted with the currently stored key. If the key of the encrypted password does not match the currently stored key, the encrypted password is rejected. In such case, you can enter the password in plain text (that is, type 0) and allow the system to encrypt it automatically.

\section*{Configuring Administrator Usernames and Passwords}

\textbf{Procedure}

\begin{tabular}{|c|c|}
\hline
\textbf{Step 1} & \textbf{Command or Action} \\
\hline
 & configure terminal \\
\hline
Example: & Switch\# configure terminal \\
\hline
 & Purpose \\
\hline
 & Enters global configuration mode. \\
\hline
\end{tabular}
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables strong password policy for the administrator user.</td>
</tr>
<tr>
<td>wireless security strong-password</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config)# wireless security strong-password</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies a username and password for an administrator. The administrator can configure the switch and view the configured information.</td>
</tr>
<tr>
<td>username admin-username password</td>
<td></td>
</tr>
<tr>
<td>{0 unencrypted_password</td>
<td>7 hidden_password</td>
</tr>
<tr>
<td>Example: Switch(config)# username adminuser1 password 0 Qzsek239@</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies the secret for the administrator.</td>
</tr>
<tr>
<td>username admin-username secret</td>
<td></td>
</tr>
<tr>
<td>{0 unencrypted_secret_text</td>
<td>4 SHA256 encrypted_secret_text</td>
</tr>
<tr>
<td>Example: Switch(config)# username adminuser1 secret 0 Qzsek239@</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specifies administrator username and password for managing all of the access points configured to the switch. You can also include the secret text to perform privileged access point management.</td>
</tr>
<tr>
<td>ap mgmtuser username username password</td>
<td></td>
</tr>
<tr>
<td>{0 unencrypted_password</td>
<td>8 AES encrypted password } secret {0 unencrypted_password</td>
</tr>
<tr>
<td>Example: Switch(config)# ap mgmtuser username cisco password 0 Qwcii12@ secret 0 Qwcii14@!</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Specifies the 802.1X username and password for managing all of the access points configured to the switch.</td>
</tr>
<tr>
<td>ap dot1x username username password</td>
<td></td>
</tr>
<tr>
<td>{0 unencrypted_password</td>
<td>8 AES encrypted password }</td>
</tr>
<tr>
<td>Example: Switch(config)# ap dot1x username cisco password 0 Qwcii12@</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Examples: Administrator Usernames and Passwords Configuration

This example shows how to configure administrator usernames and passwords with the strong password policy in configuration mode:

```
Switch# configure terminal
Switch(config)# wireless security strong-password
Switch(config)# username adminuser1 password 0 QZsek239@
Switch(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@
Switch(config)# ap dot1x username cisco password 0 Qwci12@
Switch# end
```

This example shows how to configure administrator usernames and passwords for an access point in global EXEC mode:

```
Switch# wireless security strong-password
Switch# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qwci12@ secret Qwci14@
Switch# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qwci12@
Switch# end
```
Additional References for Administrator Usernames and Passwords

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td><em>System Management Command Reference Guide (Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em></td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information For Performing Administrator Usernames and Passwords Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Feature History and Information For Performing Administrator Usernames and Passwords Configuration
802.11 parameters and Band Selection

- Finding Feature Information, on page 1259
- Restrictions on Band Selection, 802.11 Bands, and Parameters, on page 1259
- Information About Configuring Band Selection, 802.11 Bands, and Parameters, on page 1260
- How to Configure 802.11 Bands and Parameters, on page 1262
- Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters, on page 1272
- Configuration Examples for Band Selection, 802.11 Bands, and Parameters, on page 1276
- Additional References for 802.11 Parameters and Band Selection, on page 1278
- Feature History and Information For Performing 802.11 parameters and Band Selection Configuration, on page 1279

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions on Band Selection, 802.11 Bands, and Parameters

- Band selection-enabled WLANs do not support time-sensitive applications such as voice and video because of roaming delays.

- Band selection can be used only with Cisco Aironet 1140, 1250, 1260, 1550, 1600, 1800, 2600, 2800, 3500, 3600, 3700, 3800 Series access points.

- Mid-RSSI is not supported on Cisco Aironet 1600 Series access points.

- Band selection is not supported in Cisco Aironet 1040, OEAP 600 Series access points.

- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.
• The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.

• You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.

• It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing are enabled globally by default.

Information About Configuring Band Selection, 802.11 Bands, and Parameters

Band Selection

Band selection enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of 3 nonoverlapping channels. To prevent these sources of interference and improve overall network performance, configure band selection on the switch.

Band selection works by regulating probe responses to clients and it can be enabled on a per-WLAN basis. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels. In an access point, the band select table can be viewed by running the show dot11 band-select command. It can also be viewed by running the show cont d0/d1 | begin Lru command.

Note

The WMM default configuration is not shown in the show running-config command output.

Band Selection Algorithm

The band selection algorithm affects clients that use 2.4-GHz band. Initially, when a client sends a probe request to an access point, the corresponding client probe’s Active and Count values (as seen from the band select table) become 1. The algorithm functions based on the following scenarios:

• Scenario1—Client RSSI (as seen from the show cont d0/d1 | begin RSSI command output) is greater than both Mid RSSI and Acceptable Client RSSI.
  • Dual-band clients—No 2.4-GHz probe responses are seen at any time; 5-GHz probe responses are seen for all 5-GHz probe requests.
  • Single-band (2.4-GHz) clients—2.4-GHz probe responses are seen only after the probe suppression cycle.
  • After the client’s probe count reaches the configured probe cycle count, the algorithm waits for the Age Out Suppression time and then marks the client probe’s Active value as 0. Then, the algorithm is restarted.
- Scenario 2—Client RSSI (as seen from `show cont d0/d1 | begin RSSI`) lies between Mid-RSSI and Acceptable Client RSSI.
  - All 2.4-GHz and 5-GHz probe requests are responded to without any restrictions.
  - This scenario is similar to the band select disabled.

---

**Note**

The client RSSI value (as seen in the `sh cont d0 | begin RSSI` command output) is the average of the client packets received, and the Mid RSSI feature is the instantaneous RSSI value of the probe packets. As a result, the client RSSI is seen as weaker than the configured Mid RSSI value (7-dB delta). The 802.11b probes from the client are suppressed to push the client to associate with the 802.11a band.

### 802.11 Bands

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

When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully connect to an access point, but cannot pass traffic. When you configure the controller only for 802.11g traffic, you must mark 11g rates as mandatory.

---

**Note**

The Block Acks in a Cisco 2800, 3800, 1560 APs are sent at configured mandatory data rates in Cisco WLC for 2.4 GHz radio.

### 802.11n Parameters

This section provides instructions for managing 802.11n access points on your network. The 802.11n devices support the 2.4 and 5-GHz bands and offer high throughput data rates.

The 802.11n high throughput rates are available on all the 802.11n access points for the WLANs using WMM with no Layer 2 encryption or with WPA2/AES encryption enabled.

The 802.11n-only access points can filter out clients without high-throughput information element on the association request. The 802.11n-only access points access points reject association requests from clients without high-throughput information element (11n).

In the 802.11n high-throughput mode, there are no 802.11a/b/g stations using the same channel. The 802.11a/b/g devices cannot communicate with the 802.11n high-throughput mode access point, where as the 802.11n-only mode access point uses 802.11a/g rates for beacons or management frames.

---

**Note**

Some Cisco 802.11n APs may intermittently emit incorrect beacon frames, which can trigger false wIPS alarms. We recommend that you ignore these alarms. The issue is observed in the following Cisco 802.11n APs: 1140, 1250, 2600, 3500, and 3600.
### 802.11h Parameters

802.11h informs client devices about channel changes and can limit the transmit power of those client devices.

### How to Configure 802.11 Bands and Parameters

#### Configuring Band Selection (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Sets the probe cycle count for band select.</td>
</tr>
<tr>
<td><code>wireless client band-select cycle-count cycle_count</code></td>
<td>Valid range is between 1 and 10.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>wireless client band-select cycle-count 3</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the time threshold for a new scanning cycle period.</td>
</tr>
<tr>
<td><code>wireless client band-select cycle-threshold milliseconds</code></td>
<td>Valid range is between 1 and 1000.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>wireless client band-select cycle-threshold 5000</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Sets the suppression expire to the band select.</td>
</tr>
<tr>
<td><code>wireless client band-select expire suppression seconds</code></td>
<td>Valid range is between 10 and 200.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>wireless client band-select expire suppression 100</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Sets the dual band expire.</td>
</tr>
<tr>
<td><code>wireless client band-select expire dual-band seconds</code></td>
<td>Valid range is between 10 and 300.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>wireless client band-select expire dual-band 100</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Sets the client RSSI threshold.</td>
</tr>
<tr>
<td><code>wireless client band-select client-rssi client_rssi</code></td>
<td>Valid range is between 20 and 90.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>wireless client band-select client-rssi 40</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td><em>end</em></td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# <em>end</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>wlan wlan_profile_name wlan_ID SSID_network_name band-select</em></td>
<td>Configures band selection on specific WLANs. Valid range is between 1 and 512. You can enter up to 32 alphanumeric characters for <em>SSID_network_name</em> parameter.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# <em>wlan wlan1 25 ssid12</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-wlan)# <em>band-select</em></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>end</em></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <em>Ctrl-Z</em> to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# <em>end</em></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the 802.11 Bands (CLI)

The following procedure provides information about how to configure 802.11 bands and parameters.

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>configure terminal</em></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>ap dot11 5ghz shutdown</em></td>
<td>Disables the 802.11a band.</td>
</tr>
<tr>
<td>Note</td>
<td>You must disable the 802.11a band before configuring the 802.11a network parameters.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# ap dot11 5ghz shutdown</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>ap dot11 24ghz shutdown</em></td>
<td>Disables the 802.11b band.</td>
</tr>
<tr>
<td>Note</td>
<td>You must disable the 802.11b band before configuring the 802.11b network parameters.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# ap dot11 24ghz shutdown</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>*ap dot11 {5ghz</td>
<td>24ghz} beaconperiod time_unit*</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# ap dot11 5ghz beaconperiod 500</td>
<td></td>
</tr>
</tbody>
</table>

---

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E

1263
<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} fragmentation threshold`</td>
</tr>
</tbody>
</table>

**Example:**
```
Switch(config)# ap dot11 5ghz fragmentation 300
```

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} dtpc`</td>
</tr>
</tbody>
</table>

**Example:**
```
Switch(config)# ap dot11 5ghz dtpc
```

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>wireless client association limit number interval milliseconds</code></td>
<td>Specifies the maximum allowed clients that can be configured. You can configure the maximum number of association requests on a single access point slot at a given interval. The range of association limit that you can configure is from 1 to 100. The association request limit interval is measured between 100 to 10000 milliseconds.</td>
</tr>
</tbody>
</table>

**Example:**
```
Switch(config)# wireless client association limit 50 interval 1000
```

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} rate rate {disable</td>
</tr>
</tbody>
</table>

**Example:**
```
Switch(config)# ap dot11 5ghz rate 36 mandatory
```

- **disable**—Defines that the clients specify the data rates used for communication.
- **mandatory**—Defines that the clients support this data rate in order to associate to an access point on the controller.
- **supported**—Any associated clients that support this data rate can communicate with the access point using that rate. However, the clients are not required to use this rate in order to associate.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <em>rate</em>—Specifies the rate at which data is transmitted. For the 802.11a and 802.11b bands, the data is transmitted at the rate of 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.</td>
</tr>
<tr>
<td>Step 9 no ap dot11 5ghz shutdown</td>
<td>Enables the 802.11a band.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# no ap dot11 5ghz shutdown</td>
</tr>
<tr>
<td>Note</td>
<td>The default value is enabled.</td>
</tr>
<tr>
<td>Step 10 no ap dot11 24ghz shutdown</td>
<td>Enables the 802.11b band.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# no ap dot11 24ghz shutdown</td>
</tr>
<tr>
<td>Note</td>
<td>The default value is enabled.</td>
</tr>
<tr>
<td>Step 11 ap dot11 24ghz dot11g</td>
<td>Enables or disables 802.11g network support.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ap dot11 24ghz dot11g</td>
</tr>
<tr>
<td></td>
<td>The default value is enabled. You can use this command only if the 802.11b band is enabled.</td>
</tr>
<tr>
<td></td>
<td>If you disable this feature, the 802.11b band is enabled without 802.11g support.</td>
</tr>
<tr>
<td>Step 12 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
</tr>
</tbody>
</table>

### Configuring the 802.11 Bands (GUI)

**Procedure**

**Step 1** Choose Configuration > Wireless > 802.11a/n/ac > Network or Configuration > Wireless > 802.11b/g/n > Network to open the Global Parameters page.

**Step 2** Select the **802.11a/n/ac** (or **802.11b/g**) **Network Status** check box to enable the 802.11a or 802.11b/g band. To disable the band, unselect the check box. The default value is enabled. You can enable both the 802.11a and 802.11b/g bands.

**Step 3** If you enabled the 802.11b/g band in **Step 2**, select the **802.11g Support** check box if you want to enable 802.11g network support. The default value is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.

**Step 4** Specify the period at which the SSID is broadcast by the access point by entering a value between 20 and 1000 milliseconds (inclusive) in the Beacon Period text box. The default value is 100 milliseconds.
Note  The beacon period in controllers is listed in terms of milliseconds. The beacon period can also be measured in time units, where one time unit equals 1024 microseconds or 102.4 milliseconds. If a beacon interval is listed as 100 milliseconds in a controller, it is only a rounded off value for 102.4 milliseconds. Due to hardware limitation in certain radios, even though the beacon interval is, say 100 time units, it is adjusted to 102 time units, which roughly equals 104.448 milliseconds. When the beacon period is to be represented in terms of time units, the value is adjusted to the nearest multiple of 17.

Step 5 Specify the size at which packets are fragmented by entering a value between 256 and 2346 bytes (inclusive) in the Fragmentation Threshold text box. Enter a low number for areas where communication is poor or where there is a great deal of radio interference.

Step 6 Make access points advertise their channel and transmit power level in beacons and probe responses for CCX clients. Select the DTPC Support check box. Otherwise, unselect this check box. The default value is enabled.

Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

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

Note  DTPC and 801.11h power constraint cannot be enabled simultaneously.

Step 7 Specify the maximum allowed clients by entering a value between 1 to 200 in the Maximum Allowed Client text box. The default value is 200.

Step 8 Use the Data Rates options to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:

- 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps
- 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

For each data rate, choose one of these options:

- Mandatory—Clients must support this data rate in order to associate to an access point on the controller.
- Supported—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.
- Disabled—The clients specify the data rates used for communication.

Step 9 Click Apply.

Step 10 Click Save Configuration.
## Configuring 802.11n Parameters (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} dot11n`</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# ap dot11 5ghz dot11n</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} dot11n mcs tx rtu`</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# ap dot11 5ghz dot11n mcs tx 20</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>wlan wlan_profile_name wlan_ID SSID_network_name wmm require</code></td>
<td>Enables WMM on the WLAN and uses the 802.11n data rates that you configured. The <code>require</code> keyword requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# wlan wlan1 25 ssid12</code> <code>Switch(config-wlan)# wmm require</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} shutdown`</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# ap dot11 5ghz shutdown</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>`{ap</td>
<td>no ap} dot11 {5ghz</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# ap dot11 5ghz dot11n a-mpdu tx priority all</code></td>
<td></td>
</tr>
</tbody>
</table>

Aggregation is the process of grouping packet data frames together, rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). Both A-MPDU and A-MSDU are performed in the software.

You can specify the aggregation method for various types of traffic from the access point to the clients.

The list defines the priority levels (0-7) assigned per traffic type.

- 0—Best effort
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 1—Background</td>
<td></td>
</tr>
<tr>
<td>• 2—Spare</td>
<td></td>
</tr>
<tr>
<td>• 3—Excellent effort</td>
<td></td>
</tr>
<tr>
<td>• 4—Controlled load</td>
<td></td>
</tr>
<tr>
<td>• 5—Video, less than 100-ms latency and jitter</td>
<td></td>
</tr>
<tr>
<td>• 6—Voice, less than 100-ms latency and jitter</td>
<td></td>
</tr>
<tr>
<td>• 7—Network control</td>
<td></td>
</tr>
</tbody>
</table>

You can configure each priority level independently, or you can use all the parameters to configure all the priority levels at once. You can configure priority levels so that the traffic uses either A-MPDU transmission or A-MSDU transmission.

- When you use the **ap** command along with the other options, the traffic associated with that priority level uses A-MPDU transmission.
- When you use the **no ap** command along with the other options, the traffic associated with that priority level uses A-MSDU transmission.

Configure the priority levels to match the aggregation method used by the clients. By default, A-MPDU is enabled for priority level 0, 4, and 5, and the rest are disabled. By default, A-MPDU is enabled for all priorities except 6 and 7.

### Step 7

**no ap dot11 {5ghz | 24ghz} shutdown**

**Example:**

Switch(config)# no ap dot11 5ghz shutdown

Re-enables the network.

### Step 8

**ap dot11 {5ghz | 24ghz} dot11n guard-interval {any | long}**

**Example:**

Switch(config)# ap dot11 5ghz dot11n guard-interval long

Configures the guard interval for the network.
### Configuring the 802.11n Parameters (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 9</td>
<td>ap dot11 {5ghz</td>
<td>24ghz} dot11n rifs rx</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ap dot11 5ghz dot11n rifs rx</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring the 802.11n Parameters (GUI)**

**Step 1**
Choose **Configuration > Wireless > 802.11a/n/ac or 802.11b/g/n > High Throughput (802.11n)** to open the 802.11n/ac (5 GHz or 2.4 GHz) Throughput page.

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

**Step 3**
Select the check boxes of the desired rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. These data rates, which are calculated for a 20-MHz channel width using a short guard interval, are available:

- 0 (7 Mbps)
- 1 (14 Mbps)
- 2 (21 Mbps)
- 3 (29 Mbps)
- 4 (43 Mbps)
- 5 (58 Mbps)
- 6 (65 Mbps)
- 7 (72 Mbps)
- 8 (14 Mbps)
- 9 (29 Mbps)
- 10 (43 Mbps)
- 11 (58 Mbps)
- 12 (87 Mbps)
- 13 (116 Mbps)
- 14 (130 Mbps)
- 15 (144 Mbps)
• 16 (22 Mbps)
• 17 (43 Mbps)
• 18 (65 Mbps)
• 19 (87 Mbps)
• 20 (130 Mbps)
• 21 (173 Mbps)
• 22 (195 Mbps)
• 23 (217 Mbps)

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

**Step 4**
Click **Apply**.

**Step 5**
Use the 802.11n data rates that you configured by enabling WMM on the WLAN as follows:

a) Choose **WLANs** to open the WLANs page.
b) Click the ID number of the WLAN for which you want to configure WMM mode.
c) When the WLANs > Edit page appears, choose the **QoS** tab to open the WLANs > Edit (Qos) page.
d) From the WMM Policy drop-down list, choose **Required** or **Allowed** to require or allow client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

If you choose **Allowed**, devices that cannot support WMM can join the WLAN but will not benefit from the 802.11n rates.
e) Click **Apply**.

**Step 6**
Click **Save Configuration**.

**Note**
To determine if an access point supports 802.11n, look at the 11n Supported text box on either the 802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure page or the 802.11a/n/ac (or 802.11b/g/n) AP Interfaces > Details page.

---

### Configuring 802.11h Parameters (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> ap dot11 5ghz shutdown</td>
<td>Disables the 802.11a network.</td>
</tr>
</tbody>
</table>

**Example:**
```
Switch(config)# ap dot11 5ghz shutdown
```
### Configuring the 802.11h Parameters (GUI)

#### Procedure

**Step 1** Disable the 802.11 band as follows:
- a) Choose **Configuration > Wireless > 802.11a/n/ac > Network** to open the 802.11a/n/ac Global Parameters page.
- b) Unselect the **802.11a Network Status** check box.
- c) Click **Apply**.

**Step 2** Choose **Configuration > Wireless > 802.11a/n/ac > DFS (802.11h)** to open the 802.11h Global Parameters page.

**Step 3** In the Power Constraint area, enter the local power constraint. The valid range is between 0 dBm and 30 dBm.

**Step 4** In the Channel Switch Announcement area, enter the channel switch announcement mode. You can enter a value of either 1 or 0.

**Step 5** Click **Apply**.

**Step 6** Reenable the 802.11a band as follows:
- a) Choose **Wireless > 802.11a/n/ac > Network** to open the 802.11a/n/ac Global Parameters page.
- b) Select the **802.11a Network Status** check box.
- c) Click **Apply**.

**Step 7** Click **Save Configuration**.
Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters

Monitoring Configuration Settings Using Band Selection and 802.11 Bands Commands

The following commands can be used to monitor band selection, 802.11 bands, and parameters on the switch.

Table 90: Monitoring Configuration Settings Using Band Selection and 802.11 Band Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap dot11 5ghz network</td>
<td>Displays 802.11a band network parameters, 802.11a operational rates, 802.11n MCS settings, and 802.11n status information.</td>
</tr>
<tr>
<td>show ap dot11 24ghz network</td>
<td>Displays 802.11b band network parameters, 802.11b/g operational rates, 802.11n MCS settings, and 802.11n status information.</td>
</tr>
<tr>
<td>show wireless dot11h</td>
<td>Displays 802.11h configuration parameters.</td>
</tr>
<tr>
<td>show wireless band-select</td>
<td>Displays band-select configuration settings.</td>
</tr>
</tbody>
</table>

Example: Viewing the Configuration Settings for the 5-GHz Band

Switch# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled

802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported

802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
802.11n Status:
A-MPDU Tx:
  Priority 0 : Enabled
  Priority 1 : Disabled
  Priority 2 : Disabled
  Priority 3 : Disabled
  Priority 4 : Enabled
  Priority 5 : Enabled
  Priority 6 : Disabled
  Priority 7 : Disabled
A-MSDU Tx:
  Priority 0 : Enabled
  Priority 1 : Enabled
  Priority 2 : Enabled
  Priority 3 : Enabled
  Priority 4 : Enabled
  Priority 5 : Enabled
  Priority 6 : Disabled
  Priority 7 : Disabled
Guard Interval : Any
Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admission Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
Example: Viewing the Configuration Settings for the 24-GHz Band

Switch# show ap dot11 24ghz network
802.11b Network : Enabled
11gSupport : Enabled
11nSupport : Enabled

802.11b/g Operational Rates
802.11b 1M : Mandatory
802.11b 2M : Mandatory
802.11b 5.5M : Mandatory
802.11g 6M : Supported
802.11g 9M : Supported
802.11b 11M : Mandatory
802.11g 12M : Supported
802.11g 18M : Supported
802.11g 24M : Supported
802.11g 36M : Supported
802.11g 48M : Supported
802.11g 54M : Supported

802.11n MCS Settings:
MCS 0 : Supported
MCS 1 : Supported
MCS 2 : Supported
MCS 3 : Supported
MCS 4 : Supported
MCS 5 : Supported
MCS 6 : Supported
MCS 7 : Supported
MCS 8 : Supported
MCS 9 : Supported
MCS 10 : Supported
MCS 11 : Supported
MCS 12 : Supported
MCS 13 : Supported
MCS 14 : Supported
MCS 15 : Supported
MCS 16 : Supported
MCS 17 : Supported
MCS 18 : Supported
MCS 19 : Supported
MCS 20 : Supported
MCS 21 : Supported
MCS 22 : Supported
MCS 23 : Supported

802.11n Status:
A-MPDU Tx:
Priority 0 : Enabled
Priority 1 : Disabled
Priority 2 : Disabled
Priority 3 : Disabled
Priority 4 : Enabled
Priority 5 : Enabled
Priority 6 : Disabled
Priority 7 : Disabled
A-MSDU Tx:
Example: Viewing the status of 802.11h Parameters

Switch# show wireless dot11h
Power Constraint: 0
Channel Switch: 0
Channel Switch Mode: 0
Example: Verifying the Band-Selection Settings

The following example displays a band-select configuration:

```
Switch# show wireless band-select

Band Select Probe Response : per WLAN enabling
Cycle Count : 2
Cycle Threshold (milli sec) : 200
Age Out Suppression (sec) : 20
Age Out Dual Band (sec) : 60
Client RSSI (dBm) : -80
Client Mid RSSI (dBm) : -80
```

Configuration Examples for Band Selection, 802.11 Bands, and Parameters

Examples: Band Selection Configuration

This example shows how to set the probe cycle count and time threshold for a new scanning cycle period for band select:

```
Switch# configure terminal
Switch(config)# wireless client band-select cycle-count 3
Switch(config)# wireless client band-select cycle-threshold 5000
Switch(config)# end
```

This example shows how to set the suppression expiry time to the band select:

```
Switch# configure terminal
Switch(config)# wireless client band-select expire suppression 100
Switch(config)# end
```

This example shows how to set the dual-band expiry time for the band select:

```
Switch# configure terminal
Switch(config)# wireless client band-select expire dual-band 100
Switch(config)# end
```

This example shows how to set the client RSSI threshold for the band select:

```
Switch# configure terminal
Switch(config)# wireless client band-select client-rssi 40
Switch(config)# end
```

This example shows how to configure band selection on specific WLANs:

```
Switch# configure terminal
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# band-select
Switch(config)# end
```
Examples: 802.11 Bands Configuration

This example shows how to configure 802.11 bands using beacon interval, fragmentation, and dynamic transmit power control:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 24ghz shutdown
Switch(config)# ap dot11 5ghz beaconperiod 500
Switch(config)# ap dot11 5ghz fragmentation 300
Switch(config)# ap dot11 5ghz dtpc
Switch(config)# wireless client association limit 50 interval 1000
Switch(config)# ap dot11 5ghz rate 36 mandatory
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)# no ap dot11 24ghz shutdown
Switch(config)# ap dot11 24ghz dot11g
Switch(config)# end
```

Examples: 802.11n Configuration

This example shows how to configure 802.11n parameters for 5-GHz band using aggregation method:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz dot11n
Switch(config)# ap dot11 5ghz dot11n mcs tx 20
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# wmm require\nSwitch(config-wlan)# exit
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz dot11n a-mpdu tx priority all
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)# exit
```

This example shows how to configure the guard interval for 5-GHz band:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz dot11n
Switch(config)# ap dot11 5ghz dot11n mcs tx 20
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# wmm require\nSwitch(config-wlan)# exit
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz dot11n guard-interval long
Switch(config)# end
```

This example shows how to configure the RIFS for 5-GHz band:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz dot11n
Switch(config)# ap dot11 5ghz dot11n mcs tx 20
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# wmm require\nSwitch(config-wlan)# exit
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz dot11n rifs rx
Switch(config)# end
```
Examples: 802.11h Configuration

This example shows how to configure the access point to announce when it is switching to a new channel using restriction transmission:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz channelswitch mode 0
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)# end
```

This example shows how to configure the 802.11h power constraint for 5-GHz band:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz power-constraint 200
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)# end
```

Additional References for 802.11 Parameters and Band Selection

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td>System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information For Performing 802.11 parameters and Band Selection Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring Aggressive Load Balancing

- Finding Feature Information, on page 1281
- Restrictions for Aggressive Load Balancing, on page 1281
- Information for Configuring Aggressive Load Balancing Parameters, on page 1282
- How to Configure Aggressive Load Balancing, on page 1283
- Monitoring Aggressive Load Balancing, on page 1284
- Examples: Aggressive Load Balancing Configuration, on page 1284
- Additional References for Aggressive Load Balancing, on page 1285
- Feature History and Information For Performing Aggressive Load Balancing Configuration , on page 1286

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Aggressive Load Balancing

- You can configure aggressive load balancing only from the command-line interface.
- Aggressive load balancing is disabled by default, you must enable it manually.
- You can enable load balancing either separately or together with the band select configurations.
- When the band select is enabled on the dual-band clients, the load balancing parameter selects only the lowest load radio from 5-GHz radios. For the 2.4-GHz clients, there is no probe information of the client on 5 GHz and therefore the load balancing algorithm can only be selected between radio on 2.4 GHz.
- You can operate load balancing of clients between access points on the same switch but not for the clients between access points on the different switch.
• The load balancing uses an existing association denial mechanism based on the number of client on the radio and the band select is implemented by the distributed probe response suppression on the access point only.

Information for Configuring Aggressive Load Balancing Parameters

Aggressive Load Balancing

Enabling aggressive load balancing on the controller allows lightweight access points to load balance wireless clients across access points. You can enable aggressive load balancing using the controller.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. The code 17 indicates that the AP is busy. The AP does not respond with an association response bearing ‘success’ if the AP threshold is not met, and with code 17 (AP busy) if the AP utilization threshold is exceeded, and another less busy AP heard the client request.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it would be allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

Voice Client does not authenticate when delay is configured more than 300 ms. To avoid this configure a Central-Auth, Local Switching WLAN with CCKM, configure a Pagent Router between AP and WLC with a delay of 600 ms (300 ms UP and 300 ms DOWN and try associating the voice client

Note

The maximum number of client associations that the access points can support is dependent upon the following factors:

• The maximum number of client associations differs for lightweight and autonomous Cisco IOS access points.

• There may be a limit per radio and an overall limit per AP.

• AP hardware (the 16-MB APs have a lower limit than the 32-MB and higher APs)

The Client Association Limits for Lightweight Access Points are as follows:

• For 16-MB APs, the limit is 128 clients per AP. This limit is applicable to 1100 and 1200 series APs.

• For 32-MB and higher APs, there is no per-AP limit.

The maximum Client Association Limits per-radio for all of the Cisco IOS APs is 200 associations.
With 32-MB and higher lightweight Cisco IOS APs, with two radios, up to $200 + 200 = 400$ associations are supported.

Note

The maximum Client Association Limits per Autonomous Cisco IOS access point is around 80 to 127 clients per AP. This number varies depending on the following factors:

- AP model (whether it is 16 MB or 32 MB or higher)
- Cisco IOS software release
- Hardware configuration (two radios use more memory than one)
- Enabled features (WDS functionality in particular)

The per-radio limit is about 200 associations. One association will likely hit the per-AP limit first. Unlike Cisco Unified Wireless Network, autonomous Cisco IOS supports per-SSID/per-AP association limits. This limit is configured using the max-associations CLI, under dot11 SSID. The maximum number is 255 associations (which is also the default number).

Note

For a FlexConnect AP the association is locally handled. The load-balancing decisions are taken at the Cisco WLC. A FlexConnect AP initially responds to the client before knowing the result of calculations at the Cisco WLC. Load-balancing doesn't take effect when the FlexConnect AP is in standalone mode.

FlexConnect AP does not send (re)association response with status 17 for Load-Balancing as Local mode APs do; instead, it first sends (re)association with status 0 (success) and then deauth with reason 5.

How to Configure Aggressive Load Balancing

Configuring Aggressive Load Balancing

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless load-balancing window client-count</td>
<td>Sets the client window for aggressive load balancing. You can enter a value between 0 and 20 for the <code>client_count</code> parameter.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# wireless load-balancing window 1</td>
<td></td>
</tr>
</tbody>
</table>
### Monitoring Aggressive Load Balancing

This section describes the new command for aggressive load balancing.

The following command can be used to monitor aggressive load balancing on the switch.

**Table 91: Monitoring Aggressive Load Balancing Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless load-balancing</td>
<td>Displays the status of the load-balancing feature.</td>
</tr>
</tbody>
</table>

### Examples: Aggressive Load Balancing Configuration

This example shows how to configure the load balancing denial count:

```
Switch# configure terminal
Switch(config)# wireless load-balancing denial-count 1
Switch(config)# end
Switch# show wireless load-balancing
```

This example shows how to configure the client window for aggressive load balancing:
Switch# configure terminal
Switch(config)# wireless load-balancing window 1
Switch(config)# end
Switch# show wireless load-balancing

This example shows how to configure load balancing on specific WLAN:

Switch# configure terminal
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# load-balance
Switch(config)# end
Switch# show wireless load-balancing

Additional References for Aggressive Load Balancing

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
# Feature History and Information For Performing Aggressive Load Balancing Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring Client Roaming

The following are the restrictions that you should be aware while configuring client roaming:

• Cisco Compatible Extensions (CCX) support is enabled automatically for every WLAN on the switch and cannot be disabled. The switch stores the CCX version of the client in its client database and uses it to generate and respond to CCX frames appropriately. Clients must support CCXv4 or v5 (or CCXv2 for access point assisted roaming) to utilize these roaming enhancements.

• Client roaming between 600 Series Access points is not supported.

Information About Client Roaming

The controllers deliver high-end wireless services to the clients roaming across wireless network. Now, the wireless services are integrated with the switches, thus delivering a value-added Cisco unified new mobility
architecture. This unified architecture enables client-roaming services to both wireless and wired clients with seamless, fast-roaming services.

The new mobility architecture supports fast client roaming services using logical categorization of network into Mobility Domains (MDs), Mobility Groups (MGs), Mobility Subdomains (MSDs), and Switch Peer Groups (SPGs) using systems such as Mobility Oracle (MO), Mobility Controller (MC), and Mobility Agent (MA).

• A **Mobility Domain** is the entire domain across which client roaming is supported. It is a collection of mobility groups. For example, a campus network can be considered as a mobility domain.

• A **Mobility Group** is a collection of mobility subdomains across which fast roaming is supported. The mobility group can be one or more buildings within a campus across which frequent roaming is supported.

• A **Mobility Subdomain** is an autonomous portion of the mobility domain network. Each mobility subdomain contains one mobility controller (MC) and a collection of SPGs. A subdomain is equivalent to an 802.11r key domain.

• A **Switch Peer Group** is a collection of mobility agents.

• The **Mobility Oracle** acts as the point of contact for mobility events that occur across mobility subdomains. The mobility oracle also maintains a local database of each client in the entire mobility domain, their home and current subdomain. There is only one MO for an entire mobility domain. The Cisco WLC 5700 Series Controllers or Cisco Unified Wireless Networking Solution controller can act as MO.

• The **Mobility Controller** provides mobility management services for inter-SPG roaming events. The MC sends the configuration like SPG name and SPG peer member list to all of the mobility agents under its subdomain. The Cisco WLC 5700 Series Controllers, Cisco Catalyst 3850 Switch, or Cisco Unified Wireless Networking Solution controller can act as MC. The MC has MC functionality and MA functionality that is running internally into it.

• The **Mobility Agent** is the component that maintains client mobility state machine for a mobile client. All APs are connected to the mobility agent.

The new mobility architecture supports seamless roaming in the following scenarios:

• Intra-switch roaming—The client roaming between APs managed by same mobility agent.

• Intra-SPG roaming—The client roaming between mobility agents in the same SPG.

• Inter-SPG, Intra-subdomain roaming—The client roaming between mobility agents in different SPGs within the same subdomain.

• Inter-subdomain roaming—The client roaming between mobility agents across a subdomain.

**Fast Roaming**

New mobility architecture supports fast roaming when clients roam within a mobility group by eliminating the need for full authentication. Security polices should be same across the switches for fast roaming.

**Local, anchor, foreign MAs and MCs**

When a client joins an MA initially and its point of attachment has not changed, that MA is referred as local or associated MA. The MC to which this MA is associated is referred as local or associated MC.

When a client roams between two MAs, the MA to which the client was previously associated is the anchor MA (point of attachment) and the MA to which the client is currently associated is the foreign or associated.
MA (point of presence). The MCs to which these MAs are associated are referred as anchor, foreign, or associated MCs, respectively.

**Inter-Subnet Roaming**

Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group on different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the controllers allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active. The tunnel is torn down, and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 169.254.*.* client auto-IP address or when the operator-set user timeout is exceeded.

**Voice-over-IP Telephone Roaming**

802.11 voice-over-IP (VoIP) telephones actively seek out associations with the strongest RF signal to ensure the best quality of service (QoS) and the maximum throughput. The minimum VoIP telephone requirement of 20-millisecond or shorter latency time for the roaming handover is easily met by the Cisco Wireless solution, which has an average handover latency of 5 or fewer milliseconds when open authentication is used. This short latency period is controlled by controllers rather than allowing independent access points to negotiate roaming handovers.

The Cisco Wireless solution supports 802.11 VoIP telephone roaming across lightweight access points managed by controllers on different subnets, as long as the controllers are in the same mobility group. This roaming is transparent to the VoIP telephone because the session is sustained and a tunnel between controllers allows the VoIP telephone to continue using the same DHCP-assigned IP address as long as the session remains active. The tunnel is torn down, and the VoIP client must reauthenticate when the VoIP telephone sends a DHCP Discover with a 0.0.0.0 VoIP telephone IP address or a 169.254.*.* VoIP telephone auto-IP address or when the operator-set user timeout is exceeded.

**CCX Layer 2 Client Roaming**

The controller supports five CCX Layer 2 client roaming enhancements:

- **Access point assisted roaming**—This feature helps clients save scanning time. When a CCXv2 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client’s current SSID(s), and time elapsed since disassociation.

- **Enhanced neighbor list**—This feature focuses on improving a CCXv4 client’s roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.

- **Enhanced neighbor list request (E2E)**—The End-2-End specification is a Cisco and Intel joint program that defines new protocols and interfaces to improve the overall voice and roaming experience. It applies only to Intel clients in a CCX environment. Specifically, it enables Intel clients to request a neighbor list at will. When this occurs, the access point forwards the request to the controller. The controller receives the request and replies with the current CCX roaming sublist of neighbors for the access point to which the client is associated.
To see whether a particular client supports E2E, choose Wireless > Clients on the controller GUI, click the Detail link for the desired client, and look at the E2E Version text box in the Client Properties area.

- Roam reason report—This feature enables CCXv4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.

- Directed roam request—This feature enables the controller to send directed roam requests to the client in situations when the controller can better service the client on an access point different from the one to which it is associated. In this case, the controller sends the client a list of the best access points that it can join. The client can either honor or ignore the directed roam request. Non-CCX clients and clients running CCXv3 or below must not take any action. No configuration is required for this feature.

How to Configure Layer 2 or Layer 3 Roaming

Configuring Layer 2 or Layer 3 Roaming

Before you begin

To configure the mobility agent for Layer 2 or Layer 3 roaming, the following requisites should be considered:

- SSID and security polices should be same across MAs for Layer 2 and Layer 3 roaming.

- Client VLAN ID should be same for Layer 2 roaming and different for Layer 3 roaming.

- Bridge domain ID and client VLAN IDs should be same for Layer 2 roaming. Either one or both of the bridge domain ID and client VLAN ID should be different for Layer 3 roaming.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wlan wlan_profile_name wlan_ID SSID_network_name</code></td>
<td>Enters WLAN configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)#wlan wlan1</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>no mobility anchor sticky</code></td>
<td>(Optional) Disables Layer 2 anchoring.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config-wlan)#no mobility anchor sticky</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring CCX Client Roaming Parameters (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap dot11 {5ghz</td>
<td>24ghz} l2roam rf-params {default</td>
</tr>
<tr>
<td></td>
<td>Example: Switch#ap dot11 5ghz l2roam rf-params custom –80</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```
Step 1
Switch# configure terminal

Step 2
Switch# ap dot11 5ghz l2roam rf-params custom –80
```

- **Minimum RSSI**—Indicates minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point.

  If the client’s average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

  You can configure the minimum RSSI range from –50 through –90 dBm and the default value is –85 dBm.

- **Hysteresis**—Indicates how much greater the signal strength of a neighboring access point must be for the client to roam to it.

  This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points.
You can configure the hysteresis range from 3 through 20 dB and the default is 3 dB.

- **Scan Threshold**—Indicates a minimum RSSI that is allowed before the client should roam to a better access point.

  When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold.

  You can configure the RSSI range from –50 through –90 dBm and the default value is –72 dBm.

- **Transition Time**—Indicates the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client’s associated access point is below the scan threshold.

  The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

  You can configure the time period in the range from 1 through 5 seconds and the default time is 5 seconds.

### Step 3

**end**

**Example:**

Switch(config)# end

Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.
## Configuring Mobility Oracle

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless mobility oracle</td>
<td>Enables mobility oracle on the controller.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# wireless mobility</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Mobility Controller

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless mobility controller</td>
<td>Enables wireless mobility controller.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# wireless mobility</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> wireless mobility controller peer-group</td>
<td>Configures a switch peer group name. You can enter up to 31 case-sensitive ASCII printable characters for the group name. Spaces are not allowed in mobility group.</td>
</tr>
<tr>
<td>switch-peer-group-name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# wireless mobility</td>
<td></td>
</tr>
<tr>
<td>controller peer-group SPG1</td>
<td>Note: The No form of the command deletes the switch peer group.</td>
</tr>
<tr>
<td>controller peer-group SPG1</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>4</td>
<td><strong>wireless mobility controller peer-group</strong>&lt;br&gt;<strong>switch-peer-group-name member ip</strong>&lt;br&gt;<strong>ip-address {public-ip public-ip-address}</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.0.0.1</td>
</tr>
<tr>
<td>5</td>
<td><strong>wireless mobility controller peer-group</strong>&lt;br&gt;<strong>switch-peer-group-name multicast</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Switch(config)# wireless mobility controller peer-group SPG1 multicast</td>
</tr>
<tr>
<td>6</td>
<td><strong>wireless mobility controller peer-group</strong>&lt;br&gt;<strong>switch-peer-group-name multicast ip</strong>&lt;br&gt;<strong>peer-group-multicast-ip-addr</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Switch(config)# wireless mobility controller peer-group SPG1 multicast ip 10.0.0.4</td>
</tr>
<tr>
<td>7</td>
<td><strong>wireless mobility controller</strong>&lt;br&gt;<strong>peer-groups switch-peer-group-name bridge-domain-id id</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Switch(config)# wireless mobility controller peer-group SPG bridge-domain-id 10.0.0.5</td>
</tr>
<tr>
<td>8</td>
<td><strong>wireless mobility group member ip</strong>&lt;br&gt;<strong>ip-address [public-ip public-ip-address]</strong>&lt;br&gt;<strong>[group group-name]</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Switch(config)# wireless mobility group member ip 10.0.0.1</td>
</tr>
<tr>
<td>9</td>
<td><strong>wireless mobility dscp value</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Switch(config)# wireless mobility dscp 46</td>
</tr>
<tr>
<td>10</td>
<td><strong>wireless mobility group keepalive</strong> {count</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# wireless mobility group keepalive count</code></td>
<td>termed DOWN and keepalive interval which is interval between two keepalives.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
</tr>
<tr>
<td><code>wireless mobility group name name</code></td>
<td>Specifies the case sensitive wireless mobility group name which can be ASCII printable string up to 31 characters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# wireless mobility group name group1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td></td>
</tr>
<tr>
<td><code>wireless mobility oracle ip mo-ip-address</code></td>
<td>Configures the mobility oracle IP address.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# wireless mobility oracle ip 10.0.0.5</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td></td>
</tr>
<tr>
<td><code>wireless management interface interface-name</code></td>
<td>Configures the wireless management interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# wireless management interface Vlan21</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Example**

### Configuring Mobility Agent

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>wireless mobility controller ip ip-address</code></td>
<td>Sets the IP address of the mobility controller.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# wireless mobility controller ip 10.10.10.20</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>wireless mobility load-balance</code></td>
<td>Configures wireless mobility load balancing.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# wireless mobility load-balance</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

**Step 4**
- `wireless mobility load-balance threshold threshold-value`
  
  **Example:**
  ```
  Switch(config)# wireless mobility load-balance threshold 100
  ```

  Configures the number of clients that can be local or anchored on the MA. You can configure the threshold value in a range from 100 to 2000. The default value is 1000.

**Step 5**
- `wireless management interface interface-name`
  
  **Example:**
  ```
  Switch(config)# wireless management interface Vlan21
  ```

  Configures wireless management interface for the mobility agent.

**Step 6**
- `end`
  
  **Example:**
  ```
  Switch(config)# end
  ```

  Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

### Monitoring Client Roaming Parameters

This section describes the new commands for the client parameters.

The following commands can be used to monitor the client roaming parameters on the switch.

**Table 92: Monitoring Client Roaming Parameters Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show ap dot11 {5ghz</td>
<td>24ghz} l2roam rf-param`</td>
</tr>
<tr>
<td>`show ap dot11 {5ghz</td>
<td>24ghz} l2roam statistics`</td>
</tr>
<tr>
<td>`show ap dot11 {5ghz</td>
<td>24ghz} l2roam mac-address mac-address statistics`</td>
</tr>
</tbody>
</table>

### Monitoring Mobility Configurations

This section describes the new commands for monitoring mobility configurations.

The following command can be used to monitor mobility configurations on the Mobility Oracle, Mobility Controller, and Mobility Agent.

**Table 93: Monitoring Mobility Configuration Commands on the Mobility Controller and Mobility Agent**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless mobility summary</code></td>
<td>Displays the summary information for the Mobility Controller and Mobility Agent.</td>
</tr>
</tbody>
</table>
### Additional References for Configuring Client Roaming

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility configuration</td>
<td><em>Mobility Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em></td>
</tr>
</tbody>
</table>
### Related Topic

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility-related commands</td>
<td>Mobility Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

### Feature History and Information For Performing Client Roaming Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Application Visibility and Control

Application Visibility and Control (AVC) classifies applications using deep packet inspection techniques with the Network-Based Application Recognition engine, and provides application-level visibility and control (QoS) in wireless networks. After the applications are recognized, the AVC feature enables you to either drop, mark, or police the data traffic.

AVC is configured by defining a class map in a QoS client policy to match a protocol.

Using AVC, we can detect more than 1000 applications. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.
You can view list of 30 applications in Top Applications in Monitor Summary section of the UI.

Traffic flows are analyzed and recognized using the NBAR2 engine at the access point. For more information about the NBAR2 Protocol Library, see http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html. The specific flow is marked with the recognized protocol or application, such as WebEx. This per-flow information can be used for application visibility using Flexible NetFlow (FNF).

AVC QoS actions are applied with AVC filters in both upstream and downstream directions. The QoS actions supported for upstream flow are drop, mark, and police, and for downstream flow are mark and police. AVC QoS is applicable only when the application is classified correctly and matched with the class map filter in the policy map. For example, if the policy has a filter based on an application name, and the traffic has also been classified to the same application name, then the action specified for this match in the policy will be applied.

When you downgrade the controller from 8.0 to any earlier version, the AVC rate limit rules display the action as drop. This action is expected since the AVC rate limit rule is introduced in the controller version 8.0.

<table>
<thead>
<tr>
<th>Cisco WLC Platform</th>
<th>Flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 2504 WLC</td>
<td>26,250</td>
</tr>
<tr>
<td>Cisco 5508 WLC</td>
<td>183,750</td>
</tr>
<tr>
<td>Cisco WiSM2</td>
<td>393,750</td>
</tr>
<tr>
<td>Cisco 8510 WLC</td>
<td>336,000</td>
</tr>
<tr>
<td>Cisco 5520 WLC</td>
<td>336,000</td>
</tr>
<tr>
<td>Cisco 8540 WLC</td>
<td>336,000</td>
</tr>
</tbody>
</table>

Application Visibility and Control Protocol Packs

Protocol packs are a means to distribute protocol updates outside the switch software release trains, and can be loaded on the switch without replacing the switch software.

The Application Visibility and Control Protocol Pack (AVC Protocol Pack) is a single compressed file that contains multiple Protocol Description Language (PDL) files and a manifest file. A set of required protocols can be loaded, which helps AVC to recognize additional protocols for classification on your network. The manifest file gives information about the protocol pack, such as the protocol pack name, version, and some information about the available PDLs in the protocol pack.

The AVC Protocol Packs are released to specific AVC engine versions. You can load a protocol pack if the engine version on the switch platform is the same or higher than the version required by the protocol pack.

AAA override for AVC profiles

The AAA attribute for client or user profile is configured on the AAA server using authentication from RADIUS server or Cisco ACS or ISE. The AAA attribute is processed during layer 2 or layer 3 authentication by the switch and the same is overridden by what is configured on the WLAN.
The AAA AVC profile is defined as a Cisco AV air. The string option is defined as `avc-profile-name` and this value has to be configured for any AVC profile available in the switch.

## Supported AVC Class Map and Policy Map Formats

### Supported AVC Class Map Format

<table>
<thead>
<tr>
<th>Class Map Format</th>
<th>Class Map Example</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>match protocol protocol name</code></td>
<td>class-map match-any webex-class match protocol webex-media</td>
<td>Both upstream and downstream</td>
</tr>
<tr>
<td><code>match protocol attribute category category-name</code></td>
<td>class-map match-any IM match protocol attribute category instant-messaging</td>
<td>Both upstream and downstream</td>
</tr>
<tr>
<td><code>match protocol attribute sub-category sub-category-name</code></td>
<td>class-map match-any realtimeconferencing match protocol attribute sub-category voice-video-chat-collaboration</td>
<td>Both upstream and downstream</td>
</tr>
<tr>
<td><code>match protocol attribute application-group application-group-name</code></td>
<td>class-map match-any skype match protocol attribute application-group skype-group</td>
<td>Both upstream and downstream</td>
</tr>
<tr>
<td>Combination filters</td>
<td>class-map match-any webex-class match protocol webex match dscp 45 match wlan user-priority 6</td>
<td>Upstream only</td>
</tr>
</tbody>
</table>

### Supported AVC Policy Format

<table>
<thead>
<tr>
<th>Policy Format</th>
<th>QoS Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upstream client policy based on match protocol filter</td>
<td>Mark, police, and drop</td>
</tr>
<tr>
<td>Downstream client policy based on match protocol filter</td>
<td>Mark and police</td>
</tr>
</tbody>
</table>

The following table describes the detailed AVC policy format with an example:

<table>
<thead>
<tr>
<th>AVC Policy Format</th>
<th>AVC Policy Example</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic set</td>
<td>policy-map webex-policy class webex-class set dscp ef //or set up,cos</td>
<td>Upstream and downstream</td>
</tr>
<tr>
<td>AVC Policy Format</td>
<td>AVC Policy Example</td>
<td>Direction</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Basic police</td>
<td><code>policy-map webex-policy</code>&lt;br&gt;<code>class webex-class</code>&lt;br&gt;<code>police 5000000</code></td>
<td>Upstream and downstream</td>
</tr>
<tr>
<td>Basic set and police</td>
<td><code>policy-map webex-policy</code>&lt;br&gt;<code>class webex-class</code>&lt;br&gt;<code>set dscp ef //or set up,cos</code>&lt;br&gt;<code>police 5000000</code></td>
<td>Upstream and downstream</td>
</tr>
<tr>
<td>Multiple set and police including default</td>
<td><code>policy-map webex-policy</code>&lt;br&gt;<code>class webex-class</code>&lt;br&gt;<code>set dscp af31 //or set up,cos</code>&lt;br&gt;<code>police 4000000</code>&lt;br&gt;<code>class class-webex-category</code>&lt;br&gt;<code>set dscp ef //or set up,cos</code>&lt;br&gt;<code>police 6000000</code>&lt;br&gt;<code>class class-default</code>&lt;br&gt;<code>set dscp &lt;&gt;</code></td>
<td>Upstream and downstream</td>
</tr>
<tr>
<td>Hierarchical police</td>
<td><code>policy-map webex-policy</code>&lt;br&gt;<code>class webex-class</code>&lt;br&gt;<code>police 5000000</code>&lt;br&gt;<code>service-policy</code>&lt;br&gt;<code>client-in-police-only</code>&lt;br&gt;<code>policy-map</code>&lt;br&gt;<code>client-in-police-only</code>&lt;br&gt;<code>class webex-class</code>&lt;br&gt;<code>police 100000</code>&lt;br&gt;<code>class class-webex-category</code>&lt;br&gt;<code>set dscp ef //or set up,cos</code>&lt;br&gt;<code>police 6000000</code>&lt;br&gt;<code>police 200000</code></td>
<td>Upstream and downstream</td>
</tr>
<tr>
<td>Hierarchical set and police</td>
<td><code>policy-map webex-policy</code>&lt;br&gt;<code>class class-default</code>&lt;br&gt;<code>police 1500000</code>&lt;br&gt;<code>service policy</code>&lt;br&gt;<code>client-up-child</code>&lt;br&gt;<code>policy-map webex-policy</code>&lt;br&gt;<code>class webex-class</code>&lt;br&gt;<code>police 100000</code>&lt;br&gt;<code>set dscp ef</code>&lt;br&gt;<code>class class-webex-category</code>&lt;br&gt;<code>police 200000</code>&lt;br&gt;<code>set dscp af31</code></td>
<td></td>
</tr>
</tbody>
</table>
### Prerequisites for Application Visibility and Control

- The access points should be AVC capable.
- For the control part of AVC (QoS) to work, the application visibility feature with FNF has to be configured.

### Guidelines for Inter-Switch Roaming with Application Visibility and Control

Follow these guidelines to prevent clients from getting excluded due to malformed QoS policies:

- When a new QoS policy is added to the switch, a QoS policy with the same name should be added to other switch within the same roam or mobility domain.

- When a switch is loaded with a software image of a later release, the new policy formats are supported. If you have upgraded the software image from an earlier release to a later release, you should save the configuration separately. When an earlier release image is loaded, some QoS policies might show as not supported, and you should restore those QoS policies to supported policy formats.

### Restrictions for Application Visibility and Control

- AVC is supported only on the following access points:
  - Cisco Aironet 1260 Series Access Points
  - Cisco Aironet 1600 Series Access Points
  - Cisco Aironet 2600 Series Access Point
  - Cisco Aironet 2600 Series Wireless Access Points
  - Cisco Aironet 2700 Series Access Point
  - Cisco Aironet 3500 Series Access Points

### AVC Policy Format

<table>
<thead>
<tr>
<th>AVC Policy Format</th>
<th>AVC Policy Example</th>
<th>Direction</th>
</tr>
</thead>
</table>
| Drop action       | Any of the above examples apply to this format with this additional example:  
  policy-map webex-policy  
  class webex-class  
  drop  
  class netflix  
  set dscp ef //or set up,cos  
  police 6000000  
  class class-default  
  set dscp <> | Upstream only |
• Cisco Aironet 3600 Series Access Points

• AVC is not supported on Cisco Aironet 702W, 702I (128 M memory), and 1530 Series Access Points.

• Dropping or marking of the data traffic (control part) is not supported for software Release 3.3.

• Dropping or marking of the data traffic (control part) is supported in software Release 3E.

• Only the applications that are recognized with application visibility can be used for applying QoS control.

• Multicast traffic classification is not supported.

• Only the applications that are recognized with App visibility can be used for applying QoS control.

• IPv6 including ICMPv6 traffic classifications are not supported.

• Datalink is not supported for NetFlow fields for AVC.

• The following commands are not supported for AVC flow records:
  • collect flow username
  • collect interface { input | output }
  • collect wireless client ipv4 address
  • match interface { input | output }
  • match transport igmp type

• The template timeout cannot be modified on exporters configured with AVC. Even if the template timeout value is configured to a different value, only the default value of 600 seconds is used.

• For the username information in the AVC-based record templates, ensure that you configure the options records to get the user MAC address to username mapping.

• When there is a mix of AVC-enabled APs such as 3600, and non-AVC-enabled APs such as 1140, and the chosen policy for the client is AVC-enabled, the policy will not be sent to the APs that cannot support AVC.

• Only ingress AVC statistics are supported. The frequency of statistics updates depends on the number of clients loaded at the AP at that time. Statistics are not supported for very large policy format sizes.

• The total number of flows for which downstream AVC QoS supported per client is 1000.

• The maximum number of flows supported for Cisco WLC 5700 Series is 360 K and Catalyst 3850 Series Switch is 48 K.

• These are some class map and policy map-related restrictions. For supported policy formats, see Supported AVC Class Map and Policy Map Formats, on page 1301.

  • AVC and non-AVC classes cannot be defined together in a policy in a downstream direction. For example, when you have a class map with match protocol, you cannot use any other type of match filter in the policy map in the downstream direction.

  • Drop action is not applicable for the downstream AVC QoS policy.

  • Match protocol is not supported in ingress or egress for SSID policy.
• Google shares resources among several of their services because of which for some of the traffic it is not possible to say it is unique to one application. Therefore we added google-services for traffic that cannot be distinguished. The behavior you experience is expected.

How to Configure Application Visibility and Control

Configuring Application Visibility and Control (CLI)

To configure Application Visibility, follow these general steps:

1. Create a flow record by specifying keys and non-key fields to the flow.
2. Create an optional flow exporter by specifying the flow record as an option.
3. Create a flow monitor based on the flow record and flow exporter.
4. Configure WLAN to apply flow monitor in IPv4 input or output direction.

To configure Application Control, follow these general steps:

1. Create an AVC QoS policy.
2. Attach AVC QoS policy to the client in one of three ways: configuring WLAN, using ACS or ISE, or adding local policies.

Creating a Flow Record

By default, wireless avc basic (flow record) is available. When you click Apply from the GUI, then the record is mapped to the flow monitor.

Default flow record cannot be edited or deleted. If you require a new flow record, you need to create one and map it to the flow monitor from CLI.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>flow record flow_record_name</td>
<td>Enters flow record configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# flow record record1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (config-flow-record)#</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>description string</td>
<td>(Optional) Describes the flow record as a maximum 63-character string.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-flow-record)# description</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv4flow</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>match ipv4 protocol</td>
<td>Specifies a match to the IPv4 protocol.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Switch (config-flow-record) match ipv4 protocol</td>
<td>Specifies a match to the IPv4 source address-based field.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> match ipv4 source address</td>
<td>Specifies a match to the IPv4 source address-based field.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch (config-flow-record) match ipv4 source address</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> match ipv4 destination address</td>
<td>Specifies a match to the IPv4 destination address-based field.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch (config-flow-record) match ipv4 destination address</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> match transport source-port</td>
<td>Specifies a match to the transport layer source-port field.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch (config-flow-record) match transport source-port</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> match transport destination-port</td>
<td>Specifies a match to the transport layer destination-port field.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch (config-flow-record) match transport destination-port</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> match flow direction</td>
<td>Specifies a match to the direction the flow was monitored in.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch (config-flow-record) match flow direction</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> match application name</td>
<td>Specifies a match to the application name. <strong>Note</strong> This action is mandatory for AVC support, as this allows the flow to be matched against the application.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch (config-flow-record) match application name</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> match wireless ssid</td>
<td>Specifies a match to the SSID name identifying the wireless network.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch (config-flow-record) match wireless ssid</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> collect counter bytes long</td>
<td>Specifies to collect counter fields total bytes.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch (config-flow-record) collect counter bytes long</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> collect counter packets long</td>
<td>Specifies to collect counter fields total packets.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch (config-flow-record) collect counter packets long</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Creating a Flow Exporter (Optional)

You can create a flow export to define the export parameters for a flow. This is an optional procedure for configuring flow parameters.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><code>flow exporter flow_exporter_name</code></td>
<td>Enters flow exporter configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# flow exporter record1 Switch (config-flow-exporter)#</td>
<td></td>
</tr>
<tr>
<td><code>description string</code></td>
<td>Describes the flow record as a maximum 63-character string.</td>
</tr>
<tr>
<td>Example: Switch(config-flow-exporter)# description IPv4flow</td>
<td></td>
</tr>
<tr>
<td>`destination {hostname</td>
<td>ip-address}`</td>
</tr>
<tr>
<td>Example: Switch (config-flow-exporter) # destination 10.99.1.4</td>
<td></td>
</tr>
<tr>
<td><code>transport udp port-value</code></td>
<td>Configures a port value for the UDP protocol.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Creating a Flow Monitor

You can create a flow monitor and associate it with a flow record and a flow exporter.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 flow monitor monitor-name</td>
<td>Creates a flow monitor and enters flow monitor configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch (config)# flow monitor</td>
<td></td>
</tr>
<tr>
<td>flow-monitor-1</td>
<td></td>
</tr>
<tr>
<td>Step 3 description description</td>
<td>Creates a description for the flow monitor.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch (config)# description</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch (config-flow-monitor)# description flow-monitor-1</strong></td>
<td>Specifies the name of a recorder that was created previously.</td>
</tr>
<tr>
<td><strong>Step 4 record record-name</strong></td>
<td>Specifies the name of a recorder that was created previously.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-flow-monitor)# record flow-record-1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5 exporter exporter-name</strong></td>
<td>Specifies the name of an exporter that was created previously.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-flow-monitor)# exporter flow-exporter-1</td>
<td></td>
</tr>
<tr>
<td>**Step 6 cache timeout {active</td>
<td>inactive} (Optional)**</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-flow-monitor)# cache timeout active 1800 Switch (config-flow-monitor)# cache timeout inactive 200</td>
<td><strong>Note</strong> To achieve optimal result for the AVC flow monitor, we recommend you to configure the inactive cache timeout value to be greater than 90 seconds.</td>
</tr>
<tr>
<td><strong>Step 7 end</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8 show flow monitor</strong></td>
<td>Verifies your configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch # show flow monitor</td>
<td></td>
</tr>
</tbody>
</table>

### Creating AVC QoS Policy

To create AVC QoS policy, perform these general steps:

1. Create a class map with match protocol filters.
2. Create a policy map.
3. Apply a policy map to the client in one of the following ways:
   1. Apply a policy map over WLAN either from the CLI or GUI.
   2. Apply a policy map through the AAA server (ACS server or ISE) from the CLI.
      
      For more information, refer to the *Cisco Identity Services Engine User Guide* and *Cisco Secure Access Control System User Guide*.
   3. Apply local policies either from the CLI or GUI.
Creating a Class Map

You need to create a class map before configuring any match protocol filter. The QoS actions such as marking, policing, and dropping can be applied to the traffic. The AVC match protocol filters are applied only for the wireless clients. For more information about the protocols that are supported, see http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Creates a class map.</td>
</tr>
<tr>
<td>class-map class-map-name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# class-map webex-class</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies match to the application name, category name, subcategory name, or application group.</td>
</tr>
<tr>
<td>match protocol { application-name</td>
<td>attribute category category-name</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# class-map webex-class Switch(config-cmap)# match protocol webex-media Switch(config)# class-map class-webex-category Switch(config-cmap)# match protocol attribute category webex-media Switch# class-map class-webex-sub-category Switch(config-cmap)# match protocol attribute sub-category webex-media Switch# class-map class-webex-application-group Switch(config-cmap)# match protocol attribute application-group webex-media</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Creating a Policy Map

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-map <em>policy-map-name</em></td>
<td>Creates a policy map by entering the policy map name, and enters policy-map configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# policy-map webex-policy Switch(config-pmap)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class [class-map-name</td>
<td>Defines a traffic classification, and enters policy-map class configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-pmap)# class-map \webex-class Switch(config-pmap-c)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police rate-bps burst-byte [exceed-action {drop</td>
<td>policed-dscp-transmit}]</td>
<td>Defines a policer for the classified traffic.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-pmap-c)# police 100000 80000 drop</td>
<td></td>
</tr>
</tbody>
</table>

---

**Note:**

- To delete an existing policy map, use the `no policy-map policy-map-name` global configuration command.

---

**Note:**

- To delete an existing class map, use the `no class class-map-name` policy-map configuration command.

---

- For `rate-bps`, specify an average traffic rate in bits per second (b/s). The range is 8000 to 10000000000.
### Purpose
Command or Action | Purpose
--- | ---

- **For burst-byte**, specify the normal burst size in bytes. The range is 8000 to 1000000.
- (Optional) Specifies the action to take when the rates are exceeded. Use the `exceed-action drop` keywords to drop the packet. Use the `exceed-action policed-dscp-transmit` keywords to mark down the DSCP value (by using the policed-DSCP map) and to send the packet.

### Step 5
**set** `{ dscp new-dscp | cos cos-value }`<br>**Example:**<br>`Switch(config-pmap-c)# set dscp 45`

Classifies IP traffic by setting a new value in the packet.

- **For dscp new-dscp**, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63.

### Step 6
**end**<br>**Example:**<br>`Switch(config)# end`

Returns to privileged EXEC mode. Alternatively, you can also press `Ctrl-Z` to exit global configuration mode.

### What to do next
After creating your policy maps, attach the traffic policy or polices to an interface using the `service-policy` command.

### Configuring Local Policies (CLI)

#### Configuring Local Policies (CLI)

To configure local policies, complete these procedures:

1. Create a service template.
2. Create an interface template.
3. Create a parameter map.
4. Create a policy map.
5. Apply a local policy on a WLAN.

### Creating a Service Template (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Creating a Parameter Map (CLI)

Parameter map is preferred to use than class map.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch# configure terminal
```

### Switch Configuration

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enters service template configuration mode.</td>
<td>configure terminal</td>
</tr>
<tr>
<td>specifiesthe access list to be applied.</td>
<td>access-group acl_list</td>
</tr>
<tr>
<td>Specifies VLAN ID. You can specify a value from 1 to 4094.</td>
<td>vlan vlan_id</td>
</tr>
<tr>
<td>Specifies session timeout value for service template. You can specify a value from 1 to 65535.</td>
<td>absolute-timer seconds</td>
</tr>
<tr>
<td>Configures QoS policies for the client.</td>
<td>service-policy qos input</td>
</tr>
<tr>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
<td>end</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch(config)# configure terminal
Switch(config)# service-template service-template-name
test
Switch(config-service-template)# access-group foo-acl
Switch(config-service-template)# vlan 100
Switch(config-service-template)# absolute-timer 20
Switch(config-service-template)# service-policy qos input foo-qos
Switch(config)# end
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>parameter-map type subscriber attribute-to-service parameter-map-name</td>
<td>Specifies the parameter map type and name.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>map-index map { device-type</td>
<td>mac-address</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-parameter-map-filter)# 10 map device-type eq &quot;WindowsXP-Workstation&quot;</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>service-template service-template-name</td>
<td>Enters service template configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-parameter-map-filter-submode)# service-template cisco-phone-template Switch(config-parameter-map-filter-submode)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>interface-template interface-template-name</td>
<td>Enters service template configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-parameter-map-filter-submode)# interface-template cisco-phone-template Switch(config-parameter-map-filter-submode)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Information About Configuring Local Policies, on page 486
- Restrictions for Configuring Local Policies, on page 485
- Monitoring Local Policies, on page 496
- Examples: Local Policies Configuration, on page 497
### Creating a Policy Map (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | configure terminal  
**Example:**  
Switch# configure terminal | Enters global configuration mode. |
| Step 2 | policy-map type control subscriber  
policy-map-name  
**Example:**  
Switch(config)# policy-map type control subscriber Aironet-Policy | Specifies the policy map type. |
| Step 3 | event identity-update {match-all | match-first}  
**Example:**  
Switch(config-policy-map)# event identity-update match-all | Specifies match criteria to the policy map. |
| Step 4 | **class_number** class {class_map_name | always } {do-all | do-until-failure | do-until-success}  
**Example:**  
Switch(config-class-control-policymap)# 1 class local_policy1_class do-until-success | Configures the local profiling policy class map number and specifies how to perform the action. The class map configuration mode includes the following command options:  
- **always**—Executes without doing any matching but return success.  
- **do-all**—Executes all the actions.  
- **do-until-failure**—Execute all the actions until any match failure is encountered. This is the default value.  
- **do-until-success**—Execute all the actions until any match success happens. |
| Step 5 | action-index map attribute-to-service table  
parameter-map-name  
**Example:**  
Switch(config-policy-map)# 10 map attribute-to-service table Aironet-Policy-param | Specifies parameter map table to be used. |
| Step 6 | end  
**Example:**  
Switch(config)# end | Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. |
Applying a Local Policy for a Device on a WLAN (CLI)

Before you begin

If the service policy contains any device type-based rules in the parameter map, ensure that the device classifier is already enabled.

![Note]

You should use the **device classification** command to classify the device for it to be displayed correctly on the show command output.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wlan wlan-name</code></td>
<td>Enters WLAN configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config)# <code>wlan wlan1</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>service-policy type control subscriber policymapname</code></td>
<td>Applies local policy to WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-wlan)# <code>service-policy type control subscriber Aironet-Policy</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>profiling local http (optional)</code></td>
<td>Enables only profiling of devices based on HTTP protocol (optional).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-wlan)# <code>profiling local http</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>profiling radius http (optional)</code></td>
<td>Enables profiling of devices on ISE (optional).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config-wlan)# <code>profiling radius http</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>no shutdown</code></td>
<td>Specifies not to shut down the WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Local Policies (GUI)

To configure local policies, complete these procedures:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-wlan)# no shutdown</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
</tbody>
</table>

**Step 7**

Example:

Switch(config)# end

**Related Topics**

- Information About Configuring Local Policies, on page 486
- Restrictions for Configuring Local Policies, on page 485
- Monitoring Local Policies, on page 496
- Examples: Local Policies Configuration, on page 497

**Creating a Service Template (GUI)**

**Procedure**

**Step 1**

Choose **Configuration > Security > Local Policies > Service Template** to open the Service Template page.

**Step 2**

Create a new template as follows:

a) Click New to open the Service Template > New page.

b) In the Service Template name text box, enter the new service template name.

c) In the VLAN ID text box, enter the VLAN identifier that has to be associated with the policy. The value ranges from 1 to 4094.

d) In the Session timeout text box, enter the maximum amount of time, in seconds, after which a client is forced to reauthenticate. The value ranges from 1 to 65535 seconds.

e) From the Access control list drop-down list, choose the access control list to be mapped to the policy.

f) From the Ingress QoS drop-down list, choose the ingress QoS policy to be applied.

g) From the Egress QoS drop-down list, choose the egress QoS policy to be applied.

h) Click Apply to save the configuration.

**Step 3**

Edit a service template as follows:

a) From the Service Template page, click the service template to open the Service Template > Edit page.
b) In the VLAN ID text box, enter the VLAN identifier that has to be associated with the policy. The value ranges from 1 to 4094.

c) In the Session timeout text box, enter the maximum amount of time, in seconds, after which a client is forced to reauthenticate. The value ranges from 1 to 65535 seconds.

d) From the Access control list drop-down list, choose the access control list to be mapped to the policy.

e) From the Ingress QoS drop-down list, choose the ingress QoS policy to be applied.

f) From the Egress QoS drop-down list, choose the egress QoS policy to be applied.

g) Click **Apply** to save the configuration.

**Step 4**

Remove a service template as follows:

a) From the **Service Template** page, select the service template.

b) Click **Remove**.

c) Click **Apply** to save the configuration.

**Related Topics**

- [Information About Configuring Local Policies](#), on page 486
- [Restrictions for Configuring Local Policies](#), on page 485
- [Monitoring Local Policies](#), on page 496
- [Examples: Local Policies Configuration](#), on page 497

---

**Creating a Policy Map (GUI)**

**Procedure**

**Step 1**

Choose **Configuration > Security > Local Policies > Policy Map** to open the **Policy Map** page.

**Step 2**

Create a new policy map as follows:

a) Click **New** to open the **Policy Map > New** page.

b) In the Policy Map name text box, enter the new policy map name.

c) Click **Add** to open the Match Criteria area.

d) From the Device Type drop-down list, choose the device type. The match criteria for the device type can be eq, not-eq, or regex with respect to the device type you are choosing.

e) From the User Role drop-down list, select the match criteria as eq, not-eq, or regex and enter the user type or user group of the user, for example, student, teacher, and so on.

f) From the Service Template drop-down list, choose the service template to be mapped to the policy.

g) Click **Add**. The match criteria is added to the Match Criteria Lists.

h) In the Match Criteria Lists area, click **Add** to add the match criteria to the policy.

i) Click **Apply** to save the configuration.

**Step 3**

Edit a policy map as follows:

a) In the **Policy Map** page, select the policy map that you want to edit, and click **Edit** to open the **Policy Map > Edit** page.

b) In the Match Criteria area, choose the device type from the Device Type drop-down list. The match criteria for the device type can be eq, not-eq, or regex with respect to the device type you are choosing.

c) In the Match Criteria area, choose the user role from the User Role drop-down list. Select the match criteria as eq, not-eq, or regex and enter the user type or user group of the user.

d) From the Service Template drop-down list, choose the service template to be mapped to the policy.
Applying Local Policies to WLAN (GUI)

**Procedure**

**Step 1** Choose Configuration > Wireless > WLAN to open the WLANs page.

**Step 2** Click the corresponding WLAN profile. The WLANs > Edit page is displayed.

**Step 3** Click the Policy-Mapping tab.

**Step 4** Check the Device Classification check box to enable classification based on device type.

**Step 5** From the Local Subscriber Policy drop-down list, choose the policy that has to be applied for the WLAN.

**Step 6** Select Local HTTP Profiling to enable profiling on devices based on HTTP (optional).

**Step 7** Select Radius HTTP Profiling to enable profiling on devices based on RADIUS (optional).

**Step 8** Click Apply to save the configuration.

**Related Topics**

- Information About Configuring Local Policies, on page 486
- Restrictions for Configuring Local Policies, on page 485
- Monitoring Local Policies, on page 496
- Examples: Local Policies Configuration, on page 497
Configuring WLAN to Apply Flow Monitor in IPV4 Input/Output Direction

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>wlan wlan-id</code></td>
<td>Enters WLAN configuration submode. For wlan-id, enter the WLAN ID. The range is 1 to 64.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch (config) # wlan 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `ip flow monitor monitor-name {input</td>
<td>output}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch (config-wlan) # ip flow monitor</td>
<td></td>
</tr>
<tr>
<td>flow-monitor-1 input</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Application Visibility and Control (GUI)

#### Configuring Application Visibility (GUI)

You can apply the default flow record (`wireless avc basic`) to the default flow monitor (`wireless-avc-basic`). If you are using the flow record and flow monitor you have created, then the record name and monitor name should be same. This is specific only for configuring AVC from GUI and not for the CLI configuration.

You can use the flow monitor you have created either for upstream or downstream, or both, but ensure that you use the same record name while mapping with the flow monitor.

### Procedure

**Step 1** Choose **Configuration > Wireless > WLAN**.

The **WLAN** page appears.

**Step 2** Click on the corresponding WLAN ID to open the **WLAN > Edit** page and click **AVC**.

The **Application Visibility** page appears.

a) Select the **Application Visibility Enabled** check box to enable AVC on a WLAN.

b) In the **Upstream Profile** text box, enter the name of the AVC profile.

c) In the **Downstream Profile** text box, enter the name of the AVC profile.
To enable AVC, you need to enter the profile names for the upstream and downstream profiles. The profile names are the flow monitor names. By default, the flow monitor names (wireless-avc-basic) appear in the Upstream Profile and Downstream Profile text boxes. For the default flow monitor, the default flow record (wireless avc basic) will be taken. The default flow record is generated by the system and is available.

You can change the profile names for the upstream and downstream profiles but ensure that the same flow records are available for the flow monitors.

The upstream and downstream profiles can have different profile names but there should be flow records available for the flow monitors.

**Step 3**
Click Apply to apply AVC on the WLAN.

**Step 4**
To disable AVC on a specific WLAN, perform the following steps:

- Choose Configuration > Wireless > WLAN to open the WLAN page.
- Click on the corresponding WLAN ID to open the WLAN > Edit page.
- Click AVC to open the Application Visibility page.
- Uncheck the Application Visibility Enabled check box.
- Click Apply to disable AVC on the specific WLAN.

### Configuring Application Visibility and Control (GUI)

**Procedure**

**Step 1**
Choose Configuration > Wireless.

**Step 2**
Expand the QoS node by clicking the left pane and choosing QOS-Policy.

The QOS-Policy page is displayed.

**Step 3**
Click Add New to create a new QoS Policy.

The Create QoS Policy page is displayed.

**Step 4**
Select Client from the Policy Type drop-down list.

**Step 5**
Select the direction into which the policy needs to be applied from the Policy Direction drop-down list.

The available options are:

- Ingress
- Egress

**Step 6**
In the Policy Name text box, specify a policy name.

**Step 7**
In the Description text box, provide a description to the policy.

**Step 8**
Check the Enable Application Recognition check box to configure the AVC class map for a client policy.

**Note**
For an egress client policy, when you enable Application Recognition, the Voice, Video, and User Defined check boxes are disabled.
The following options are available:

- **Trust**—Specify a classification type for this policy.
  - **Protocol**—Allows you to choose the protocols and configure the marking and policing of the packets.
  - **Category**—Allows you to choose the category of the application, for example, browsing.
  - **Subcategory**—Allows you to choose the subcategory of the application, for example, file-sharing.
  - **Application-Group**—Allows you to choose the application group, for example, ftp-group.

- **Protocol Choice**—Choose the protocols, category, subcategory, or application group from the Available Protocols list into the Assigned Protocols to apply the marking and policing of the packets.

- **Mark**—Specify the marking label for each packet. The following options are available:
  - **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  - **CoS**—Matches IEEE 802.1Q class of service. The range is from 0 to 7.
  - **None**—Does not mark the packets.

- **Police (kbps)**—Specify the policing rate in kbps. This option is available when the Policy Direction is egress.

- **Drop**—Specify to drop the ingress packets that correspond to the chosen protocols.

**Note** You can add a maximum of five AVC classes for each client policy.

Step 9  Click **Add** to create an AVC class map. The new class map is listed in a tabular format.

Step 10 Click **Apply** to create an AVC QoS policy.

Step 11 Click the QoS policy link in the **QOS-Policy** page to edit the QoS policy. The **QOS-Policy > Edit** page is displayed. Make changes and click **Apply** to commit your changes.

Step 12 Remove an AVC class map from the QoS policy by navigating to the corresponding AVC class map row in the AVC class map table and clicking **Remove**. Click **Apply** to commit your changes.

---

**Monitoring Application Visibility and Control**

**Monitoring Application Visibility and Control (CLI)**

This section describes the new commands for application visibility.

The following commands can be used to monitor application visibility on the switch and access points.

**Table 97: Monitoring Application Visibility Commands on the switch**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show avc client client-mac top n application [aggregate</td>
<td>upstream</td>
</tr>
<tr>
<td>show avc wlan ssid top n application [aggregate</td>
<td>upstream</td>
</tr>
<tr>
<td>avc top user[enable</td>
<td>disable]</td>
</tr>
</tbody>
</table>
Monitor application visibility and control (GUI)

You can view AVC information on a WLAN in a single shot using an AVC on WLAN pie chart on the Home page of the switch. The pie chart displays the AVC data (Aggregate - Application Cumulative usage %) of the first WLAN. In addition, the top 5 WLANs based on clients are displayed first. Click on any one of the WLANs to view the corresponding pie chart information. If AVC is not enabled on the first WLAN, then the Home page does not display the AVC pie chart.

Procedure

Step 1
Choose Monitor > Controller > AVC > WLANs.
The WLANs page appears.

Step 2
Click the corresponding WLAN profile.
The Application Statistics page appears.

From the Top Applications drop-down list, choose the number of top applications you want to view and click Apply. The valid range is between 5 to 30, in multiples of 5.

a) On the Aggregate, Upstream, and Downstream tabs, you can view the application cumulative and last 90 seconds statistics and usage percent with the following fields:
   a. Application name
   b. Packet count

```plaintext
show avc wlan wlan-id application app name topN [aggregate | upstream | downstream]
Displays to know network usage information on a per user basis within an application.

Note
On Catalyst 4500E Supervisor Engine 8-E, in the information about top N users that is displayed, the client's MAC address and username are not displayed. This issue occurs only within 90 seconds after the client is disconnected.

show wlan id wlan-id
Displays information whether AVC is enabled or disabled on a particular WLAN.

show flow monitor flow_monitor_name cache
Displays information about flow monitors.

show wireless client mac-address mac-address service-policy { input | output }
Displays information about policy mapped to the wireless clients.
```

Table 98: Clearing Application Visibility Statistics Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear avc client mac stats</td>
<td>Clears the statistics per client.</td>
</tr>
<tr>
<td>clear avc wlan wlan-name stats</td>
<td>Clears the statistics per WLAN.</td>
</tr>
</tbody>
</table>

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
Monitoring SSID and Client Policies Statistics (GUI)

Statistics are supported only for ingress policies with a maximum of five classes on wireless targets. For very large policies, statistics for ingress policies are not visible at the switch. The frequency of the statistics depends on the number of clients associated with the access point.

<table>
<thead>
<tr>
<th>Type of Statistics</th>
<th>Method</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID Policies</td>
<td>Choose Monitor &gt; Controller &gt; Statistics &gt; QoS.</td>
<td>The QoS page is displayed with a list of SSID policies, Radio Type, and AP. Choose an SSID policy, radio, and access point from the drop-down lists and click Apply to view the statistics of the chosen SSID policy. You can view details such as match criteria, confirmed bytes, conformed rate, and exceeded rate.</td>
</tr>
</tbody>
</table>
The Clients page is displayed with a list of client MAC addresses, AP, and other details. Click the MAC address of a client and click the QoS Statistics tab. You can view details such as match criteria, confirmed bytes, conformed rate, and exceeded rate.

### Examples: Application Visibility and Control

#### Examples: Application Visibility Configuration

This example shows how to create a flow record, create a flow monitor, apply the flow record to the flow monitor, and apply the flow monitor on a WLAN:

```plaintext
Switch(config)# configure terminal
Switch(config)# flow record fr_v4
Switch(config-flow-record)# match ipv4 protocol
Switch(config-flow-record)# match ipv4 source address
Switch(config-flow-record)# match ipv4 destination address
Switch(config-flow-record)# match transport destination-port
Switch(config-flow-record)# match flow direction
Switch(config-flow-record)# match application name
Switch(config-flow-record)# match wireless ssid
Switch(config-flow-record)# collect counter bytes long
Switch(config-flow-record)# collect counter packets long
Switch(config-flow-record)# collect wireless ap mac address
Switch(config-flow-record)# collect wireless client mac address
Switch(config)# end
```

```plaintext
Switch(config)# configure terminal
Switch(config)# flow monitor fm_v4
Switch(config-flow-monitor)# record fr_v4
Switch(config-flow-monitor)# cache timeout active 1800
Switch(config)# end
```

```plaintext
Switch(config)# wlan wlan1
Switch(config-wlan)# flow monitor fm_v4 input
Switch(config-wlan)# flow monitor fm_v4 output
Switch(config)# end
```

#### Examples: Application Visibility and Control QoS Configuration

This example shows how to create class maps with apply match protocol filters for application name, category, and subcategory:
Switch# configure terminal
Switch(config)# class-map cat-browsing
Switch(config-cmap)# match protocol attribute category browsing
Switch(config-cmap)# end

Switch# configure terminal
Switch(config)# class-map cat-fileshare
Switch(config-cmap)# match protocol attribute category file-sharing
Switch(config-cmap)# end

Switch# configure terminal
Switch(config)# class-map match-any subcat-terminal
Switch(config-cmap)# match protocol attribute sub-category terminal
Switch(config-cmap)# end

Switch# configure terminal
Switch(config)# class-map match-any webex-meeting
Switch(config-cmap)# match protocol webex-meeting
Switch(config-cmap)# end

This example shows how to create policy maps and define existing class maps for upstream QoS:

Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class cat-browsing
Switch(config-pmap-c)# police 150000
Switch(config-pmap-c)# set dscp 12
Switch(config-pmap-c)# end

Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class cat-fileshare
Switch(config-pmap-c)# police 1000000
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap-c)# end

Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class subcat-terminal
Switch(config-pmap-c)# police 120000
Switch(config-pmap-c)# set dscp 15
Switch(config-pmap-c)# end

Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class webex-meeting
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# set dscp 21
Switch(config-pmap-c)# end

This example shows how to create policy maps and define existing class maps for downstream QoS:

Switch# configure terminal
Switch(config)# policy-map test-avc-down
Switch(config-pmap)# class cat-browsing
Switch(config-pmap-c)# police 200000
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# end
Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class cat-fileshare
Switch(config-pmap-c)# police 300000
Switch(config-pmap-c)# set wlan user-priority 2
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap-c)# end

Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class subcat-terminal
Switch(config-pmap-c)# police 100000
Switch(config-pmap-c)# set dscp 25
Switch(config-pmap-c)# end

Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class webex-meeting
Switch(config-pmap-c)# police 60000000
Switch(config-pmap-c)# set dscp 41
Switch(config-pmap-c)# end

This example shows how to apply defined QoS policy on a WLAN:

Switch# configure terminal
Switch(config)# wlan alpha
Switch(config-wlan)# shut
Switch(config-wlan)# end
Switch(config-wlan)# service-policy client input test-avc-up
Switch(config-wlan)# service-policy client output test-avc-down
Switch(config-wlan)# no shut
Switch(config-wlan)# end

Example: Configuring QoS Attribute for Local Profiling Policy

The following example shows how to configure QoS attribute for a local profiling policy:

Switch(config)# class-map type control subscriber match-all local_policy1_class
Switch(config-filter-control-classmap)# match device-type android
Switch(config)# service-template local_policy1_template
Switch(config-service-template)# vlan 40
Switch(config-service-template)# service-policy qos output local_policy1
Switch(config)# policy-map type control subscriber local_policy1
Switch(config-event-control-policymap)# event identity-update match-all
Switch(config-class-control-policymap)# 1 class local_policy1_class do-until-success
Switch(config-action-control-policymap)# 1 activate service-template local_policy1_template
Switch(config)# wlan open_auth 9
Switch(config-wlan)# client vlan VLAN40
Switch(config-wlan)# service-policy type control subscriber local_policy1
Additional References for Application Visibility and Control

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td><em>System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em></td>
</tr>
<tr>
<td>Flexible NetFlow commands</td>
<td><em>Flexible NetFlow Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em></td>
</tr>
<tr>
<td>QoS configuration</td>
<td><em>QoS Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)</em></td>
</tr>
<tr>
<td>QoS commands</td>
<td><em>QoS Command Reference, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)</em></td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
Feature History and Information For Application Visibility and Control

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3E</td>
<td>AVC control with QoS was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 69

Configuring Voice and Video Parameters

• Finding Feature Information, on page 1331
• Prerequisites for Voice and Video Parameters, on page 1331
• Restrictions for Voice and Video Parameters, on page 1331
• Information About Configuring Voice and Video Parameters, on page 1332
• How to Configure Voice and Video Parameters, on page 1337
• Monitoring Voice and Video Parameters, on page 1347
• Configuration Examples for Voice and Video Parameters, on page 1349
• Additional References for Voice and Video Parameters, on page 1351
• Feature History and Information For Performing Voice and Video Parameters Configuration, on page 1352

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Voice and Video Parameters

You can confirm the following points before configuring voice and video parameters:

• Ensure that the switch has access points connected to it.
• Configure SSID.

Restrictions for Voice and Video Parameters

The following are the restrictions that you should keep in mind while configuring voice and video parameters:

• SIP CAC can be used for the 9971 Cisco phones that support TSPEC-based admission control. You can also use the phones that support Status code 17.
• SIP snooping is supported for providing voice priority to the non-TSPEC SIP phones.
• TSPEC for video CAC is not supported.
• The following features are not supported for the 802.11 module on the Cisco 3600 Access Point:
  • Voice support
  • CAC support
  • TSM support

• When the 802.11ac module is enabled, the 11n LBCAC parameters can be inaccurate resulting in degradation in voice quality of 11ac enabled calls.
• Cisco 792x IP phones that are admitted as non-WMM devices with 11K enabled will experience audio problems with the phones.

---

**Note**

Disable 11K for voice WLAN for all 792x Cisco IP phones that are admitted as non-WMM devices with 11K enabled. Upgrade the firmware on Cisco Unified Call Manager to 1.4.5 to resolve this issue. Refer to the Cisco Unified Call Manager configuration guide for more information.

---

### Information About Configuring Voice and Video Parameters

Three parameters on the switch affect voice and/or video quality:

• Call Admission Control
• Expedited bandwidth requests
• Unscheduled automatic power save delivery

Call Admission Control (CAC) and UAPSD are supported on Cisco Compatible Extensions (CCX) v4 and v5; however, these parameters are also supported even without CCX but on any device implementing WMM (that supports 802.1e). Expedited bandwidth requests are supported only on CCXv5.

Traffic stream metrics (TSM) can be used to monitor and report issues with voice quality.

### Call Admission Control

Call Admission Control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The WMM protocol deployed in CCXv4 maintains QoS under differing network loads.

Two types of Over The Air (OTA) CAC are available: static-based CAC and load-based CAC.

The switch supports the following QoS policies:

• User-defined policies: You can define your own QoS policies. You can have more control over these policies than the existing metal policies.
• System-defined precious metal policies: To support backward compatibility.
  • Platinum: Used for VoIP clients.
  • Gold: Used for video clients.
  • Silver: Used for best effort traffic.
  • Bronze: Used for NRT traffic.

Static-Based CAC

Voice over WLAN applications supporting WMM and TSPEC can specify how much bandwidth or shared medium time is required to initiate a call. Bandwidth-based, or static, CAC enables the access point to determine whether it is capable of accommodating a particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

The QoS setting for a WLAN determines the level of bandwidth-based CAC support. To use bandwidth-based CAC with voice applications, the WLAN must be configured for Platinum QoS. With bandwidth-based CAC, the access point bandwidth availability is determined based on the amount of bandwidth currently used by the access point clients, to which the bandwidth requested by the Voice over WLAN applications is added. If this total exceeds a configured bandwidth threshold, the new call is rejected.

Note
You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, bandwidth-based CAC does not operate properly for these CCXv4 clients.

Load-Based CAC

Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types (including that from clients), cochannel access point loads, and coallocated channel interference, for voice and video applications. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

In load-based CAC, the access point continuously measures and updates the utilization of the RF channel (that is, the mean time of bandwidth that has been exhausted), channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents oversubscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

Note
If you disable load-based CAC, the access points start using bandwidth-based CAC.

IOSd Call Admission Control

IOSd Call Admission Control (CAC) controls bandwidth availability from switch to access point. You can configure class-based, unconditional packet marking features on your switch for CAC.

CAC is a concept that applies to voice and video traffic only—not data traffic. If an influx of data traffic oversubscribes a particular link in the network, queueing, buffering, and packet drop decisions resolve the
congestion. The extra traffic is simply delayed until the interface becomes available to send the traffic, or, if traffic is dropped, the protocol or the end user initiates a timeout and requests a retransmission of the information.

Network congestion cannot be resolved in this manner when real-time traffic, sensitive to both latency and packet loss, is present, without jeopardizing the quality of service (QoS) expected by the users of that traffic. For real-time delay-sensitive traffic such as voice, it is better to deny network access under congestion conditions than to allow traffic onto the network to be dropped and delayed, causing intermittent impaired QoS and resulting in customer dissatisfaction.

CAC is therefore a deterministic and informed decision that is made before a voice call is established and is based on whether the required network resources are available to provide suitable QoS for the new call.

Based on the admit CAC CLI configuration in addition to the existing CAC algorithm, switch allows either voice or video with TSPEC or SIP snooping. The admit cac CLI is mandatory for the voice call to pass through.

If the BSSID policer is configured for the voice or video traffic, then additional checks are performed on the packets.

**Expedited Bandwidth Requests**

The expedited bandwidth request feature enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. When the controller receives this request, it attempts to facilitate the urgency of the call in any way possible without potentially altering the quality of other TSPEC calls that are in progress.

You can apply expedited bandwidth requests to both bandwidth-based and load-based CAC. Expedited bandwidth requests are disabled by default. When this feature is disabled, the controller ignores all expedited requests and processes TSPEC requests as normal TSPEC requests.

The following table lists examples of TSPEC request handling for normal TSPEC requests and expedited bandwidth requests.
Table 99: TSPEC Request Handling Examples

<table>
<thead>
<tr>
<th>CAC Mode</th>
<th>Reserved bandwidth for voice calls</th>
<th>Usage</th>
<th>Normal TSPEC Request</th>
<th>TSPEC with Expedited Bandwidth Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth-based CAC</td>
<td>75% (default setting)</td>
<td>Less than 75%</td>
<td>Admitted</td>
<td>Admitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Between 75% and 90% (reserved bandwidth for voice calls exhausted)</td>
<td>Rejected</td>
<td>Admitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>More than 90%</td>
<td>Rejected</td>
<td>Rejected</td>
</tr>
<tr>
<td>Load-based CAC</td>
<td></td>
<td>Less than 75%</td>
<td>Admitted</td>
<td>Admitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Between 75% and 85% (reserved bandwidth for voice calls exhausted)</td>
<td>Rejected</td>
<td>Admitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>More than 85%</td>
<td>Rejected</td>
<td>Rejected</td>
</tr>
</tbody>
</table>

17 For bandwidth-based CAC, the voice call bandwidth usage is per access point radio and does not take into account cochannel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.

18 Bandwidth-based CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

Note

Admission control for TSPEC G711-20ms and G711-40 ms codec types are supported.

U-APSD

Unscheduled automatic power save delivery (U-APSD) is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. U-APSD is enabled automatically when WMM is enabled.

Traffic Stream Metrics

In a voice-over-wireless LAN (VoWLAN) deployment, traffic stream metrics (TSM) can be used to monitor voice-related metrics on the client-access point air interface. It reports both packet latency and packet loss. You can isolate poor voice quality issues by studying these reports.

The metrics consist of a collection of uplink (client side) and downlink (access point side) statistics between an access point and a client device that supports CCX v4 or later releases. If the client is not CCX v4 or CCXv5 compliant, only downlink statistics are captured. The client and access point measure these metrics. The access point also collects the measurements every 5 seconds, prepares 90-second reports, and then sends the reports.
to the controller. The controller organizes the uplink measurements on a client basis and the downlink measurements on an access point basis and maintains an hour’s worth of historical data. To store this data, the controller requires 32 MB of additional memory for uplink metrics and 4.8 MB for downlink metrics.

TSM can be configured through either the GUI or the CLI on a per radio-band basis (for example, all 802.11a radios). The controller saves the configuration in flash memory so that it persists across reboots. After an access point receives the configuration from the controller, it enables TSM on the specified radio band.

This table shows the upper limit for TSM entries in different controller series.

<table>
<thead>
<tr>
<th>TSM Entries</th>
<th>5700</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAX AP TSM entries</td>
<td>100</td>
</tr>
<tr>
<td>MAX Client TSM entries</td>
<td>250</td>
</tr>
<tr>
<td>MAX TSM entries</td>
<td>100*250=25000</td>
</tr>
</tbody>
</table>

Note: Once the upper limit is reached, additional TSM entries cannot be stored and sent to WCS or NCS. If client TSM entries are full and AP TSM entries are available, then only the AP entries are stored, and vice versa. This leads to partial output. TSM cleanup occurs every one hour. Entries are removed only for those APs and clients that are not in the system.

Information About Configuring Voice Prioritization Using Preferred Call Numbers

You can configure a switch to provide support for SIP calls from VoWLAN clients that do not support TSPEC-based calls. This feature is known as SIP CAC support. If bandwidth is available in the configured voice pool, the SIP call uses the normal flow and the switch allocates the bandwidth to those calls.

You can also prioritize up to six preferred call numbers. When a call comes to one of the configured preferred numbers, the switch does not check the configured maximum voice bandwidth. The switch allocates the bandwidth needed for the call, even if it exceeds the maximum bandwidth for voice configured for voice CAC. The preferred call will be rejected if bandwidth allocation exceeds 85% of the radio bandwidth. The bandwidth allocation is 85 percent of the entire bandwidth pool, not just from the maximum configured voice pool. The bandwidth allocation is the same even for roaming calls.

You must configure the following parameters before configuring voice prioritization:

- Set WLAN QoS to allow voice calls to pass through.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.

Information About Enhanced Distributed Channel Access Parameters

Enhanced Distributed Channel Access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.
## How to Configure Voice and Video Parameters

### Configuring Voice Parameters (CLI)

**Before you begin**

Ensure that you have configured SIP-based CAC.

You should have created a class map for CAC before beginning this procedure.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>show wlan summary</code></td>
<td>Specifies all of the WLANs configured on the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# show wlan summary</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>show wlan wlan_id</code></td>
<td>Specifies the WLAN that you plan to modify. For voice over WLAN, ensure that the WLAN is configured for WMM and the QoS level is set to Platinum.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# show wlan 25</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>policy-map policy-map name</code></td>
<td>Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# policy-map test_2000</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-pmap)#</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-pmap-c)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>`class {class-name</td>
<td>class-default}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-pmap)# class test_1000</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-pmap-c)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>admit cac wmm-tspec</code></td>
<td>(Optional) Admits the request for Call Admission Control (CAC) for policy map.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-pmap-c)# admit cac wmm-tspec</td>
<td></td>
</tr>
<tr>
<td>Switch(config-pmap-c)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> service-policy policy-map name</td>
<td>Configures the QoS service policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-pmap-c)# service-policy test_2000</td>
<td></td>
</tr>
<tr>
<td>Switch(config-pmap-c)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> wlan wlan_profile_name wlan_ID SSID_network_name wlan shutdown</td>
<td>Disables all WLANs with WMM enabled prior to changing the video parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td>Switch(config-wlan)# wlan shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> wlan wlan_profile_name wlan_ID SSID_network_name</td>
<td>Disables all WLANs with WMM enabled prior to changing the voice parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td>Switch(config-wlan)# wlan shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> wlan wlan_name call-snoop</td>
<td>Enables the call-snooping on a particular WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# wlan wlan1 call-snoop</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> wlan wlan_name service-policy input input_policy_name</td>
<td>Configures input SSID policy on a particular WLAN to voice.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td>Switch(config-wlan)# service-policy input platinum-up</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> wlan wlan_name service-policy output output_policy_name</td>
<td>Configures output SSID policy on a particular WLAN to voice.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td>Switch(config-wlan)# service-policy output platinum</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> wlan wlan_name service-policy input ingress_policy_name</td>
<td>Configures ingress SSID policy on a particular WLAN as user-defined policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Example:**
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy input policy1 | **Step 15**
wlan wlan\_name service-policy output egress\_policy\_name

**Example:**
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy output policy2 | Configures egress SSID policy on a particular WLAN as user-defined policy. |
| **Step 16**
ap dot11 {5ghz | 24ghz} shutdown

**Example:** | Disables the radio network. |
| **Step 17**
ap dot11 {5ghz | 24ghz} cac voice sip

**Example:** | Enables or disables SIP IOSd CAC for the 802.11a or 802.11b/g network. |
| **Step 18**
ap dot11 {5ghz | 24ghz} cac voice acm

**Example:** | Enables or disables bandwidth-based voice CAC for the 802.11a or 802.11b/g network. |
| **Step 19**
ap dot11 {5ghz | 24ghz} cac voice max-bandwidth bandwidth

**Example:** | Sets the percentage of maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network. |
| **Step 20**
ap dot11 {5ghz | 24ghz} cac voice roam-bandwidth bandwidth

**Example:** | Sets the percentage of maximum allocated bandwidth reserved for roaming voice clients. |
| **Step 21**
no wlan shutdown

**Example:** | Reenables all WLANs with WMM enabled. |
| **Step 22**
no ap dot11 {5ghz | 24ghz} shutdown

**Example:** | Reenables the radio network. |
### Configuring Video Parameters (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Specifies all of the WLANs configured on the switch.</td>
</tr>
<tr>
<td><code>show wlan summary</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# <code>show wlan summary</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies the WLAN that you plan to modify.</td>
</tr>
<tr>
<td><code>show wlan wlan_id</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# <code>show wlan 25</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. In WLAN, you need to configure service-policy for these commands to take effect.</td>
</tr>
<tr>
<td><code>policy-map policy-map name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# <code>policy-map test_2000</code> Switch(config-pmap)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Specifies the name of the class whose policy you want to create or change. You can also create a system default class for unclassified packets.</td>
</tr>
<tr>
<td>`class {class-name</td>
<td>class-default}`</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-pmap)# <code>class test_1000</code> Switch(config-pmap-c)#</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>6</td>
<td>admit cac wmm-tspec</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config-pmap-c)# admit cac wmm-tspec</td>
</tr>
<tr>
<td></td>
<td>Switch(config-pmap-c)#</td>
</tr>
<tr>
<td>7</td>
<td>service-policy policy-map name</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config-pmap-c)# service-policy test_2000</td>
</tr>
<tr>
<td></td>
<td>Switch(config-pmap-c)#</td>
</tr>
<tr>
<td>8</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td>9</td>
<td>wlan wlan_profile_name</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# wlan wlan1</td>
</tr>
<tr>
<td></td>
<td>Switch(config-wlan)# wlan shutdown</td>
</tr>
<tr>
<td>10</td>
<td>ap dot11 {5ghz</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ap dot11 5ghz shutdown</td>
</tr>
<tr>
<td>11</td>
<td>ap dot11 {5ghz</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ap dot11 5ghz cac video acm</td>
</tr>
<tr>
<td>12</td>
<td>ap dot11 {5ghz</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ap dot11 5ghz cac video load-based</td>
</tr>
<tr>
<td></td>
<td>If you do not enter this command, then the default static CAC is applied.</td>
</tr>
<tr>
<td>13</td>
<td>ap dot11 {5ghz</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ap dot11 5ghz cac video max-bandwidth 20</td>
</tr>
<tr>
<td></td>
<td>The bandwidth range is 5 to 85%, and the default value is 75%. The default value is 0, which means no bandwidth request control. The sum of the voice bandwidth and video bandwidth should not exceed 85% or configured maximum media bandwidth.</td>
</tr>
</tbody>
</table>
### Configuring SIP-Based CAC (CLI)

SIP CAC controls the total number of SIP calls that can be made.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wlan wlan-name</td>
<td>Enters WLAN configuration submode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# wlan qos-wlan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-wlan)#</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>call-snoop</td>
<td>Enables the call-snooping feature for a particular WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-wlan)# call-snoop</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Assigns a policy map to WLAN input traffic. Ensure that you provide QoS policy to voice for input traffic.</td>
<td></td>
</tr>
<tr>
<td>service-policy [client] input policy-map name</td>
<td>Example: Switch(config-wlan)# service-policy input platinum-up</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Assigns policy map to WLAN output traffic. Ensure that you provide QoS policy to voice for output traffic.</td>
<td></td>
</tr>
<tr>
<td>service-policy [client] output policy-map name</td>
<td>Example: Switch(config-wlan)# service-policy output platinum</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Verifies the configured QoS policy on the WLAN.</td>
<td></td>
</tr>
<tr>
<td>show wlan {wlan-id</td>
<td>wlan-name}</td>
<td>Example: Switch# show wlan qos-wlan</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Enables the ACM static on the radio. When enabling SIP snooping, use the static CAC, not the load-based CAC.</td>
<td></td>
</tr>
<tr>
<td>ap dot11 {5ghz</td>
<td>24ghz} cac {voice</td>
<td>video} acm</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Configures SIP-based CAC.</td>
<td></td>
</tr>
<tr>
<td>ap dot11 {5ghz</td>
<td>24ghz} cac voice sip</td>
<td>Example: Switch(config)# ap dot11 5ghz cac voice sip</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Preferred Call Number (CLI)

Before you begin
You must set the following parameters before configuring a preferred call number.

- Set WLAN QoS to voice.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.
- Enable SIP-based CAC.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>wlan wlan-name qos platinum</code></td>
<td>Sets QoS to voice on a particular WLAN.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`ap dot11 {5ghz</td>
<td>24ghz} cac {voice</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>wlan wlan-name</code></td>
<td>Enables the call-snooping feature for a particular WLAN.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>wireless sip preferred-call-no call_index call_number</code></td>
<td>Adds a new preferred call.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>no wireless sip preferred-call-no call_index</code></td>
<td>Removes a preferred call.</td>
</tr>
</tbody>
</table>
### Configuring EDCA Parameters (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap dot11 {5ghz</td>
<td>24ghz } shutdown</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# ap dot11 5ghz shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ap dot11 {5ghz</td>
<td>24ghz} edca-parameters {custom-voice</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# ap dot11 5ghz edca-parameters optimized-voice</td>
<td></td>
</tr>
</tbody>
</table>

**Purpose**

- **End**
  - **Example:** Switch(config)# end
  - Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

---

**Example**
### Configuring EDCA Parameters (GUI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>`no ap dot11 {5ghz</td>
<td>24ghz} shutdown`</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# no ap dot11 5ghz shutdown</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>`show ap dot11 {5ghz</td>
<td>24ghz} network`</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch# show ap dot11 5ghz network</code></td>
<td></td>
</tr>
</tbody>
</table>

**Configuring EDCA Parameters (GUI)**

**Step 1**
Choose **Configuration > Wireless > 802.11a/n/ac > EDCA Parameters** or **Configuration > Wireless > 802.11b/g/n > EDCA Parameters** to open EDCA Parameters page.

**Step 2**
Choose one of the following options from the **EDCA Profile** drop-down list:

- **wmm-default**—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.

- **svp-voice**—Enables SpectraLink voice priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.

- **optimized-voice**—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are deployed on your network.

- **optimized-video-voice**—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
• **custom-voice**—Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.

**Note** If you deploy video services, admission control (ACM) must be disabled.

**Step 3**
If you want to enable MAC optimization for voice, select the **Enable Low Latency MAC** check box. Otherwise, leave this check box unselected, which is the default value. This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, which improves the number of voice calls serviced per access point.

**Note** We do not recommend you to enable low latency MAC. You should enable low latency MAC only if the WLAN allows WMM clients. If WMM is enabled, then low latency MAC can be used with any of the EDCA profiles.

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

**Step 5**  
To reenable the radio network, choose **Network** under 802.11a/n/ac or 802.11b/g/n, select the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box, and click **Apply**.

**Step 6**  
Click **Save Configuration**.

---

**Monitoring Voice and Video Parameters**

This section describes the new commands for the voice and video parameters.

The following commands can be used to monitor voice and video parameters.

**Table 100: Monitoring Voice Parameters Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show ap dot11 [5ghz</td>
<td>24ghz] network`</td>
</tr>
<tr>
<td><code>show ap name ap_name dot11 24ghz tsm all</code></td>
<td>Displays the TSM voice metrics and current status of MAC optimization for voice.</td>
</tr>
<tr>
<td><code>show ap name apname cac voice</code></td>
<td>Displays the information about CAC for a particular access point.</td>
</tr>
<tr>
<td><code>show client detail client_mac</code></td>
<td>Displays the U-APSD status for a particular client.</td>
</tr>
<tr>
<td><code>show policy-map interface wireless client</code></td>
<td>Displays the video client policy details.</td>
</tr>
<tr>
<td><code>show access-list</code></td>
<td>Displays the video client dynamic access-list from the switch.</td>
</tr>
<tr>
<td><code>show wireless client voice diag status</code></td>
<td>Displays information about whether voice diagnostics are enabled or disabled. If enabled, this also displays information about the clients in the watch list and the time remaining for the diagnostics of the voice call.</td>
</tr>
</tbody>
</table>

**Note** To work on voice diagnostics CLIs, you need to enter the following command: `debug voice-diagnostic mac-addr client_mac_01 client_mac_02`
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless client voice diag tspec</td>
<td>Displays the TSPEC information sent from the clients that are enabled for voice diagnostics.</td>
</tr>
<tr>
<td>show wireless client voice diag qos-map</td>
<td>Displays information about the QoS/DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.</td>
</tr>
<tr>
<td>show wireless client voice diag rssi</td>
<td>Display the client’s RSSI values in the last 5 seconds when voice diagnostics is enabled.</td>
</tr>
<tr>
<td>show client voice-diag roam-history</td>
<td>Displays information about the last three roaming calls. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, reason for roaming-failure.</td>
</tr>
<tr>
<td>show policy-map interface wireless mac mac-address</td>
<td>Displays information about the voice and video data packet statistics.</td>
</tr>
<tr>
<td>show wireless media-stream client summary</td>
<td>Displays a summary of the media stream and video client information.</td>
</tr>
<tr>
<td>show controllers d0</td>
<td>b queue</td>
</tr>
<tr>
<td>show platform qos queue stats interface</td>
<td>Displays which queue packets are going through from the switch.</td>
</tr>
</tbody>
</table>

You can monitor the video parameters using the following commands.

**Table 101: Monitoring Video Parameters Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap join stats summary ap_mac</td>
<td>Displays the last join error detail for a specific access point.</td>
</tr>
<tr>
<td>show ip igmp snooping wireless mgid</td>
<td>Displays the TSM voice metrics and current status of MAC optimization for voice.</td>
</tr>
<tr>
<td>show wireless media-stream multicast-direct state</td>
<td>Displays the media stream multicast-direct parameters.</td>
</tr>
<tr>
<td>show wireless media-stream group summary</td>
<td>Displays the summary of the media stream and client information.</td>
</tr>
<tr>
<td>show wireless media-stream group detail group_name</td>
<td>Displays the details of a specific media-stream group.</td>
</tr>
<tr>
<td>show wireless media-stream client summary</td>
<td>Displays the details for a set of media-stream clients.</td>
</tr>
<tr>
<td>show wireless media-stream client detail group_name</td>
<td>Displays the details for a set of media-stream clients.</td>
</tr>
<tr>
<td>show ap dot11 {5ghz</td>
<td>24ghz} media-stream rrc</td>
</tr>
<tr>
<td>show wireless media-stream message details</td>
<td>Displays information about the message configuration.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>show ap name ap-name auto-rf dot11 5ghz i Util</code></td>
<td>Displays the details of channel utilization.</td>
</tr>
<tr>
<td>`show controllers d0</td>
<td>b queue`</td>
</tr>
<tr>
<td>`show controllers d1</td>
<td>b queue`</td>
</tr>
<tr>
<td>`show cont d1</td>
<td>b Media`</td>
</tr>
<tr>
<td><code>show capwap mcast mgid all</code></td>
<td>Displays information about all of the multicast groups and their corresponding multicast group identifications (MGIDs) associated to the access point.</td>
</tr>
<tr>
<td><code>show capwap mcast mgid id id</code></td>
<td>Displays information about all of the video clients joined to the multicast group in a specific MGID.</td>
</tr>
</tbody>
</table>

## Configuration Examples for Voice and Video Parameters

### Example: Configuring Voice and Video

#### Configuring Egress SSID Policy for Voice and Video

The following example shows how to create and configure an egress SSID policy for voice and video:

```plaintext
table-map egress_ssid_tb
  map from 24 to 24
  map from 34 to 34
  map from 46 to 46
  default copy

class-map match-any voice
  match dscp ef

class-map match-any video
  match dscp af41

policy-map ssid-cac
  class class-default
    shape average 25000000
    set dscp dscp table egress_ssid_tb
    queue-buffers ratio 0
    service-policy ssid-child-cac

policy-map ssid-child-cac
  class voice
    priority level 1
    police 5000000
    conform-action transmit
    exceed-action drop
    admit cac wmm-tspec
    rate 1000
    wlan-up 6 7
  class video
    priority level 2
```
police 10000000
   conform-action transmit
   exceed-action drop
   admit cac wmm-tspec
   rate 3000
   wlan-up 4 5

Configuring Ingress SSID Policy for Voice and Video

The following example shows how to create and configure an ingress SSID policy for voice and video:

table-map up_to_dscp
   map from 0 to 0
   map from 1 to 8
   map from 2 to 8
   map from 3 to 0
   map from 4 to 34
   map from 5 to 34
   map from 6 to 46
   map from 7 to 48
   default copy

policy-map ingress_ssid
   class class-default
      set dscp wlan user-priority table up_to_dscp

Configuring Egress Port Policy Voice and Video

The following example shows how to create and configure an egress port policy for voice and video:

policy-map port_child_policy
   class non-client-nrt-class
      bandwidth remaining ratio 10

   class voice
      priority level 1
      police rate 3000000

   class video
      priority level 2
      police rate 4000000

Applying Ingress and Egress SSID policies for Voice and Video on a WLAN

The following example shows how to apply ingress and egress SSID policies for voice and video on a WLAN:

wlan voice_video 1 voice_video
   service-policy input ingress_ssid
   service-policy output ssid-cac
# Additional References for Voice and Video Parameters

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast configuration</td>
<td><em>Multicast Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em></td>
</tr>
<tr>
<td>VideoStream configuration</td>
<td><em>VideoStream Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em></td>
</tr>
</tbody>
</table>

## Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
## Feature History and Information For Performing Voice and Video Parameters Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring RFID Tag Tracking

- Finding Feature Information, on page 1353
- Information About Configuring RFID Tag Tracking, on page 1353
- How to Configure RFID Tag Tracking, on page 1353
- Monitoring RFID Tag Tracking Information, on page 1354
- Additional References RFID Tag Tracking, on page 1355
- Feature History and Information For Performing RFID Tag Tracking Configuration, on page 1356

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring RFID Tag Tracking

The device enables you to configure radio-frequency identification (RFID) tag tracking. RFID tags are small wireless devices that are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller, and the location appliance.

How to Configure RFID Tag Tracking

Configuring RFID Tag Tracking (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>location rfid status</td>
<td>Enables RFID tag tracking.</td>
</tr>
</tbody>
</table>
### Monitoring RFID Tag Tracking Information

This section describes the new commands for the RFID tag tracking Information.

The following commands can be used to monitor the RFID tag tracking Information on the switch.

#### Table 102: Monitoring RFID Tag Tracking Information Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show location rfid config</td>
<td>Displays the current configuration for RFID tag tracking.</td>
</tr>
</tbody>
</table>
show location rfid detail `mac_address` | Displays the detailed information for a specific RFID tag.
--- | ---
show location rfid summary | Displays a list of all RFID tags currently connected to the switch.
show location rfid client | Displays a list of RFID tags that are associated to the switch as clients.

## Additional References RFID Tag Tracking

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td><em>System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em></td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
# Feature History and Information For Performing RFID Tag Tracking Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 71

Configuring Location Settings

- Finding Feature Information, on page 1357
- Information About Configuring Location Settings, on page 1357
- How to Configure Location Settings, on page 1358
- Monitoring Location Settings and NMSP Settings, on page 1362
- Examples: Location Settings Configuration, on page 1363
- Examples: NMSP Settings Configuration, on page 1363
- Additional References for Location Settings, on page 1363
- Feature History and Information For Performing Location Settings Configuration, on page 1364

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Location Settings

The switch determines the location of client devices by gathering Received Signal Strength Indication (RSSI) measurements from access points all around the client of interest. The switch can obtain location reports from up to 16 access points for clients, RFID tags, and rogue access points.

You can configure the path loss measurement (S60) request for normal clients or calibrating clients to improve location accuracy.
# How to Configure Location Settings

## Configuring Location Settings (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>location plm {calibrating [multiband</td>
<td>uniband]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# location plm client 100</td>
<td>The path loss measurement request improves the location accuracy. You can configure the <strong>burst_interval</strong> parameter for the normal, noncalibrating client from zero through 3600 seconds, and the default value is 60 seconds. You can configure the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio or on the associated 802.11a/b/g radio. If a client does not send probes often or sends them only on a few channels, its location cannot be updated or cannot be updated accurately. The <strong>location plm</strong> command forces clients to send more packets on all channels. When a CCXv4 (or higher) client associates, the Switch sends it a path loss measurement request, which instructs the client to transmit on the bands and channels that the access points are on (typically, channels 1, 6, and 11 for 2.4-GHz-only access points) at a configurable interval (such as 60 seconds) indefinitely.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>location rssi-half-life {calibrating-client</td>
<td>client</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# location rssi-half-life calibrating-client 60</td>
<td>You can enter the <strong>location rssi-half-life</strong> parameter value for the clients, calibrating clients, RFID tags, and rogue access points as 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 4** location expiry { calibrating-client | client | rogue-aps | tags } timeout | Some client devices transmit at reduced power immediately after changing channels, and RF is variable, so RSSI values might vary considerably from packet to packet. The location rssi-half-life command increases accuracy by averaging nonuniformly arriving data using a configurable forget period (or half life).  
**Note** We recommend that you do not use or modify the location rssi-half-life command. |

**Example:**
Switch(config)# location expiry calibrating-client 50

| Step 5 location algorithm { rssi-average | simple} | Configures the RSSI timeout value for the clients, calibrating clients, RFID tags, and rogue access points.  
You can enter the RSSI timeout value for the clients, RFID tags, and rogue access points from 5 through 3600 seconds, and the default value is 5 seconds.  
For the calibrating clients, you can enter the RSSI timeout value from 0 through 3600 seconds, and the default value is 5 seconds.  
Ensuring that recent, strong RSSIs are retained by the CPU is critical to location accuracy. The location expiry command enables you to specify the length of time after which old RSSI averages expire.  
**Note** We recommend that you do not use or modify the location expiry command. |

**Example:**
Switch(config)# location algorithm rssi-average

| Step 5 location algorithm { rssi-average | simple} | Configures the algorithm used to average RSSI and signal-to-noise ratio (SNR) values.  
You can enter the location algorithm rssi-average command to specify a more accurate algorithm but requires more CPU overhead or the location algorithm simple command to specify a faster algorithm that requires low CPU overhead but provides less accuracy.  
**Note** We recommend that you do not use or modify the location algorithm command. |

**Example:**
Switch(config)# location algorithm rssi-average
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 6    | **location admin-tag** `string`  
**Example:**  
`Switch(config)# location admin-tag` | Sets administrative tag or site information for the location of client devices. |
| 7    | **location civic-location** identifier `{identifier | host}`  
**Example:**  
`Switch(config)# location civic-location identifier host` | Specifies civic location information.  
You can set the civic location identifier either as a string or host. |
| 8    | **location custom-location** identifier `{identifier | host}`  
**Example:**  
`Switch(config)# location custom-location identifier host` | Specifies custom location information.  
You can set the custom location identifier either as a string or host. |
| 9    | **location geo-location** identifier `{identifier | host}`  
**Example:**  
`Switch(config)# location geo-location identifier host` | Specifies geographical location information of the client devices.  
You can set the location identifier either as a string or host. |
| 10   | **location prefer** `{cdp | lldp-med | static}` weight `priority_value`  
**Example:**  
`Switch(config)# location prefer weight cdp 50` | Sets location information source priority.  
You can enter the priority weight from zero through 255. |
| 11   | **location rfid** `{status | timeout | vendor-name}`  
**Example:**  
`Switch(config)# location rfid timeout 100` | Configures RFID tag tracking options such as RFID tag status, RFID timeout value, and RFID tag vendor name.  
You can enter the RFID timeout value in a range from 60 and 7200 seconds. |
| 12   | `end`  
**Example:**  
`Switch(config)# end` | Returns to privileged EXEC mode.  
Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. |

**Example**

### Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues

NMSP manages communication between the Cisco Mobility Services Engine (Cisco MSE) and the controller for incoming and outgoing traffic. If your application requires more frequent location updates, you can modify...
the NMSP notification interval (to a value between 1 and 180 seconds) for clients, active RFID tags, and rogue access points and clients.

**Note**
The TCP port (16113) that the controller and Cisco MSE communicate over must be open (not blocked) on any firewall that exists between the controller and the Cisco MSE for NMSP to function.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**  
```
nmsp notification interval {attachment seconds | location seconds | rssi [clients interval | rfid interval | rogues [ap | client ] interval]}
```

**Example:**  
```
Switch(config)# nmsp notification interval rssi rfid 50
```

**Step 3**  
```
end
```

**Example:**  
```
Switch(config)# end
```

---

### Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**  
```
location notify-threshold {clients | rogues ap | tags } threshold
```

**Example:**  
```
Switch(config)# location notify-threshold clients 5
```

**Step 3**  
```
end
```

**Example:**  
```
Switch(config)# end
```
Monitoring Location Settings and NMSP Settings

Monitoring Location Settings (CLI)

This section describes the new commands for location settings.
The following commands can be used to monitor location settings on the switch.

Table 103: Monitoring Location Settings Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show location summary</td>
<td>Displays the current location configuration values.</td>
</tr>
<tr>
<td>show location statistics rfid</td>
<td>Displays the location-based RFID statistics.</td>
</tr>
<tr>
<td>show location detail client_mac_addr</td>
<td>Displays the RSSI table for a particular client.</td>
</tr>
</tbody>
</table>

Monitoring NMSP Settings (CLI)

The following commands can be used to monitor NMSP settings on the switch.

Table 104: Monitoring NMSP Settings Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show nmsp attachment suppress interfaces</td>
<td>Displays the attachment suppress interfaces.</td>
</tr>
<tr>
<td>show nmsp capability</td>
<td>Displays the NMSP capabilities.</td>
</tr>
<tr>
<td>show nmsp notification interval</td>
<td>Displays the NMSP notification intervals.</td>
</tr>
<tr>
<td>show nmsp statistics connection</td>
<td>Displays the connection-specific NMSP counters.</td>
</tr>
<tr>
<td>show nmsp statistics summary</td>
<td>Displays the common NMSP counters.</td>
</tr>
<tr>
<td>show nmsp status</td>
<td>Displays the status of active NMSP connections.</td>
</tr>
<tr>
<td>show nmsp subscription detail</td>
<td>Displays all of the mobility services to which the switch is subscribed.</td>
</tr>
<tr>
<td>show nmsp subscription detail ip_addr</td>
<td>Displays details only for the mobility services subscribed to by a specific IP address.</td>
</tr>
<tr>
<td>show nmsp subscription summary</td>
<td>Displays details for all of the mobility services to which the switch is subscribed.</td>
</tr>
</tbody>
</table>
Examples: Location Settings Configuration

This example shows how to configure the path loss measurement (S60) request for calibrating client on the associated 802.11a or 802.11b/g radio:

Switch# configure terminal
Switch(config)# location plm calibrating uniband
Switch(config)# end
Switch# show location summary

This example shows how to configure the RSSI half life for a rogue access point:

Switch# configure terminal
Switch(config)# location rssi-half-life rogue-aps 20
Switch(config)# end
Switch# show location summary

Examples: NMSP Settings Configuration

This example shows how to configure the NMSP notification interval for RFID tags:

Switch# configure terminal
Switch(config)# nmsp notification interval rssi rfid 50
Switch(config)# end
Switch# show nmsp notification interval

This example shows how to configure the NMSP notification interval for clients:

Switch# configure terminal
Switch(config)# nmsp notification interval rssi clients 180
Switch(config)# end
Switch# show nmsp notification interval

Additional References for Location Settings

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td>System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information For Performing Location Settings Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Monitoring Flow Control

- Finding Feature Information, on page 1365
- Information About Flow Control, on page 1365
- Monitoring Flow Control, on page 1365
- Examples: Monitoring Flow Control, on page 1366
- Additional References for Monitoring Flow Control, on page 1367
- Feature History and Information For Monitoring Flow Control, on page 1367

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Flow Control

Flow control is enabled by default on the switch.

Flow control provides shim layers between WCM and Cisco IOS for a reliable IPC. Every component in WCM has a dedicated channel. Few of the components in WCM have leveraged flow control in that. There is no configuration of flow control from CLI. You can monitor the flow control for any channel.

Monitoring Flow Control

This section describes the new commands for flow control.

The following commands can be used to monitor flow control on the switch.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>

Table 105: Monitoring Flow Control
Displays information about flow control on a particular channel.

show wireless flow-control channel-id

Displays statistical information about flow control on a particular channel.

show wireless flow-control channel-id statistics

Examples: Monitoring Flow Control

This example shows how to view information pertaining to any channel:

Switch# show wireless flow-control 3
Switch#

Channel Name : CAPWAP
FC State : Disabled
Remote Server State : Enabled
Pass-thru Mode : Disabled
EnQ Disabled : Disabled
Queue Depth : 2048
Max Retries : 5
Min Retry Gap (mSec): 3

This example shows how to view flow control for a particular channel:

Switch# show wireless flow-control 3
Switch#

Channel Name : CAPWAP
# of times channel went into FC : 0
# of times channel came out of FC : 0
Total msg count received by the FC Infra : 1
Pass-thru msgs send count : 0
Pass-thru msgs fail count : 0
# of msgs successfully queued : 0
# of msgs for which queuing failed : 0
# of msgs sent thru after queuing : 0
# of msgs sent w/o queuing : 1
# of msgs for which send failed : 0
# of invalid EAGAINs received : 0
Highest watermark reached : 0
# of times Q hit max capacity : 0
Avg time channel stays in FC (mSec) : 0
Additional References for Monitoring Flow Control

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information For Monitoring Flow Control

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 73

Configuring System Message Logs

- Finding Feature Information, on page 1369
- Restrictions for Configuring System Message Logs, on page 1369
- Information About Configuring System Message Logs, on page 1369
- How to Configure System Message Logs, on page 1372
- Monitoring and Maintaining System Message Logs, on page 1380
- Configuration Examples for System Message Logs, on page 1380
- Additional References for System Message Logs, on page 1381
- Feature History and Information For System Message Logs, on page 1382

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring System Message Logs

When the logging discriminator command is configured, the device may experience memory leak or crash. This usually happens during heavy syslog or debug output. The rate of the memory leak is dependent on the number of logs being produced. In extreme cases, the device may also crash. As a workaround, use the no logging discriminator command to disable the logging discriminator.

Information About Configuring System Message Logs

System Message Logging

By default, a switch sends 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.

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 appear on the active consoles 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 consoles and each of the destinations. You can time-stamp log messages or set the syslog source address to enhance real-time debugging and management. For information on possible messages, see the system message guide for this release.

You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. The switch software saves syslog messages in an internal buffer on a standalone switch. If a standalone switch, the log is lost unless you had saved it to flash memory.

You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch through Telnet, through the console port, or through the Ethernet management port.

---

**Note**

The syslog format is compatible with 4.3 BSD UNIX.

---

### System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information, if configured. Depending on the switch, messages appear in one of these formats:

- `seq no:timestamp: %facility-severity-MNEMONIC: description (hostname-n)`
- `seq no:timestamp: %facility-severity-MNEMONIC: description`

The part of the message preceding the percent sign depends on the setting of these global configuration commands:

- `service sequence-numbers`
- `service timestamps log datatime`
- `service timestamps log datatime [localtime] [msec] [show-timezone]`
- `service timestamps log uptime`

---

**Table 106: System Log Message Elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seq no:</code></td>
<td>Stamps log messages with a sequence number only if the <code>service sequence-numbers</code> global configuration command is configured.</td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>timestamp formats:</td>
<td><em>mm/dd h h:mm:ss</em> or <em>hh:mm:ss</em> (short uptime) or <em>d h</em> (long uptime)</td>
</tr>
<tr>
<td>facility</td>
<td>The facility to which the message refers (for example, SNMP, SYS, and so forth).</td>
</tr>
<tr>
<td>severity</td>
<td>Single-digit code from 0 to 7 that is the severity of the message.</td>
</tr>
<tr>
<td>MNEMONIC</td>
<td>Text string that uniquely describes the message.</td>
</tr>
<tr>
<td>description</td>
<td>Text string containing detailed information about the event being reported.</td>
</tr>
<tr>
<td>hostname-n</td>
<td>Hostname of a stack member and its switch number in the stack. Though the host is a stack member, it does not append its hostname to system messages.</td>
</tr>
</tbody>
</table>

### Default System Message Logging Settings

**Table 107: Default System Message Logging Settings**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>System message logging to the console</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Console severity</td>
<td>Debugging.</td>
</tr>
<tr>
<td>Logging file configuration</td>
<td>No filename specified.</td>
</tr>
<tr>
<td>Logging buffer size</td>
<td>4096 bytes.¹⁹</td>
</tr>
<tr>
<td>Logging history size</td>
<td>1 message.</td>
</tr>
<tr>
<td>Time stamps</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Synchronous logging</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Logging server</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Syslog server IP address</td>
<td>None configured.</td>
</tr>
<tr>
<td>Server facility</td>
<td>Local7</td>
</tr>
<tr>
<td>Server severity</td>
<td>Informational.</td>
</tr>
</tbody>
</table>

¹⁹ For Cisco IOS XE 3.6E release, the default logging buffer size is 16384 bytes.
Syslog Message Limits

If you 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 switch history table. You also can 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 are stored in the history table even if syslog traps are not enabled.

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.

The history table lists the level keywords and severity level. For SNMP usage, the severity level values increase by 1. For example, `emergencies` equal 1, not 0, and `critical` equals 3, not 2.

Enabling Syslog Trap Messages

You can enable Syslog traps using the `snmp-server enable traps syslog` command.

After enabling Syslog traps, you have to specify the trap message severity. Use the `logging snmp-trap` command to specify the trap level. By default, the command enables severity 0 to 4. To enable all the severity level, configure the `logging snmp-trap 0 7` command.

To enable individual trap levels, configure the following commands:

- `logging snmp-trap emergencies`: Enables only severity 0 traps.
- `logging snmp-trap alert`: Enables only severity 1 traps.

Note that, along with the Syslog traps, the Syslog history should also be applied. Without this configuration, Syslog traps are not sent.

Use the `logging history informational` command to enable the Syslog history.

How to Configure System Message Logs

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console.

This task is optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

Example:
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td>Logs messages to an internal buffer on the switch or on a standalone switch or, in the case of a switch stack, on the . The range is 4096 to 2147483647 bytes. The default buffer size is 4096 bytes. If a standalone switch or the . fails, the log file is lost unless you previously saved it to flash memory. See Step 4. <strong>Note</strong> Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should <em>not</em> be set to this amount.</td>
</tr>
<tr>
<td><strong>Step 2</strong> logging buffered [size]</td>
<td>Logs messages to a UNIX syslog server host. <em>host</em> specifies 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.</td>
</tr>
<tr>
<td><strong>Step 3</strong> logging host</td>
<td>Logs messages to a UNIX syslog server host. <em>host</em> specifies 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.</td>
</tr>
</tbody>
</table>
| **Step 4** logging file flash: filename [max-file-size [min-file-size]] [severity-level-number | type] | Stores log messages in a file in flash memory on a standalone switch or, in the case of a switch stack, on the .  
  • *filename*—Enters the log message filename.  
  • (Optional) **max-file-size**—Specifies the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes.  
  • (Optional) **min-file-size**—Specifies the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes.  
  • (Optional) **severity-level-number | type**—Specifies either the logging severity level or the logging type. The severity range is 0 to 7. | type] |
Synchronizing Log Messages

You can synchronize unsolicited messages and `debug` privileged EXEC command output with solicited device output and prompts for a specific console port line or virtual terminal line. You can identify the types of messages to be output asynchronously based on the level of severity. You can also configure the maximum number of buffers for storing asynchronous messages for the terminal after which messages are dropped.

When synchronous logging of unsolicited messages and `debug` command output is enabled, unsolicited device output appears on the console or printed after solicited device output appears or is printed. Unsolicited messages and `debug` command output appear on the console after the prompt for user input is returned. Therefore, unsolicited messages and `debug` command output are not interspersed with solicited device output and prompts. After the unsolicited messages appear, the console again displays the user prompt.

This task is optional.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> line [console</td>
<td>vty] line-number [ending-line-number]</td>
</tr>
<tr>
<td>Example: Switch(config)# line console</td>
<td>• <code>console</code>—Specifies configurations that occur through the switch console port or the Ethernet management port.</td>
</tr>
<tr>
<td></td>
<td>• <code>line vty line-number</code>—Specifies which vty lines are to have synchronous logging enabled. You use a vty connection for configurations that occur through a Telnet</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong> logging synchronous [level [severity-level</td>
<td>Enables synchronous logging of messages.</td>
</tr>
<tr>
<td>all]]</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# logging synchronous level 3 limit 1000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Disabling 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, which logs messages to designated locations asynchronously to the processes that generated the messages.
Disabling the logging process can slow down the switch because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages appear 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**.

To reenable message logging after it has been disabled, use the **logging on** global configuration command.

This task is optional.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>no logging console</td>
<td>Enables message logging.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# no logging console</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling and Disabling Time Stamps on Log Messages

By default, log messages are not time-stamped.

This task is optional.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables log time stamps.</td>
</tr>
<tr>
<td>Use one of these commands:</td>
<td></td>
</tr>
</tbody>
</table>
Enabling and Disabling Sequence Numbers in Log Messages

If there is more than one log message with the same time stamp, you can display messages with sequence numbers to view these messages. By default, sequence numbers in log messages are not displayed. This task is optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> service sequence-numbers</td>
<td>Enables sequence numbers.</td>
</tr>
<tr>
<td>Example: Switch(config)# service sequence-numbers</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Defining the Message Severity Level

Limit messages displayed to the selected device by specifying the severity level of the message. This task is optional.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>logging console level</td>
<td>Limits messages logged to the console. By default, the console receives debugging messages and numerically lower levels.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# logging console 3</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>logging monitor level</td>
<td>Limits messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# logging monitor 3</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>logging trap level</td>
<td>Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# logging trap 3</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Limiting Syslog Messages Sent to the History Table and to SNMP

This task explains how to limit syslog messages that are sent to the history table and to SNMP. This task is optional.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> logging history level</td>
<td>Changes the default level of syslog messages stored in the history file and sent to the SNMP server.</td>
</tr>
<tr>
<td>Example:</td>
<td>By default, <strong>warnings</strong>, <strong>errors</strong>, <strong>critical</strong>, <strong>alerts</strong>, and <strong>emergencies</strong> messages are sent.</td>
</tr>
<tr>
<td>Switch(config)# logging history 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> logging history size number</td>
<td>Specifies the number of syslog messages that can be stored in the history table.</td>
</tr>
<tr>
<td>Example:</td>
<td>The default is to store one message. The range is 0 to 500 messages.</td>
</tr>
<tr>
<td>Switch(config)# logging history size 200</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Logging Messages to a UNIX Syslog Daemon

This task is optional.

**Note**

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 decide what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

**Before you begin**

- Log in as root.
- Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server.
Monitoring and Maintaining System Message Logs

Monitoring Configuration Archive Logs

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show archive log config {all</td>
<td>number [end-number]</td>
</tr>
</tbody>
</table>

Configuration Examples for System Message Logs

Example: Switch System Message

This example shows a partial switch system message on a switch:

```
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
```
Additional References for System Message Logs

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td>System Management Command Reference (Catalyst 3850 Switches) System Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Platform-independent command references</td>
<td>Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Platform-independent configuration information</td>
<td>Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information For System Message Logs

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Online Diagnostics

Online Diagnostics

With online diagnostics, you can test and verify the hardware functionality of the Switch while the Switch is connected to a live network.

The online diagnostics contain packet switching tests that check different hardware components and verify the data path and the control signals.

The online diagnostics detect problems in these areas:

- Hardware components
- Interfaces (Ethernet ports and so forth)
- Solder joints
Online diagnostics are categorized as on-demand, scheduled, or health-monitoring diagnostics. On-demand diagnostics run from the CLI; scheduled diagnostics run at user-designated intervals or at specified times when the Switch is connected to a live network; and health-monitoring runs in the background with user-defined intervals. By default, the health-monitoring test runs for every 30 seconds.

After you configure online diagnostics, you can manually start diagnostic tests or display the test results. You can also see which tests are configured for the Switch or switch stack and the diagnostic tests that have already run.

## How to Configure Online Diagnostics

### Starting Online Diagnostic Tests

After you configure diagnostic tests to run on the Switch, use the `diagnostic start` privileged EXEC command to begin diagnostic testing.

After starting the tests, you cannot stop the testing process.

Use this privileged EXEC command to manually start online diagnostic testing:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Starts the diagnostic tests.</td>
</tr>
<tr>
<td>`diagnostic start switch number test {name</td>
<td>test-id</td>
</tr>
<tr>
<td></td>
<td>• <em>name</em>—Enters the name of the test.</td>
</tr>
<tr>
<td></td>
<td>• <em>test-id</em>—Enters the ID number of the test.</td>
</tr>
<tr>
<td></td>
<td>• <em>test-id-range</em>—Enters the range of test IDs by using integers separated by a comma and a hyphen.</td>
</tr>
<tr>
<td></td>
<td>• <em>all</em>—Starts all of the tests.</td>
</tr>
<tr>
<td></td>
<td>• <em>basic</em>—Starts the basic test suite.</td>
</tr>
<tr>
<td></td>
<td>• <em>complete</em>—Starts the complete test suite.</td>
</tr>
<tr>
<td></td>
<td>• <em>minimal</em>—Starts the minimal bootup test suite.</td>
</tr>
<tr>
<td></td>
<td>• <em>non-disruptive</em>—Starts the non-disruptive test suite.</td>
</tr>
<tr>
<td></td>
<td>• <em>per-port</em>—Starts the per-port test suite.</td>
</tr>
</tbody>
</table>
Configuring Online Diagnostics

You must configure the failure threshold and the interval between tests before enabling diagnostic monitoring.

Scheduling Online Diagnostics

You can schedule online diagnostics to run at a designated time of day or on a daily, weekly, or monthly basis for a Switch. Use the `no` form of this command to remove the scheduling.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Schedules on-demand diagnostic tests for a specific day and time.</td>
</tr>
<tr>
<td>`diagnostic schedule switch number test {name</td>
<td>test-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# diagnostic schedule switch 3 test 1-5 on July 3 2013 23:10</td>
<td></td>
</tr>
</tbody>
</table>

- **name**—Name of the test that appears in the `show diagnostic content` command output.
- **test-id**—ID number of the test that appears in the `show diagnostic content` command output.
- **test-id-range**—ID numbers of the tests that appear in the `show diagnostic content` command output.
- **all**—All test IDs.
- **basic**—Starts the basic on-demand diagnostic tests.
- **complete**—Starts the complete test suite.
- **minimal**—Starts the minimal bootup test suite.
- **non-disruptive**—Starts the non-disruptive test suite.
- **per-port**—Starts the per-port test suite.

You can schedule the tests as follows:

- Daily—Use the `daily hh:mm` parameter.
Configuring Health-Monitoring Diagnostics

You can configure health-monitoring diagnostic testing on a Switch while it is connected to a live network. You can configure the execution interval for each health-monitoring test, enable the Switch to generate a syslog message because of a test failure, and enable a specific test.

Use the `no` form of this command to disable testing.

By default, health monitoring is disabled, but the Switch generates a syslog message when a test fails.

Follow these steps to configure and enable the health-monitoring diagnostic tests:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>`diagnostic monitor interval switch number test {name</td>
<td>test-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# diagnostic monitor interval switch 2 test 1 12:30:00 750 5</td>
<td>When specifying the tests, use one of these parameters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>name</code>—Name of the test that appears in the <code>show diagnostic content</code> command output.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>test-id</code>—ID number of the test that appears in the <code>show diagnostic content</code> command output.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>test-id-range</code>—ID numbers of the tests that appear in the <code>show diagnostic content</code> command output.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>all</strong>—All of the diagnostic tests.</td>
<td>When specifying the interval, set these parameters:</td>
</tr>
<tr>
<td>• <strong>hh:mm:ss</strong>—Monitoring interval in hours, minutes, and seconds. The range for <strong>hh</strong> is 0 to 24, and the range for <strong>mm</strong> and <strong>ss</strong> is 0 to 60.</td>
<td></td>
</tr>
<tr>
<td>• <strong>milliseconds</strong>—Monitoring interval in milliseconds (ms). The range is from 0 to 999.</td>
<td></td>
</tr>
<tr>
<td>• <strong>day</strong>—Monitoring interval in the number of days. The range is from 0 to 20.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 4

**diagnostic monitor syslog**

**Example:**

```
Switch(config)# diagnostic monitor syslog
```

(Optional) Configures the switch to generate a syslog message when a health-monitoring test fails.

### Step 5

**diagnostic monitor threshold switch number number test {name | test-id | test-id-range | all} failure count count**

**Example:**

```
Switch(config)# diagnostic monitor threshold switch 2 test 1 failure count 20
```

(Optional) Sets the failure threshold for the health-monitoring tests. When specifying the tests, use one of these parameters:

- **name**—Name of the test that appears in the `show diagnostic content` command output.
- **test-id**—ID number of the test that appears in the `show diagnostic content` command output.
- **test-id-range**—ID numbers of the tests that appear in the `show diagnostic content` command output.
- **all**—All of the diagnostic tests.

The range for the failure threshold `count` is 0 to 99.

### Step 6

**diagnostic monitor switch number test {name | test-id | test-id-range | all}**

**Example:**

```
Switch(config)# diagnostic monitor switch 2 test 1
```

Enables the specified health-monitoring tests.

The `switch number` keyword is supported only on stacking switches. When specifying the tests, use one of these parameters:
### Monitoring and Maintaining Online Diagnostics

#### Displaying Online Diagnostic Tests and Test Results

You can display the online diagnostic tests that are configured for the Switch or Switch stack and check the test results by using the privileged EXEC show commands in this table:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>name—Name of the test that appears in the show diagnostic content command output.</td>
<td></td>
</tr>
<tr>
<td>test-id—ID number of the test that appears in the show diagnostic content command output.</td>
<td></td>
</tr>
<tr>
<td>test-id-range—ID numbers of the tests that appear in the show diagnostic content command output.</td>
<td></td>
</tr>
<tr>
<td>all—All of the diagnostic tests.</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 7

**Example:**

```
Step 7
Switch(config)# end
```

Returns to privileged EXEC mode.

#### Step 8

**Example:**

```
Step 8
Switch# show running-config
```

Verifies your entries.

#### Step 9

**Example:**

```
Step 9
Switch# copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

### What to do next

Use the **no diagnostic monitor interval test test-id | test-id-range** global configuration command to change the interval to the default value or to zero. Use the **no diagnostic monitor syslog** command to disable generation of syslog messages when a health-monitoring test fails. Use the **diagnostic monitor threshold test test-id | test-id-range** failure count command to remove the failure threshold.
### Configuration Examples for Online Diagnostic Tests

#### Examples: Start Diagnostic Tests

This example shows how to start a diagnostic test by using the test name:

```
Switch# diagnostic start switch 2 test TestInlinePwrCtlr
```

This example shows how to start all of the basic diagnostic tests:

```
Switch# diagnostic start switch 1 test all
```

#### Example: Configure a Health Monitoring Test

This example shows how to configure a health-monitoring test:

```
Switch(config)# diagnostic monitor threshold switch 1 test 1 failure count 50
Switch(config)# diagnostic monitor interval switch 1 test TestPortAsicStackPortLoopback
```

#### Examples: Schedule Diagnostic Test

This example shows how to schedule diagnostic testing for a specific day and time on a specific switch:

```
Switch(config)# diagnostic schedule test DiagThermalTest on June 3 2013 22:25
```

This example shows how to schedule diagnostic testing to occur weekly at a certain time on a specific switch:

---

### Table 108: Commands for Diagnostic Test Configuration and Results

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diagnostic content switch [number</td>
<td>all]</td>
</tr>
<tr>
<td>show diagnostic status</td>
<td>Displays the currently running diagnostic tests.</td>
</tr>
<tr>
<td>show diagnostic result switch [number</td>
<td>all] [detail</td>
</tr>
<tr>
<td>show diagnostic switch [number</td>
<td>all] [detail]</td>
</tr>
<tr>
<td>show diagnostic schedule switch [number</td>
<td>all]</td>
</tr>
<tr>
<td>show diagnostic post</td>
<td>Displays the POST results. (The output is the same as the show post command output.)</td>
</tr>
</tbody>
</table>
Examples: Displaying Online Diagnostics

This example shows how to display on demand diagnostic settings:

```
Switch# show diagnostic ondemand settings
Test iterations = 1
Action on test failure = continue
```

This example shows how to display diagnostic events for errors:

```
Switch# show diagnostic events event-type error
Diagnostic events (storage for 500 events, 0 events recorded)
Number of events matching above criteria = 0
No diagnostic log entry exists.
```

This example shows how to display the description for a diagnostic test:

```
Switch# show diagnostic description switch 1 test all
DiagGoldPktTest :
   The GOLD packet Loopback test verifies the MAC level loopback
effectiveness. In this test, a GOLD packet, for which doppler
provides the support in hardware, is sent. The packet loops back
at MAC level and is matched against the stored packet. It is a non
-disruptive test.

DiagThermalTest :
   This test verifies the temperature reading from the sensor is below the yellow
temperature threshold. It is a non-disruptive test and can be run as a health
monitoring test.

DiagFanTest :
   This test verifies all fan modules have been inserted and working properly on the
board
   It is a non-disruptive test and can be run as a health monitoring test.

DiagPhyLoopbackTest :
   The PHY Loopback test verifies the PHY level loopback
functionality. In this test, a packet is sent which loops back
at PHY level and is matched against the stored packet. It is a
disruptive test and cannot be run as a health monitoring test.

DiagScratchRegisterTest :
   The Scratch Register test monitors the health of application-specific
integrated circuits (ASICS) by writing values into registers and reading
back the values from these registers. It is a non-disruptive test and can
be run as a health monitoring test.

DiagPoETest :
   This test checks the PoE controller functionality. This is a disruptive test
and should not be performed during normal switch operation.
```
DiagMemoryTest:
This test runs the exhaustive ASIC memory test during normal switch operation
NG3K utilizes mbist for this test. Memory test is very disruptive
in nature and requires switch reboot after the test.

Switch#

This example shows how to display the boot up level:

Switch# show diagnostic bootup level
Current bootup diagnostic level: minimal
Switch#

Additional References for Online Diagnostics

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td>System Management Command Reference (Catalyst 3850 Switches) System Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Platform-independent command reference</td>
<td>Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Platform-independent configuration information</td>
<td>Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information for Configuring Online Diagnostics

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Predownloading an Image to Access Points

- Finding Feature Information, on page 1393
- Information About Predownloading an Image to an Access Point, on page 1393
- Restrictions for Predownloading an Image to an Access Point, on page 1393
- How to Predownload an Image to an Access Point, on page 1394
- Monitoring the Access Point Predownload Process, on page 1395
- Examples: Access Point Predownload Process, on page 1396
- Additional References for Predownloading an Image to an Access Point, on page 1396
- Feature History and Information For Performing Predownloading an Image to an Access Point, on page 1397

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Predownloading an Image to an Access Point

To minimize network outages, download an upgrade image to an access point from the switch without resetting the access point or losing network connectivity. Previously, you could download an upgrade image to the switch and reset it, causing the access point to go into discovery mode. After the access point discovered the controller with the new image, the access point would download the new image, reset it, go into discovery mode, and rejoin the switch.

Now, you can download the upgrade image to the switch and then download the image to the access point while the network is still up. When both devices are up, the access point discovers and rejoins the switch.

Restrictions for Predownloading an Image to an Access Point

The following are the restrictions for predownloading an image to an access point:
• The maximum number of concurrent predownloads is limited to half the number of concurrent normal image downloads. This limitation allows new access points to join the controller during image downloading.

If you reach the predownload limit, then the access points that cannot get an image sleep for a time between 180 to 600 seconds and then reattempt the predownload.

• Access points with 16-MB total available memory may not have enough free memory to download an upgrade image and may automatically delete crash information files, radio files, and backup images, if any, to free up space. However, this limitation does not affect the predownload process because the predownload image replaces backup image, if any, on the access point.

• All of the primary, secondary, and tertiary controllers should run the same images. Otherwise, the feature will not be effective.

• At the time of reset, you must make sure that all of the access points have downloaded the image.

• An access point can store only 2 software images.

**How to Predownload an Image to an Access Point**

**Predownloading an Image to Access Points (CLI)**

**Before you begin**

There are some prerequisites that you must keep in mind while predownloading an image to an access point:

• Predownloading can be done only when the switch is booted in the install mode.

• You can copy the new image either from the TFTP server, flash image, or USB.

• Before predownloading the new image, you must install the new software using the `software install` command and select `no` to the `reload` option.

• If the latest upgrade image is already present in the AP, predownload will not be triggered. Check whether the primary and backup image versions are the same as the upgrade image, using the `show ap image` command.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Downloads the new image to all the access points or a specific access point connected to the switch.</td>
</tr>
<tr>
<td>ap image predownload</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# ap image predownload</td>
<td></td>
</tr>
<tr>
<td>Switch#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Verifies the access point's predownload status.</td>
</tr>
<tr>
<td>show ap image</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Switch# <code>show ap image</code></td>
<td>This command initially displays the status as Predownloading and then moves to Completed, when download is complete.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Example:</td>
</tr>
<tr>
<td>Switch# <code>ap image swap</code></td>
<td>Swaps the images of the APs that have completed predownload.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Example:</td>
</tr>
<tr>
<td><code>ap image reset</code></td>
<td>Resets the access points.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Example:</td>
</tr>
<tr>
<td><code>reload</code></td>
<td>Resets the system.</td>
</tr>
</tbody>
</table>

## Monitoring the Access Point Predownload Process

This section describes the commands that you can use to monitor the access point predownload process.

While downloading an access point predownload image, enter the `show ap image` command to verify the predownload progress on the corresponding access point:

```
Switch# `show ap image`
Total number of APs : 1

Number of APs
Initiated : 1
Predownloading : 1
Completed predownloading : 0
Not Supported : 0
Failed to Predownload : 0

AP Name | Primary Image | Backup Image | Predownload Status
--------|--------------|--------------|------------------
AP1     | 10.0.1.66    | 10.0.1.66    | Predownloading

Switch# `show ap image`
Total number of APs : 1

Number of APs
Initiated : 1
Predownloading : 0
Completed predownloading : 1
Not Supported : 0
Failed to Predownload : 0

AP Name | Primary Image | Backup Image | Predownload Status
--------|--------------|--------------|------------------
AP1     | 10.0.1.66    | 10.0.1.67    | Complete
Use the following command to view the image details of a particular AP:

Switch# show ap name APe4aa.5dd1.99b0 image

AP Name : APe4aa.5dd1.99b0
Primary Image : 16.6.230.46
Backup Image : 3.0.51.0
Predownload Status : None
Predownload Version : 000.000.000.000
Next Retry Time : N/A
Retry Count : 0

Examples: Access Point Predownload Process

This example shows how to predownload an image to an access point AP1:

Switch# ap image predownload
Switch# show ap image
Switch# ap image swap
Switch# show ap image
Switch# ap image reset
Switch# reload

Additional References for Predownloading an Image to an Access Point

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lightweight access points configuration</td>
<td>Lightweight Access Point Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Lightweight Access Point commands</td>
<td>Lightweight Access Point Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases,</td>
</tr>
<tr>
<td></td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information For Performing Predownloading an Image to an Access Point

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 76

Configuring Wireless Virtual Switching System

- Information About Wireless Virtual Switching System, on page 1399
- Configuring VSS for the Cisco Catalyst 4500 Series Switch (Supervisor Engine 8-E), on page 1401
- Verifying DC Bootup with VSS, on page 1403
- How to Boot a Switch in Wireless Mode, on page 1404

Information About Wireless Virtual Switching System

The Cisco Wireless Virtual Switching System (VSS) is a clustering technology that pools two Cisco Catalyst 4500-E Series Switches into a single virtual switch. In a VSS, the data plane of both the clustered switches are active at the same time in both the chassis. VSS members are connected by virtual switch links (VSLs) using connections between the VSS members. VSLs can carry regular user traffic in addition to the control plane communication between the VSS members.

Note

We recommend that you use 10-Gigabit Ethernet links for a VSL bundle.
The Cisco Catalyst 4500E Supervisor 8-E Switch supports wireless in VSS. It can be operated as a mobility agent (MA) or mobility controller (MC). An MA maintains Control and Provisioning of Wireless Access Points (CAPWAP) tunnels of directly connected access points and client mobility state machine. An MC provides mobility management services for group roaming events.

MA and MC can be co-located on the same switch. AP-count licenses are used only when the switch is in MC mode. The MC is the gatekeeper for tracking the AP-count licenses and decides whether an access point can be included in or not.

**Note**

All the features supported in the wireless mode on a stand-alone chassis are also supported in the wireless VSS mode.


**VSS Conversion Methods**

The wireless VSS can be deployed in a network using any of the following methods:

- Migrating the wired VSS to wireless VSS.
- Migrating the existing wireless network to a wireless VSS network.

**Restrictions**

The wireless VSS feature is supported on Cisco Wireless LAN Controller (WLC) with the following restrictions:

- Multiple APs per port are not supported.
The wireless VSS feature is not supported by Cisco Prime Infrastructure on Cisco IOS XE 3.8.0.

The supervisors cannot be booted in any other mode except the wireless mode.

Related Topics
- Configuring VSS for the Cisco Catalyst 4500 Series Switch (Supervisor Engine 8-E), on page 1401
- Verifying DC Bootup with VSS, on page 1403

Configuring VSS for the Cisco Catalyst 4500 Series Switch (Supervisor Engine 8-E)

The Cisco Wireless Virtual Switching System (VSS) is a clustering technology that pools two Cisco Catalyst 4500-E Series Switches into a single virtual switch. In a VSS, the data plane of both clustered switches are active at the same time in both the chassis. VSS members are connected by virtual switch links (VSLs) using connections between the VSS members. VSLs can carry regular user traffic in addition to the control plane communication between the VSS members.

Procedure

**Step 1**
Assign the virtual switch domain and switch number.

Configure the same virtual switch domain number on both switches of the VSS. The virtual switch domain is a number between 1 and 255. After configuring the domain number, configure one switch as switch number 1 and the other switch as switch number 2.

**Example:**

````
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# switch virtual domain 10
Domain ID 10 config will take effect only after the exec command 'switch convert mode virtual' is issued
SW1(config-vs-domain)# switch 1
SW1(config-vs-domain)# exit

SW2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)# switch virtual domain 10
Domain ID 10 config will take effect only after the exec command 'switch convert mode virtual' is issued
SW2(config-vs-domain)# switch 2
SW2(config-vs-domain)# exit
```

**Step 2**
Configure the VSL port channel.

Configure VSL with a unique port channel on each switch. During the conversion, the VSS configures both the port channels on the VSS active switch. If the VSS standby switch's VSL port channel number has been configured for another use, the VSS comes up in RPR mode. To avoid this situation, check whether both the port channel numbers are available on both the switches.

**Example:**
Step 3 Configure VSL ports.

Add the VSL physical ports to the port-channel. In the following example, interfaces TenGigabitEthernet 1/1 and 1/2 on Switch 1 are connected to interfaces TenGigabitEthernet 1/1 and 1/2 on Switch 2.

**Note** After the interfaces are included in the VSL port-channel with channel-group command, the interfaces move to the “notconnect” status. The interface status will be up, but the line protocol will be down. The interface will be in UP/down (notconnect) status, till the switch is rebooted in step 4.

**Example:**

```
SW1(config)# interface range Te1/1 - 2
SW1(config-if-range)# switchport mode trunk
SW1(config-if-range)# channel-group 5 mode on
WARNING: Interface TenGigabitEthernet1/1 placed in restricted config mode. All extraneous configs removed!
WARNING: Interface TenGigabitEthernet1/2 placed in restricted config mode. All extraneous configs removed!
SW1(config-if-range)# exit

SW2(config)# interface range Te1/1 - 2
SW2(config-if-range)# switchport mode trunk
SW2(config-if-range)# channel-group 10 mode on
WARNING: Interface TenGigabitEthernet1/1 placed in restricted config mode. All extraneous configs removed!
WARNING: Interface TenGigabitEthernet1/2 placed in restricted config mode. All extraneous configs removed!
SW2(config-if-range)# exit
```

Step 4 Convert the Switch to VSS.

Enter the switch convert mode virtual command on Switch 1 for converting switch's mode to Virtual Switch Mode. Enter your confirmation at the next prompt. The system creates a converted configuration file, and saves the file to bootflash.

**Example:**

```
SW1# switch convert mode virtual

This command will convert all interface names to naming convention "interface-type switch-number/slot/port", save the running config to startup-config and reload the switch. Do you want to proceed? [yes/no]: yes
Converting interface names
Building configuration...
Compressed configuration from 6551 bytes to 2893 bytes[OK]
Saving converted configuration to bootflash: ...
```
Destination filename [startup-config.converted_vs-20130124-062921]? 
Please stand by while rebooting the system...

Restarting system.

Rommon (G) Signature verification PASSED
Rommon (P) Signature verification PASSED
FPGA (P) Signature verification PASSED

!Enter the switch convert mode virtual command on Switch 2 for converting the switch's mode to Virtual Switch Mode.

SW2# switch convert mode virtual

This command will convert all interface names to naming convention "interface-type switch-number/slot/port", save the running config to startup-config and reload the switch.

Do you want to proceed? [yes/no]: yes

Converting interface names
Building configuration...
Compressed configuration from 6027 bytes to 2774 bytes[OK]
Saving converted configuration to bootflash: ...
Destination filename [startup-config.converted_vs-20130124-052526]? 
Please stand by while rebooting the system...

Restarting system.

Rommon (G) Signature verification PASSED
Rommon (P) Signature verification PASSED
FPGA (P) Signature verification PASSED

<table>
<thead>
<tr>
<th>Related Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information About Wireless Virtual Switching System, on page 1399</td>
</tr>
<tr>
<td>Verifying DC Bootup with VSS, on page 1403</td>
</tr>
</tbody>
</table>

**Verifying DC Bootup with VSS**

The wireless mode will show dc boot status and errors (if any) during boot up.

vss# show module

Switch Number: 1 Role: Virtual Switch Active
Chassis Type : WS-C4507R+E
Power consumed by backplane : 40 Watts

<table>
<thead>
<tr>
<th>Mod</th>
<th>Ports</th>
<th>Card Type</th>
<th>Model</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>48</td>
<td>10/100/1000BaseT Premium POE E Series</td>
<td>WS-X4748-RJ45V+E</td>
<td>CAT1737LUBS</td>
</tr>
<tr>
<td>4</td>
<td>12</td>
<td>Sup 8-E 10GE (SFP+), 1000BaseX (SFP)</td>
<td>WS-X45-SUP8-E</td>
<td>CAT1746L6B9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M</th>
<th>MAC addresses</th>
<th>Hw</th>
<th>Fw</th>
<th>Sw</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>885a.9244.1740 to 885a.9244.176f</td>
<td>1.3</td>
<td>Ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2894.0f2a.404c to 2894.0f2a.4057</td>
<td>1.0 15.1(1r)SG(0 03.08.00.E.91)</td>
<td>Ok</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod</th>
<th>Redundancy role</th>
<th>Operating mode</th>
<th>Redundancy status</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Active Supervisor</td>
<td>SSO</td>
<td>Active</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod</th>
<th>Submodule</th>
<th>Model</th>
<th>Serial No.</th>
<th>Hw</th>
<th>Status</th>
</tr>
</thead>
</table>

**Related Topics**

Information About Wireless Virtual Switching System, on page 1399
Verifying DC Bootup with VSS, on page 1403
Switch Number: 2 Role: Virtual Switch Standby
Chassis Type: WS-C4503-E
Power consumed by backplane: 0 Watts

<table>
<thead>
<tr>
<th>Mod</th>
<th>Ports</th>
<th>Card Type</th>
<th>Model</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12</td>
<td>Sup 8-E 10GE (SFP+), 1000BaseX (SFP)</td>
<td>WS-X45-SUP8-E</td>
<td>CAT1731L0PF</td>
</tr>
<tr>
<td>3</td>
<td>48</td>
<td>10/100/1000BaseT Premium POE E Series</td>
<td>WS-X4748-RJ45V+E</td>
<td>CAT1418L030</td>
</tr>
</tbody>
</table>

MAC addresses

<table>
<thead>
<tr>
<th>Mod</th>
<th>MAC addresses</th>
<th>Hw</th>
<th>Fw</th>
<th>Sw</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>001b.2a68.48c0 to 001b.2a68.48cb</td>
<td>1.0</td>
<td>15.1(1r)</td>
<td>SG(0 03.08.00.E.91</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>0026.9927.f310 to 0026.9927.f33f</td>
<td>0.4</td>
<td>Ok</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Redundancy role

<table>
<thead>
<tr>
<th>Mod</th>
<th>Redundancy role</th>
<th>Operating mode</th>
<th>Redundancy status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Standby</td>
<td>Supervisor</td>
<td>Standby hot</td>
</tr>
</tbody>
</table>

Related Topics
- Information About Wireless Virtual Switching System, on page 1399
- Configuring VSS for the Cisco Catalyst 4500 Series Switch (Supervisor Engine 8-E), on page 1401

How to Boot a Switch in Wireless Mode

To boot a switch in wireless mode (this is called the install boot), additional steps are required. For more information, see the Install Boot section of the Cisco Catalyst 4500 Supervisor Engine 8-E Wireless Mode Quick-Start Guide at: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/guide-c07-733704.html
CHAPTER 77

Troubleshooting the Software Configuration

This chapter describes how to identify and resolve software problems related to the Cisco IOS software on the switch. Depending on the nature of the problem, you can use the command-line interface (CLI), Device Manager, or Network Assistant to identify and solve problems.

Additional troubleshooting information, such as LED descriptions, is provided in the hardware installation guide.

- Finding Feature Information, on page 1405
- Finding Feature Information, on page 1405
- Information About Troubleshooting the Software Configuration, on page 1406
- How to Troubleshoot the Software Configuration, on page 1414
- Verifying Troubleshoot of the Software Configuration, on page 1427
- Scenarios for Troubleshooting the Software Configuration, on page 1429
- Configuration Examples for Troubleshooting Software, on page 1431
- Additional References for Troubleshooting Software Configuration, on page 1434
- Feature History and Information for Troubleshooting Software Configuration, on page 1435

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Information About Troubleshooting the Software Configuration

Software Failure on a Switch

Switch software can be corrupted during an upgrade by downloading the incorrect file to the switch, and by deleting the image file. In all of these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity.

Related Topics
Recovering from a Software Failure, on page 1414

Lost or Forgotten Password on a Switch

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.

Note
On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message reminds you to return to the default configuration during the recovery process.

Note
You cannot recover encryption password key, when Cisco WLC configuration is copied from one Cisco WLC to another (in case of an RMA).

Related Topics
Recovering from a Lost or Forgotten Password, on page 1417

Power over Ethernet Ports

A Power over Ethernet (PoE) switch port automatically supplies power to one of these connected devices if the switch detects that there is no power on the circuit:

- a Cisco pre-standard powered device (such as a Cisco IP Phone or a Cisco Aironet Access Point)
- an IEEE 802.3af-compliant powered device
- an IEEE 802.3at-compliant powered device

A powered device can receive redundant power when it is connected to a PoE switch port and to an AC power source. The device does not receive redundant power when it is only connected to the PoE port.

After the switch detects a powered device, the switch determines the device power requirements and then grants or denies power to the device. The switch can also detect the real-time power consumption of the device by monitoring and policing the power usage.
For more information, see the "Configuring PoE" chapter in the *Interface and Hardware Component Configuration Guide (Catalyst 3850 Switches)* Interface Configuration Guide (Cisco WLC 5700 Series).

**Related Topics**

*Scenarios to Troubleshoot Power over Ethernet (PoE)*, on page 1429

### Disabled Port Caused by Power Loss

If a powered device (such as a Cisco IP Phone 7910) that is connected to a PoE Switch port and powered by an AC power source loses power from the AC power source, the device might enter an error-disabled state. To recover from an error-disabled state, enter the `shutdown` interface configuration command, and then enter the `no shutdown` interface command. You can also configure automatic recovery on the Switch to recover from the error-disabled state.

On a Switch, the `errdisable recovery cause loopback` and the `errdisable recovery interval seconds` global configuration commands automatically take the interface out of the error-disabled state after the specified period of time.

### Disabled Port Caused by False Link-Up

If a Cisco powered device is connected to a port and you configure the port by using the `power inline never` interface configuration command, a false link-up can occur, placing the port into an error-disabled state. To take the port out of the error-disabled state, enter the `shutdown` and the `no shutdown` interface configuration commands.

You should not connect a Cisco powered device to a port that has been configured with the `power inline never` command.

### Ping

The Switch supports IP ping, which you can use to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply. Ping returns one of these responses:

- **Normal response**—The normal response (*hostname* is alive) occurs in 1 to 10 seconds, depending on network traffic.
- **Destination does not respond**—If the host does not respond, a `no-answer` message is returned.
- **Unknown host**—If the host does not exist, an `unknown host` message is returned.
- **Destination unreachable**—If the default gateway cannot reach the specified network, a `destination-unreachable` message is returned.
- **Network or host unreachable**—If there is no entry in the route table for the host or network, a `network or host unreachable` message is returned.

**Related Topics**

*Executing Ping*, on page 1423

*Example: Pinging an IP Host*, on page 1431
Layer 2 Traceroute

The Layer 2 traceroute feature allows the switch to identify the physical path that a packet takes from a source device to a destination device. Layer 2 traceroute supports only unicast source and destination MAC addresses. Traceroutefinds the path by using the MAC address tables of the Switch in the path. When the Switch detects a device in the path that does not support Layer 2 traceroute, the Switch continues to send Layer 2 trace queries and lets them time out.

The Switch can only identify the path from the source device to the destination device. It cannot identify the path that a packet takes from source host to the source device or from the destination device to the destination host.

Layer 2 Traceroute Guidelines

- Cisco Discovery Protocol (CDP) must be enabled on all the devices in the network. For Layer 2 traceroute to function properly, do not disable CDP.
  If any devices in the physical path are transparent to CDP, the switch cannot identify the path through these devices.

- A Switch is reachable from another Switch when you can test connectivity by using the `ping` privileged EXEC command. All Switch in the physical path must be reachable from each other.

- The maximum number of hops identified in the path is ten.

- You can enter the `traceroute mac` or the `traceroute mac ip` privileged EXEC command on a Switch that is not in the physical path from the source device to the destination device. All Switch in the path must be reachable from this switch.

- The `traceroute mac` command output shows the Layer 2 path only when the specified source and destination MAC addresses belong to the same VLAN. If you specify source and destination MAC addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

- If you specify a multicast source or destination MAC address, the path is not identified, and an error message appears.

- If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

- The `traceroute mac ip` command output shows the Layer 2 path when the specified source and destination IP addresses belong to the same subnet. When you specify the IP addresses, the Switch uses the Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.
  - If an ARP entry exists for the specified IP address, the Switch uses the associated MAC address and identifies the physical path.
  - If an ARP entry does not exist, the Switch sends an ARP query and tries to resolve the IP address. If the IP address is not resolved, the path is not identified, and an error message appears.

- When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute feature is not supported. When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

- This feature is not supported in Token Ring VLANs.
IP Traceroute

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Your Switch can participate as the source or destination of the traceroute privileged EXEC command and might or might not appear as a hop in the traceroute command output. If the Switch is the destination of the traceroute, it is displayed as the final destination in the traceroute output. Intermediate Switch do not show up in the traceroute output if they are only bridging the packet from one port to another within the same VLAN. However, if the intermediate Switch is a multilayer Switch that is routing a particular packet, this Switch shows up as a hop in the traceroute output.

The traceroute privileged EXEC command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute finds the address of the first hop by examining the source address field of the ICMP time-to-live-exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-to-live-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To learn when a datagram reaches its destination, traceroute sets the UDP destination port number in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram destined to itself containing a destination port number that is unused locally, it sends an ICMP port-unreachable error to the source. Because all errors except port-unreachable errors come from intermediate hops, the receipt of a port-unreachable error means that this message was sent by the destination port.

Related Topics

- Executing IP Traceroute, on page 1424
- Example: Performing a Traceroute to an IP Host, on page 1432

Time Domain Reflector Guidelines

You can use the Time Domain Reflector (TDR) feature to diagnose and resolve cabling problems. When running TDR, a local device sends a signal through a cable and compares the reflected signal to the initial signal.

TDR is supported only on 10/100/1000 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports and on SFP module ports.

TDR is supported on 10/100/1000 copper Ethernet ports and on Multigigabit Ethernet (100Mbps/1/2.5/5/10 Gbps) ports. It is not supported on SFP module ports.

TDR can detect these cabling problems:

- Open, broken, or cut twisted-pair wires—The wires are not connected to the wires from the remote device.

- Shorted twisted-pair wires—The wires are touching each other or the wires from the remote device. For example, a shorted twisted pair can occur if one wire of the twisted pair is soldered to the other wire.
If one of the twisted-pair wires is open, TDR can find the length at which the wire is open.

---

**Note**

When using the feature with Multigigabit Ethernet ports, the cable length is displayed only when an open or short condition is detected.

Use TDR to diagnose and resolve cabling problems in these situations:

- Replacing a Switch
- Setting up a wiring closet
- Troubleshooting a connection between two devices when a link cannot be established or when it is not operating properly

When you run TDR, the Switch reports accurate information in these situations:

- The cable for the gigabit link is a solid-core cable.
- The open-ended cable is not terminated.

When you run TDR, the Switch does not report accurate information in these situations:

- The cable for the gigabit link is a twisted-pair cable or is in series with a solid-core cable.
- The link is a 10-megabit or a 100-megabit link.
- The cable is a stranded cable.
- The link partner is a Cisco IP Phone.
- The link partner is not IEEE 802.3 compliant.

---

## Debug Commands

**Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use `debug` commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use `debug` commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased `debug` command processing overhead will affect system use.

All `debug` commands are entered in privileged EXEC mode, and most `debug` commands take no arguments.

**Related Topics**

- Redirecting Debug and Error Message Output, on page 1424
- Example: Enabling All System Diagnostics, on page 1433
Crashinfo Files

The crashinfo files save information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch generates two files at the time of the failure: full core and crashinfo.

The information in the crashinfo file includes the Cisco IOS image name and version that failed, a list of the processor registers, and a stack trace. You can provide this information to the Cisco technical support representative by using the `show tech-support` privileged EXEC command.

The file names have the following format:

```
[fullcore | crashinfo]_[process that crashed]_[date]_[timestamp]-UTC
```

From IOS, you can view the crashinfo files on each switch by using the following command:

```
Switch# dir crashinfo?
```

For example, to access the crashinfo directory for switch 1, enter

```
Switch dir crashinfo-1
```

From the ROMMON prompt, you can view the crashinfo files by using the `dir` command:

```
Switch: dir sda1
```

The following is sample output of a crashinfo file

```
Switch# dir crashinfo:
Directory of crashinfo:/
12  -rwx  2768  Dec 31 1969 16:00:15 -08:00  koops.dat
15  -rwx  0  Jan 12 2000 22:53:40 -08:00  deleted_crash_files
16  -rwx 424676  Jan 12 2000 22:53:40 -08:00  crashinfo_stack-mgr_20000113-065250-UTC
17  -rwx  50  Oct 2 2012 03:18:42 -08:00  last_crashinfo
20  -rwx 4391796  Feb 1 2000 17:50:44 -08:00  crashinfo_stack-mgr_20000202-014954-UTC
21  -rwx 2920325  Feb 1 2000 17:50:45 -08:00  fullcore_stack-mgr_20000202-014954-UTC
34817  -rw- 1050209  Jan 10 2013 20:26:23 -08:00  system-report_1_20130111-042535-UTC.gz
18434  -rw- 1016913  Jan 11 2013 10:35:28 -08:00  system-report_1_20130111-183440-UTC.gz
18435  -rw- 1136167  Jan 22 2013 14:14:11 -08:00  system-report_1_20130122-221322-UTC.gz
34821  -rw- 1094631  Jan 2 2013 17:59:23 -08:00  system-report_1_20130103-015835-UTC.gz
6147  -rw-  967429  Jan 3 2013 10:32:44 -08:00  system-report_1_20130113-183156-UTC.gz
34824  -rw-  50  Jan 22 2013 14:14:14 -08:00  deleted_sysreport_files
6155  -rw-  373  Jan 22 2013 14:14:13 -08:00  last_systemreport_log

145898496 bytes total (18569216 bytes free)
```

The file name of the most recent crashinfo file is stored in `last_crashinfo`.
The file name of the most recent system report is stored in `last_systemreport`.
**System Reports**

When a switch crashes, a system report is automatically generated for each switch in the switch stack. The system report file captures all the trace buffers, and other system-wide logs found on the switch. System reports are located in the crashinfo directory in the following format:

```
system-report_[switch number]_[date]-[timestamp]-UTC.gz
```

After a switch crash, you should check if a system report file was generated. The name of the most recently generated system report file is stored in the last_systemreportfile under the crashinfo directory. The system report and crashinfo files assist TAC when troubleshooting your issue.

**Onboard Failure Logging on the Switch**

You can use the onboard failure logging (OBFL) feature to collect information about the Switch. The information includes uptime, temperature, and voltage information and helps Cisco technical support representatives to troubleshoot Switch problems. We recommend that you keep OBFL enabled and do not erase the data stored in the flash memory.

By default, OBFL is enabled. It collects information about the Switch and small form-factor pluggable (SFP) modules. The Switch stores this information in the flash memory:

- CLI commands—Record of the OBFL CLI commands that are entered on a standalone Switch or a switch stack member.
- Environment data—Unique device identifier (UDI) information for a standalone Switch or a switch stack member and for all the connected FRU devices: the product identification (PID), the version identification (VID), and the serial number.
- Message—Record of the hardware-related system messages generated by a standalone Switch or a switch stack member.
- Power over Ethernet (PoE)—Record of the power consumption of PoE ports on a standalone Switch or a switch stack member.
- Temperature—Temperature of a standalone Switch or a switch stack member.
- Uptime data—Time when a standalone Switch or a switch stack member starts, the reason the Switch restarts, and the length of time the Switch has been running since it last restarted.
- Voltage—System voltages of a standalone Switch or a switch stack member.

You should manually set the system clock or configure it by using Network Time Protocol (NTP).

When the Switch is running, you can retrieve the OBFL data by using the `show logging onboard` privileged EXEC commands. If the Switch fails, contact your Cisco technical support representative to find out how to retrieve the data.

When an OBFL-enabled Switch is restarted, there is a 10-minute delay before logging of new data begins.

**Related Topics**

- Configuring OBFL, on page 1425
Fan Failures

By default, the feature is disabled. When more than one of the fans fails in a field-replaceable unit (FRU) or in a power supply, the Switch does not shut down, and this error message appears:

Multiple fan(FRU/PS) failure detected. System may get overheated. Change fan quickly.

The Switch might overheat and shut down.

To enable the fan failures feature, enter the `system env fan-fail-action shut` privileged EXEC command. If more than one fan in the Switch fails, the Switch automatically shuts down, and this error message appears:

Faulty (FRU/PS) fans detected, shutting down system!

After the first fan shuts down, if the Switch detects a second fan failure, the Switch waits for 20 seconds before it shuts down.

To restart the Switch, it must be power cycled.

Possible Symptoms of High CPU Utilization

Excessive CPU utilization might result in these symptoms, but the symptoms might also result from other causes:

You may see increased system memory usage when Cisco Catalyst 4500E Supervisor Engine 8-E is used in wireless mode.

- Spanning tree topology changes
- EtherChannel links brought down due to loss of communication
- Failure to respond to management requests (ICMP ping, SNMP timeouts, slow Telnet or SSH sessions)
- UDLD flapping
- IP SLAs failures because of SLAs responses beyond an acceptable threshold
- DHCP or IEEE 802.1x failures if the switch does not forward or respond to requests
How to Troubleshoot the Software Configuration

Recovering from a Software Failure

Before you begin

This recovery procedure requires that you have physical access to the switch.
This procedure uses boot loader commands and TFTP to recover from a corrupted or incorrect image file.

Procedure

Step 1 From your PC, download the software image file \(image.bin\) from Cisco.com.

Step 2 Load the software image to your TFTP server.

Step 3 Connect your PC to the switch Ethernet management port.

Step 4 Unplug the switch power cord.

Step 5 Press the Mode button, and at the same time, reconnect the power cord to the switch.

Step 6 From the bootloader (ROMMON) prompt, ensure that you can ping your TFTP server.
   a) Set the IP address \(\text{switch: set IP\_ADDRESS ip\_address subnet\_mask}\)
      
      Example:
      
      switch: set IP\_ADDRESS 192.0.2.123/255.255.255.0

   b) Set the default router IP address \(\text{switch: set DEFAULT\_ROUTER ip\_address}\)
      
      Example:
      
      switch: set DEFAULT\_ROUTER 192.0.2.1

   c) Verify that you can ping the TFTP server \(\text{switch: ping ip\_address\_of\_TFTP\_server}\)
      
      Example:
      
      switch: ping 192.0.2.15
      ping 192.0.2.1 with 32 bytes of data...
      Host 192.0.2.1 is alive.
      switch:

Step 7 Verify that you have a recovery image in your recovery partition (sda9:).

This recovery image is required for recovery using the emergency-install feature.

Example:

switch: dir sda9:
Directory of sda9:/
  2 drwx 1024 .
  2 drwx 1024 ..
11 -rw- 18923068 c3850-recovery.bin
Step 8  From the bootloader (ROMMON) prompt, initiate the emergency-install feature that assists you in recovering the software image on your switch.

**WARNING:** The emergency install command will erase your entire boot flash!

**Example:**

```
Switch# emergency-install
tftp://192.0.2.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
```

The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin)...
Reading full image into memory..................done
Nova Bundle Image
--------------------------------------------------
Kernel Address : 0x6042e5cc
Kernel Size : 0x318261/3244641
Initramfs Address : 0x60746830
Initramfs Size : 0xdb0fb9/14356409
Compression Format: .mzip

Bootable image at @ ram:0x6042e5cc
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000, 0x90000000].
**************************************************************************************************************************
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

Initiating Emergency Installation of bundle
tftp://192.0.2.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin

Downloading bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Validating bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Installing bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Verifying bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Package cat3k_caa-base..pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-infra.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.03.02.00.SE.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.
Booting... (use DDR clock 667 MHz) Initializing and Testing RAM +++@@###...++@++@@++@@++@

switch: emergency-install tftp://172.20.249.254/katana/ct5760.renum.bin

The bootflash will be erased during install operation, continue (y/n)? y
Starting emergency recovery (tftp://172.20.249.254/katana/ct5760.renum.bin)...
Loading "sda9:ct5760-recovery.bin"
Reading full image into memory....................done
Verifying image digital signature.
Nova Bundle Image

-----------------------------
Kernel Address : 0x8b35b598
Kernel Size : 0x367550/3568976
Initramfs Address : 0x8b6c2ae8
Initramfs Size : 0xbfe484/12575876
Compression Format: unknown

File "sda9:ct5760-recovery.bin" uncompressed and installed, entry point: 0x8b35b598
Image validated

Initiating Emergency Installation of bundle tftp://172.20.249.254/katana/ct5760.renum.bin

Downloading bundle tftp://172.20.249.254/katana/ct5760.renum.bin...
Validating bundle tftp://172.20.249.254/katana/ct5760.renum.bin...
Installing bundle tftp://172.20.249.254/katana/ct5760.renum.bin...
Verifying bundle tftp://172.20.249.254/katana/ct5760.renum.bin...
Package ct5760-base.SPA.03.02.00.pkg is Digitally Signed
Package ct5760-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package ct5760-infra.SPA.03.02.00.pkg is Digitally Signed
Package ct5760-ipservicesk9.SPA.150-1.EX.pkg is Digitally Signed
Package ct5760-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package ct5760-wcm.SPA.10.0.10.48.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.
Xmodem file system is available.
Base ethernet MAC Address: 20:37:06:4d:64:00
Verifying bootloader digital signature.

The system is not configured to boot automatically. The following command will finish loading the operating system software:

    boot

Related Topics

Software Failure on a Switch, on page 1406
Recovering from a Lost or Forgotten Password

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.

---

**Note**

On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message shows this during the recovery process.

---

**Procedure**

**Step 1**

Connect a terminal or PC to the switch.

- Connect a terminal or a PC with terminal-emulation software to the switch console port.
- Connect a PC to the Ethernet management port.

**Step 2**

Set the line speed on the emulation software to 9600 baud.

**Step 3**

Power off the standalone switch or the entire switch stack.

**Step 4**

Reconnect the power cord to the or the . Within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until a prompt is seen; then release the **Mode** button.

Switch:
Xmodem file system is available.
Base ethernet MAC Address: 20:37:06:4d:e9:80
Verifying bootloader digital signature.

The system has been interrupted prior to loading the operating system software, console will be reset to 9600 baud rate.

Proceed to the Procedure with Password Recovery Enabled section, and follow the steps.

**Step 5**

After recovering the password, reload the switch or the .

On a switch:

```
Switch> reload
Proceed with reload? [confirm] y
```

**Related Topics**

Lost or Forgotten Password on a Switch, on page 1406
Procedure with Password Recovery Enabled

If the password-recovery operation is enabled, this message appears:

**Procedure**

**Step 1** Initialize the flash file system.

Switch: `flash_init`

**Step 2** Ignore the startup configuration with the following command:

Switch: `SWITCH_IGNORE_STARTUP_CFG=1`

**Step 3** Boot the switch with the `packages.conf` file from flash.

Switch: `boot flash:packages.conf`

**Step 4** Terminate the initial configuration dialog by answering No.

Would you like to enter the initial configuration dialog? [yes/no]: No

**Step 5** At the switch prompt, enter privileged EXEC mode.

Switch>` enable
Switch#

**Step 6** Copy the startup configuration to running configuration.

Switch# `copy startup-config running-config Destination filename [running-config]?

Press Return in response to the confirmation prompts. The configuration file is now reloaded, and you can change the password.

**Step 7** Enter global configuration mode and change the `enable` password.

Switch# `configure terminal
Switch(config)#

**Step 8** Write the running configuration to the startup configuration file.

Switch(config)# `copy running-config startup-config`

**Step 9** Confirm that manual boot mode is enabled.
Switch# show boot

BOOT variable = flash:packages.conf;
Manual Boot = yes
Enable Break = yes

**Step 10**  Reload the switch.

Switch# reload

**Step 11**  Return the Bootloader parameters (previously changed in Steps 2 and 3) to their original values.

switch: SWITCH_IGNORE_STARTUP_CFG=0

**Step 12**  Boot the switch with the *packages.conf* file from flash.

Switch: boot flash:packages.conf

**Step 13**  After the switch boots up, disable manual boot on the switch.

Switch(config)# no boot manual

---

**Procedure with Password Recovery Disabled**

If the password-recovery mechanism is disabled, this message appears:

The password-recovery mechanism has been triggered, but is currently disabled. Access to the boot loader prompt through the password-recovery mechanism is disallowed at this point. However, if you agree to let the system be reset back to the default system configuration, access to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?

---

**Caution**

Returning the Switch to the default configuration results in the loss of all existing configurations. We recommend that you contact your system administrator to verify if there are backup Switch and VLAN configuration files.

- If you enter n (no), the normal boot process continues as if the Mode button had not been pressed; you cannot access the boot loader prompt, and you cannot enter a new password. You see the message:

  Press Enter to continue........
• If you enter y (yes), the configuration file in flash memory and the VLAN database file are deleted. When the default configuration loads, you can reset the password.

Procedure

Step 1 Choose to continue with password recovery and delete the existing configuration:

Would you like to reset the system back to the default configuration (y/n)? Y

Step 2 Display the contents of flash memory:

Switch: dir flash:

The Switch file system appears.

Directory of flash:/
.
.
15494 drwx 4096 Jan 1 2000 00:20:20 +00:00 kirch
15508 -rw- 258065648 Sep 4 2013 14:19:03 +00:00 cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin

Step 3 Boot up the system:

Switch: boot

You are prompted to start the setup program. To continue with password recovery, enter N at the prompt:

Continue with the configuration dialog? [yes/no]: N

Step 4 At the Switch prompt, enter privileged EXEC mode:

Switch> enable

Step 5 Enter global configuration mode:

Switch# configure terminal

Step 6 Change the password:

Switch(config)# enable secret password

The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 7 Return to privileged EXEC mode:
Switch(config)# exit
Switch#

**Note** Before continuing to Step 9, power on any connected stack members and wait until they have completely initialized.

**Step 8** Write the running configuration to the startup configuration file:

Switch# copy running-config startup-config

The new password is now in the startup configuration.

**Step 9** You must now reconfigure the Switch. If the system administrator has the backup Switch and VLAN configuration files available, you should use those.

---

**Preventing Switch Stack Problems**

To prevent switch stack problems, you should do the following:

- Make sure that the Switch that you add to or remove from the switch stack are powered off. For all powering considerations in switch stacks, see the “Switch Installation” chapter in the hardware installation guide.

- Press the Mode button on a stack member until the Stack mode LED is on. The last two port LEDs on the Switch should be green. Depending on the Switch model, the last two ports are either 10/100/1000 ports or small form-factor pluggable (SFP) module. If one or both of the last two port LEDs are not green, the stack is not operating at full bandwidth.

- We recommend using only one CLI session when managing the switch stack. Be careful when using multiple CLI sessions to the . Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible that you might not be able to identify the session from which you entered a command.

- Manually assigning stack member numbers according to the placement of the Switch in the stack can make it easier to remotely troubleshoot the switch stack. However, you need to remember that the Switch have manually assigned numbers if you add, remove, or rearrange Switch later. Use the switch current-stack-member-number renumber new-stack-member-number global configuration command to manually assign a stack member number.

If you replace a stack member with an identical model, the new Switch functions with the exact same configuration as the replaced Switch. This is also assuming the new Switch is using the same member number as the replaced Switch.

Removing powered-on stack members causes the switch stack to divide (partition) into two or more switch stacks, each with the same configuration. If you want the switch stacks to remain separate, change the IP address or addresses of the newly created switch stacks. To recover from a partitioned switch stack, follow these steps:

1. Power off the newly created switch stacks.

2. Reconnect them to the original switch stack through their StackWise Plus ports.

3. Power on the Switch.
For the commands that you can use to monitor the switch stack and its members, see the Displaying Switch Stack Information section.

**Preventing Autonegotiation Mismatches**

The IEEE 802.3ab autonegotiation protocol manages the Switch settings for speed (10 Mb/s, 100 Mb/s, and 1000 Mb/s, excluding SFP module ports) and duplex (half or full). There are situations when this protocol can incorrectly align these settings, reducing performance. A mismatch occurs under these circumstances:

- A manually set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port.
- A port is set to autonegotiate, and the connected port is set to full duplex with no autonegotiation.

To maximize Switch performance and ensure a link, follow one of these guidelines when changing the settings for duplex and speed:

- Let both ports autonegotiate both speed and duplex.
- Manually set the speed and duplex parameters for the ports on both ends of the connection.

Note: If a remote device does not autonegotiate, configure the duplex settings on the two ports to match. The speed parameter can adjust itself even if the connected port does not autonegotiate.

**Troubleshooting SFP Module Security and Identification**

Cisco small form-factor pluggable (SFP) modules have a serial EEPROM that contains the module serial number, the vendor name and ID, a unique security code, and cyclic redundancy check (CRC). When an SFP module is inserted in the Switch, the Switch software reads the EEPROM to verify the serial number, vendor name and vendor ID, and recompute the security code and CRC. If the serial number, the vendor name or vendor ID, the security code, or CRC is invalid, the software generates a security error message and places the interface in an error-disabled state.

Note: The security error message references the GBIC_SECURITY facility. The Switch supports SFP modules and does not support GBIC modules. Although the error message text refers to GBIC interfaces and modules, the security messages actually refer to the SFP modules and module interfaces.

If you are using a non-Cisco SFP module, remove the SFP module from the Switch, and replace it with a Cisco module. After inserting a Cisco SFP module, use the `errdisable recovery cause gbic-invalid` global configuration command to verify the port status, and enter a time interval for recovering from the error-disabled state. After the elapsed interval, the Switch brings the interface out of the error-disabled state and retries the operation. For more information about the `errdisable recovery` command, see the command reference for this release.

If the module is identified as a Cisco SFP module, but the system is unable to read vendor-data information to verify its accuracy, an SFP module error message is generated. In this case, you should remove and reinsert the SFP module. If it continues to fail, the SFP module might be defective.
Monitoring SFP Module Status

You can check the physical or operational status of an SFP module by using the `show interfaces transceiver` privileged EXEC command. This command shows the operational status, such as the temperature and the current for an SFP module on a specific interface and the alarm status. You can also use the command to check the speed and the duplex settings on an SFP module. For more information, see the `show interfaces transceiver` command in the command reference for this release.

Executing Ping

If you attempt to ping a host in a different IP subnetwork, you must define a static route to the network or have IP routing configured to route between those subnets.

IP routing is disabled by default on all Switches.

Note

Though other protocol keywords are available with the `ping` command, they are not supported in this release.

Use this command to ping another device on the network from the Switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ping ip host</td>
<td>address`</td>
</tr>
<tr>
<td>Switch# ping 172.20.52.3</td>
<td>Pings a remote host through IP or by supplying the hostname or network address.</td>
</tr>
</tbody>
</table>

Related Topics

- [Ping](#), on page 1407
- Example: [Pinging an IP Host](#), on page 1431

Monitoring Temperature

The Switch monitors the temperature conditions and uses the temperature information to control the fans.

Use the `show env temperature status` privileged EXEC command to display the temperature value, state, and thresholds. The temperature value is the temperature in the Switch (not the external temperature). You can configure only the yellow threshold level (in Celsius) by using the `system env temperature threshold yellow value` global configuration command to set the difference between the yellow and red thresholds. You cannot configure the green or red thresholds. For more information, see the command reference for this release.

Monitoring the Physical Path

You can monitor the physical path that a packet takes from a source device to a destination device by using one of these privileged EXEC commands:
Table 109: Monitoring the Physical Path

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tracertoute mac [interface interface-id]</code> <code>{source-mac-address} [interface interface-id]</code> <code>{destination-mac-address} [vlan vlan-id] [detail]</code></td>
<td>Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.</td>
</tr>
<tr>
<td><code>tracertoute mac ip</code> `{source-ip-address</td>
<td>source-hostname} `{destination-ip-address</td>
</tr>
</tbody>
</table>

Executing IP Traceroute

Note

Though other protocol keywords are available with the `traceroute` privileged EXEC command, they are not supported in this release.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>traceroute ip host</code> Switch# traceroute ip 192.51.100.1</td>
<td>Traces the path that packets take through the network.</td>
</tr>
</tbody>
</table>

Related Topics

- IP Traceroute, on page 1409
- Example: Performing a Traceroute to an IP Host, on page 1432

Running TDR and Displaying the Results

To run TDR, enter the `test cable-diagnostics tdr interface interface-id` privileged EXEC command.

To display the results, enter the `show cable-diagnostics tdr interface interface-id` privileged EXEC command.

Redirecting Debug and Error Message Output

By default, the network server sends the output from `debug` commands and system error messages to the console. If you use this default, you can use a virtual terminal connection to monitor debug output instead of connecting to the console port or the Ethernet management port.

Possible destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. The syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX and its derivatives.
Be aware that the debugging destination you use affects system overhead. When you log messages to the console, very high overhead occurs. When you log messages to a virtual terminal, less overhead occurs. Logging messages to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method.

For more information about system message logging, see "Configuring System Message Logging".

**Related Topics**
- Debug Commands, on page 1410

## Using the show platform forward Command

The output from the `show platform forward` privileged EXEC command provides some useful information about the forwarding results if a packet entering an interface is sent through the system. Depending upon the parameters entered about the packet, the output provides lookup table results and port maps used to calculate forwarding destinations, bitmaps, and egress information.

Most of the information in the output from the command is useful mainly for technical support personnel, who have access to detailed information about the Switch application-specific integrated circuits (ASICs). However, packet forwarding information can also be helpful in troubleshooting.

## Using the show debug command

The `show debug` command is entered in privileged EXEC mode. This command displays all debug options available on the switch.

To view all conditional debug options run the command `show debug condition`. The commands can be listed by selecting either a condition identifier `<1-1000>` or `all` conditions.

To disable debugging, use the `no debug all` command.

**Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use `debug` commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use `debug` commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased `debug` command processing overhead will affect system use.

For more information, see Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 16.1 (Catalyst 3850 Switches).

## Configuring OBFL

**Caution**

We recommend that you do not disable OBFL and that you do not remove the data stored in the flash memory.
• To enable OBFL, use the `hw-switch switch [switch-number] logging onboard [message level level]` global configuration command. On switches, the range for `switch-number` is from 1 to 9. Use the `message level level` parameter to specify the severity of the hardware-related messages that the switch generates and stores in the flash memory.

• To copy the OBFL data to the local network or a specific file system, use the `copy onboard switch switch-number url url-destination` privileged EXEC command.

• To disable OBFL, use the `no hw-switch switch [switch-number] logging onboard [message level level]` global configuration command.

• To clear all the OBFL data in the flash memory except for the uptime and CLI command information, use the `clear onboard switch switch-number` privileged EXEC command.

• In a switch stack, you can enable OBFL on a standalone switch or on all stack members by using the `hw-switch switch [switch-number] logging onboard [message level level]` global configuration command.

• You can enable or disable OBFL on a member switch from the .

For more information about the commands in this section, see the command reference for this release.

Related Topics

Onboard Failure Logging on the Switch, on page 1412
Displaying OBFL Information, on page 1427

WSMA Configuration for WebUI

WSMA configurations are available by default to access the Web UI. If you explicitly delete the configuration, you have to reconfigure as below:

```
Switch(config)#wsma agent exec
Switch(wsma-exec-agent)# profile httplistener
Switch(wsma-exec-agent)# profile httpslistener
Switch(wsma-exec-agent)#exit
Switch(config)#wsma agent config
Switch(wsma-config-agent)# profile httplistener
Switch(wsma-config-agent)# profile httpslistener
Switch(wsma-config-agent)#exit
Switch(config)#wsma agent filesys
Switch(wsma-filesys-agent)# profile httplistener
Switch(wsma-filesys-agent)# profile httpslistener
Switch(wsma-filesys-agent)#exit
Switch(config)#wsma agent notify
```
Verifying Troubleshooting of the Software Configuration

Displaying OBFL Information

Table 110: Commands for Displaying OBFL Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show onboard switch switch-number clilog</code></td>
<td>Displays the OBFL CLI commands that were entered on a standalone switch or the specified stack members.</td>
</tr>
<tr>
<td>Switch# show onboard switch 1 clilog</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number environment</code></td>
<td>Displays the UDI information for a standalone switch or the specified stack members and for all the connected FRU devices: the PID, the VID, and the serial number.</td>
</tr>
<tr>
<td>Switch# show onboard switch 1 environment</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number message</code></td>
<td>Displays the hardware-related messages generated by a standalone switch or the specified stack members.</td>
</tr>
<tr>
<td>Switch# show onboard switch 1 message</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number counter</code></td>
<td>Displays the counter information on a standalone switch or the specified stack members.</td>
</tr>
<tr>
<td>Switch# show onboard switch 1 counter</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number temperature</code></td>
<td>Displays the temperature of a standalone switch or the specified switch stack members.</td>
</tr>
<tr>
<td>Switch# show onboard switch 1 temperature</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number uptime</code></td>
<td>Displays the time when a standalone switch or the specified stack members start, the reason the standalone switch or specified stack members restart, and the length of time that the standalone switch or specified stack members have been running since they last restarted.</td>
</tr>
<tr>
<td>Switch# show onboard switch 1 uptime</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number voltage</code></td>
<td>Displays the system voltages of a standalone switch or the specified stack members.</td>
</tr>
<tr>
<td>Switch# show onboard switch 1 voltage</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number status</code></td>
<td>Displays the status of a standalone switch or the specified stack members.</td>
</tr>
<tr>
<td>Switch# show onboard switch 1 status</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Onboard Failure Logging on the Switch, on page 1412
- Configuring OBFL, on page 1425
Example: Verifying the Problem and Cause for High CPU Utilization

To determine if high CPU utilization is a problem, enter the `show processes cpu sorted` privileged EXEC command. Note the underlined information in the first line of the output example.

```
Switch# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

This example shows normal CPU utilization. The output shows that utilization for the last 5 seconds is 8%/0%, which has this meaning:

- The total CPU utilization is 8 percent, including both time running Cisco IOS processes and time spent handling interrupts.
- The time spent handling interrupts is zero percent.

**Table 111: Troubleshooting CPU Utilization Problems**

<table>
<thead>
<tr>
<th>Type of Problem</th>
<th>Cause</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interrupt percentage value is almost as high as total CPU utilization value.</td>
<td>The CPU is receiving too many packets from the network.</td>
<td>Determine the source of the network packet. Stop the flow, or change the switch configuration. See the section on “Analyzing Network Traffic.”</td>
</tr>
<tr>
<td>Total CPU utilization is greater than 50% with minimal time spent on interrupts.</td>
<td>One or more Cisco IOS process is consuming too much CPU time. This is usually triggered by an event that activated the process.</td>
<td>Identify the unusual event, and troubleshoot the root cause. See the section on “Debugging Active Processes.”</td>
</tr>
</tbody>
</table>
## Scenarios for Troubleshooting the Software Configuration

### Scenarios to Troubleshoot Power over Ethernet (PoE)

#### Table 112: Power over Ethernet Troubleshooting Scenarios

<table>
<thead>
<tr>
<th>Symptom or Problem</th>
<th>Possible Cause and Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only one port does not have PoE. Trouble is on only one switch port. PoE and non-PoE devices do not work on this port, but do on other ports.</td>
<td>Verify that the powered device works on another PoE port. Use the <code>show run</code>, or <code>show interface status</code> user EXEC commands to verify that the port is not shut down or error-disabled. <strong>Note</strong> Most switches turn off port power when the port is shut down, even though the IEEE specifications make this optional. Verify that <code>power inline never</code> is not configured on that interface or port. Verify that the Ethernet cable from the powered device to the switch port is good: Connect a known good non-PoE Ethernet device to the Ethernet cable, and make sure that the powered device establishes a link and exchanges traffic with another host. <strong>Note</strong> Cisco powered device works only with straight cable and not with crossover one. Verify that the total cable length from the switch front panel to the powered device is not more than 100 meters. Disconnect the Ethernet cable from the switch port. Use a short Ethernet cable to connect a known good Ethernet device directly to this port on the switch front panel (not on a patch panel). Verify that it can establish an Ethernet link and exchange traffic with another host, or ping the port VLAN SVI. Next, connect a powered device to this port, and verify that it powers on. If a powered device does not power on when connected with a patch cord to the switch port, compare the total number of connected powered devices to the switch power budget (available PoE). Use the <code>show inline power</code> command to verify the amount of available power.</td>
</tr>
</tbody>
</table>
### Symptom or Problem
No PoE on all ports or a group of ports.

Trouble is on all switch ports. Nonpowered Ethernet devices cannot establish an Ethernet link on any port, and PoE devices do not power on.

### Possible Cause and Solution
If there is a continuous, intermittent, or reoccurring alarm related to power, replace the power supply if possible it is a field-replaceable unit. Otherwise, replace the switch.

If the problem is on a consecutive group of ports but not all ports, the power supply is probably not defective, and the problem could be related to PoE regulators in the switch.

Use the `show log` privileged EXEC command to review alarms or system messages that previously reported PoE conditions or status changes.

If there are no alarms, use the `show interface status` command to verify that the ports are not shut down or error-disabled. If ports are error-disabled, use the `shut` and `no shut` interface configuration commands to reenable the ports.

Use the `show env power` and `show power inline` privileged EXEC commands to review the PoE status and power budget (available PoE).

Review the running configuration to verify that `power inline never` is not configured on the ports.

Connect a nonpowered Ethernet device directly to a switch port. Use only a short patch cord. Do not use the existing distribution cables. Enter the `shut` and `no shut` interface configuration commands, and verify that an Ethernet link is established. If this connection is good, use a short patch cord to connect a powered device to this port and verify that it powers on. If the device powers on, verify that all intermediate patch panels are correctly connected.

Disconnect all but one of the Ethernet cables from switch ports. Using a short patch cord, connect a powered device to only one PoE port. Verify the powered device does not require more power than can be delivered by the switch port.

Use the `show power inline` privileged EXEC command to verify that the powered device can receive power when the port is not shut down. Alternatively, watch the powered device to verify that it powers on.

If a powered device can power on when only one powered device is connected to the switch, enter the `shut` and `no shut` interface configuration commands on the remaining ports, and then reconnect the Ethernet cables one at a time to the switch PoE ports. Use the `show interface status` and `show power inline` privileged EXEC commands to monitor inline power statistics and port status.

If there is still no PoE at any port, a fuse might be open in the PoE section of the power supply. This normally produces an alarm. Check the log again for alarms reported earlier by system messages.
<table>
<thead>
<tr>
<th>Symptom or Problem</th>
<th>Possible Cause and Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco pre-standard powered device disconnects or resets. After working normally, a Cisco phone intermittently reloads or disconnects from PoE.</td>
<td>Verify all electrical connections from the switch to the powered device. Any unreliable connection results in power interruptions and irregular powered device functioning such as erratic powered device disconnects and reloads. Verify that the cable length is not more than 100 meters from the switch port to the powered device. Notice what changes in the electrical environment at the switch location or what happens at the powered device when the disconnect occurs. Notice whether any error messages appear at the same time a disconnect occurs. Use the <code>show log</code> privileged EXEC command to review error messages. Verify that an IP phone is not losing access to the Call Manager immediately before the reload occurs. (It might be a network problem and not a PoE problem.) Replace the powered device with a non-PoE device, and verify that the device works correctly. If a non-PoE device has link problems or a high error rate, the problem might be an unreliable cable connection between the switch port and the powered device.</td>
</tr>
<tr>
<td>IEEE 802.3af-compliant or IEEE 802.3at-compliant powered devices do not work on Cisco PoE switch. A non-Cisco powered device is connected to a Cisco PoE switch, but never powers on or powers on and then quickly powers off. Non-PoE devices work normally.</td>
<td>Use the <code>show power inline</code> command to verify that the switch power budget (available PoE) is not depleted before or after the powered device is connected. Verify that sufficient power is available for the powered device type before you connect it. Use the <code>show interface status</code> command to verify that the switch detects the connected powered device. Use the <code>show log</code> command to review system messages that reported an overcurrent condition on the port. Identify the symptom precisely: Does the powered device initially power on, but then disconnect? If so, the problem might be an initial surge-in (or inrush) current that exceeds a current-limit threshold for the port.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Power over Ethernet Ports, on page 1406

**Configuration Examples for Troubleshooting Software**

**Example: Pinging an IP Host**

This example shows how to ping an IP host:

```
Switch# ping 172.20.52.3
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch#

Table 113: Ping Output Display Characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Each exclamation point means receipt of a reply.</td>
</tr>
<tr>
<td>.</td>
<td>Each period means the network server timed out while waiting for a reply.</td>
</tr>
<tr>
<td>U</td>
<td>A destination unreachable error PDU was received.</td>
</tr>
<tr>
<td>C</td>
<td>A congestion experienced packet was received.</td>
</tr>
<tr>
<td>I</td>
<td>User interrupted test.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>&amp;</td>
<td>Packet lifetime exceeded.</td>
</tr>
</tbody>
</table>

To end a ping session, enter the escape sequence (Ctrl-^X by default). Simultaneously press and release the Ctrl, Shift, and 6 keys and then press the X key.

Related Topics
- Ping, on page 1407
- Executing Ping, on page 1423

Example: Performing a Traceroute to an IP Host

This example shows how to perform a traceroute to an IP host:

Switch# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10

1 192.0.2.1 0 msec 0 msec 4 msec
2 192.0.2.203 12 msec 8 msec 0 msec
3 192.0.2.100 4 msec 0 msec 0 msec
4 192.0.2.10 0 msec 4 msec 0 msec

The display shows the hop count, the IP address of the router, and the round-trip time in milliseconds for each of the three probes that are sent.

Table 114: Traceroute Output Display Characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>The probe timed out.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>Character</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>A</td>
<td>Administratively unreachable. Usually, this output means that an access list is blocking traffic.</td>
</tr>
<tr>
<td>H</td>
<td>Host unreachable.</td>
</tr>
<tr>
<td>N</td>
<td>Network unreachable.</td>
</tr>
<tr>
<td>P</td>
<td>Protocol unreachable.</td>
</tr>
<tr>
<td>Q</td>
<td>Source quench.</td>
</tr>
<tr>
<td>U</td>
<td>Port unreachable.</td>
</tr>
</tbody>
</table>

To end a trace in progress, enter the escape sequence (Ctrl-^ X by default). Simultaneously press and release the Ctrl, Shift, and 6 keys and then press the X key.

**Related Topics**
- IP Traceroute, on page 1409
- Executing IP Traceroute, on page 1424

**Example: Enabling All System Diagnostics**

⚠️ **Caution**

Because debugging output takes priority over other network traffic, and because the `debug all` privileged EXEC command generates more output than any other `debug` command, it can severely diminish switch performance or even render it unusable. In virtually all cases, it is best to use more specific `debug` commands.

This command disables all-system diagnostics:

```
Switch# debug all
```

The `no debug all` privileged EXEC command disables all diagnostic output. Using the `no debug all` command is a convenient way to ensure that you have not accidentally left any `debug` commands enabled.

**Related Topics**
- Debug Commands, on page 1410
Additional References for Troubleshooting Software Configuration

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td>System Management Command Reference (Catalyst 3850Switches) System Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Platform-independent command reference</td>
<td>Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Platform_independent configuration information</td>
<td>Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information for Troubleshooting Software Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

Related Topics

Finding Feature Information, on page 133
PART XIII

VideoStream

- VideoStream, on page 1439
- Configuring VideoStream GUI, on page 1445
CHAPTER 78

VideoStream

- Finding Feature Information, on page 1439
- Prerequisites for VideoStream, on page 1439
- Restrictions for Configuring VideoStream, on page 1439
- Information about VideoStream, on page 1440
- How to Configure VideoStream, on page 1440
- Monitoring Media Streams, on page 1444

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VideoStream

- Make sure that the multicast feature is enabled. We recommend that you configure IP multicast on the controller with multicast-multicast mode.

- Check for the IP address on the client machine. The machine should have an IP address from the respective VLAN.

- Verify that the access points have joined the controllers.

Restrictions for Configuring VideoStream

IGMP snooping is required to switch ON for this MC2UC feature to be functional.

Cisco 5700 Series WLC is not supported in centralized cmm mode.
Information about VideoStream

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. The multicast frame packets are sent at a predetermined rate irrespective of the wireless client optimal data rate. As a result, if any multicast packet is lost in the air, it is not sent again which may cause an IP multicast stream unviewable. Also if the packets are delivered faster, the packets get congested.

The VideoStream feature makes the IP multicast stream delivery reliable over the air, by converting the multicast frame to a unicast frame over the air. Each VideoStream client acknowledges receiving a video IP multicast stream.

How to Configure VideoStream

Configuring Multicast-Direct Globally for Media-Stream

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless multicast</td>
<td>Enables multicast for wireless forwarding.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>IP igmp snooping</td>
<td>Enables IGMP snooping on a per-VLAN basis. If the global setting is disabled, then all VLANs are treated as disabled, whether they are enabled or not.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>IP igmp snooping querier</td>
<td>Configures a snooping querier on an interface when there is no multicast router in the VLAN to generate queries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>wireless media-stream multicast-direct</td>
<td>Configures the global multicast-direct feature for the controller.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)#wireless media-stream multicast-direct</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>wireless media-stream message</td>
<td>Configures various message configuration parameters like phone, URL, email and notes. That is, when a media stream is refused (due to bandwidth constraints), a message can be sent to the user. These parameters configure the messages to send IT support email address, notes (message to display explaining why the</td>
</tr>
</tbody>
</table>
Configure each media stream and its parameters like expected multicast destination addresses, stream bandwidth consumption and stream priority parameters.

**Example:**
```
Switch(config)#wireless media-stream group grp1 231.1.1.1 239.1.1.3
```

Supported Commands:
- avg-packet-size: Configures average packet size
- default: Set a command to its defaults
- exit: Exit sub-mode
- max-bandwidth: Configures maximum bandwidth
- expected-stream-bandwidth: Configures maximum expected stream bandwidth in Kbps
- no: Negate a command or set its defaults
- policy: Configure media stream admission policy
- qos: Configure Over the AIR QoS class, '<video>' ONLY
- <cr>:

**Step 8**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>`ap dot11 24ghz</td>
<td>5ghz media-stream multicast-direct`</td>
</tr>
<tr>
<td>`ap dot11 24ghz</td>
<td>5ghz media-stream video-redirect`</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

**Example:**

```
Switch(config)# ap dot11 24ghz
media-stream video-redirect
```

**Step 4**

```
ap dot11 24ghz | 5ghz media-stream multicast-direct admission-besteffort
```

**Example:**

```
Switch(config)# ap dot11 24ghz
media-stream multicast-direct admission-besteffort
```

Configures the media stream to still be sent through the best effort queue if a media stream cannot be prioritized due to bandwidth availability limitations. Add no in the command to drop the stream if the media stream cannot be prioritized due to bandwidth availability limitations.

**Step 5**

```
ap dot11 24ghz | 5ghz media-stream multicast-direct client-maximum [<value>]
```

**Example:**

```
Switch(config)# ap dot11 24ghz
media-stream multicast-direct client-max 15
```

Configures maximum number of allowed media streams per individual client. The maximum is 15 and the default is 0. Value 0 denotes unlimited streams.

**Step 6**

```
ap dot11 24ghz | 5ghz media-stream multicast-direct radio-maximum 20
```

**Example:**

```
Switch(config)# ap dot11 24ghz
media-stream multicast-direct radio-max 20
```

Configures maximum number of radio streams. The range is from 1 to 20. Default is 0. Value 0 denotes unlimited streams.

**Step 7**

```
ap dot11 24ghz | 5ghz cac multimedia max-bandwidth [<bandwidth>]
```

**Example:**

```
Switch(config)# ap dot11 24ghz cac
media-stream multicast-direct max-bandwidth 60
```

Configure maximum media (voice + video) bandwidth in %. The range is between 5% and 85%.

**Step 8**

```
ap dot11 24ghz | 5ghz cac media-stream multicast-direct min_client_rate [<dot11_rate>]
```

**Example:**

```
Switch(config)# ap dot11 24ghz cac
media-stream multicast-direct min_client_rate
```

Configures the minimum PHY rate needed for a client to send media-stream as unicast. Clients communicating below this rate will not receive the media stream as a unicast flow. Typically, this PHY rate is equal to or higher than the rate at which multicast frames are sent.

**Step 9**

```
ap dot11 5ghz cac media-stream
```

**Step 10**

```
ap dot11 5ghz cac multimedia
```

Configures CAC parameters for media access category, used for voice and video.

**Step 11**

```
ap dot11 5ghz cac video
```

Configures CAC parameters for video access category, used for voice signaling.

**Step 12**

```
ap dot11 5ghz cac voice
```

Configures CAC parameters for voice access category.
### Configuring WLAN to Stream Video

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal &lt;br&gt;Example: Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wlan wlan_name &lt;br&gt;Example: Switch(config)# wlan wlan50</td>
</tr>
<tr>
<td></td>
<td>Enters the WLAN configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>shutdown &lt;br&gt;Example: Switch(config-wlan)# shutdown</td>
</tr>
<tr>
<td></td>
<td>Disables the WLAN for configuring it parameters.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>media-stream multicast-direct &lt;br&gt;Example: Switch(config)#media-stream multicast-direct</td>
</tr>
<tr>
<td></td>
<td>Configures the multicast-direct feature on media-stream for the WLAN.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>no shutdown &lt;br&gt;Example: Switch(config-wlan)# no shutdown</td>
</tr>
<tr>
<td></td>
<td>Enables the WLAN.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end &lt;br&gt;Example: Switch(config)# end</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

### Deleting a Media-Stream

**Before you begin**

The media-stream should be enabled and configured for it to be deleted.
Monitoring Media Streams

Table 115: Commands for monitoring media streams

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless media-stream client detail group name</td>
<td>Displays media stream client details of the particular group.</td>
</tr>
<tr>
<td>show wireless media-stream client summary</td>
<td>Displays the media stream information of all the clients.</td>
</tr>
<tr>
<td>show wireless media-stream group detail group name</td>
<td>Displays the media stream configuration details of the particular group.</td>
</tr>
<tr>
<td>show wireless media-stream group summary</td>
<td>Displays the media stream configuration details of all the groups.</td>
</tr>
<tr>
<td>show wireless media-stream message details</td>
<td>Displays the session announcement message details.</td>
</tr>
<tr>
<td>show wireless multicast</td>
<td>Displays the multicast-direct configuration state.</td>
</tr>
<tr>
<td>show ap dot11 24ghz</td>
<td>5ghz media-stream rrc</td>
</tr>
</tbody>
</table>
CHAPTER 79

Configuring VideoStream GUI

- Configuring VideoStream (GUI), on page 1445

Configuring VideoStream (GUI)

Complete the following steps to configure VideoStream using GUI.

Procedure

Step 1
Configure the multicast feature by following these steps:

a) Choose Wireless > MediaStream > General.

b) Select or unselect the Multicast Direct feature check box. The default value is disabled.

Note: Enabling the multicast direct feature does not automatically reset the existing client state. The wireless clients must rejoin the multicast stream after enabling the multicast direct feature on the controller.

c) In the Session Message Config area, select Session announcement State check box to enable the session announcement mechanism. If the session announcement state is enabled, clients are informed each time a controller is not able to serve the multicast direct data to the client.

d) In the Session announcement URL text box, enter the URL where the client can find more information when an error occurs during the multicast media stream transmission.

e) In the Session announcement e-mail text box, enter the e-mail address of the person who can be contacted.

f) In the Session announcement Phone text box, enter the phone number of the person who can be contacted.

g) In the Session announcement Note text box, enter a reason as to why a particular client cannot be served with a multicast media.

h) Click Apply.

Step 2
Add a media stream by following these steps:

a) Choose Wireless > Media Stream > Streams to open the Media Stream page.

b) Click Add New to configure a new media stream. The Media Stream > New page appears.

Note: The Stream Name, Multicast Destination Start IP Address (IPv4 or IPv6), and Multicast Destination End IP Address (IPv4 or IPv6) text boxes are mandatory. You must enter information in these text boxes.

c) In the Stream Name text box, enter the media stream name. The stream name can be up to 64 characters.
d) In the **Multicast Destination Start IP Address (IPv4 or IPv6)** text box, enter the start (IPv4 or IPv6) address of the multicast media stream.

e) In the **Multicast Destination End IP Address (IPv4 or IPv6)** text box, enter the end (IPv4 or IPv6) address of the multicast media stream.

**Example:**

**Note** Ensure that the Multicast Destination Start and End IP addresses are of the same type, that is both addresses should be of either IPv4 or IPv6 type.

f) In the **Maximum Expected Bandwidth** text box, enter the maximum expected bandwidth that you want to assign to the media stream. The values can range between 1 to 35000 kbps.

**Example:**

**Note** We recommend that you use a template to add a media stream to the controller.

g) From the **Select from Predefined Templates** drop-down list under **Resource Reservation Control (RRC) Parameters**, choose one of the following options to specify the details about the resource reservation control:

- Very Coarse (below 300 kbps)
- Coarse (below 500 kbps)
- Ordinary (below 750 kbps)
- Medium (below 3 Mbps)
- High (below 5 Mbps)

**Note** When you select a predefined template from the drop-down list, the following text boxes under the **Resource Reservation Control (RRC) Parameters** list their default values that are assigned with the template.

- Low (below 1 Mbps)
- Average Packet Size (100-1500 bytes)—Specifies the average packet size. The value can be in the range of 100 to 1500 bytes. The default value is 1200.
- RRC Periodic update—Enables the RRC (Resource Reservation Control Check) Periodic update. By default, this option is enabled. RRC periodically updates the admission decision on the admitted stream according to the correct channel load. As a result, it may deny certain low priority admitted stream requests.
- RRC Priority (1-8)—Specifies the priority bit set in the media stream. The priority can be any number between 1 and 8. The larger the value means the higher the priority is. For example, a priority of 1 is the lowest value and a value of 8 is the highest value. The default priority is 4. The low priority stream may be denied in the RRC periodic update.
- Traffic Profile Violation—Specifies the action to perform in case of a violation after a re-RRC. Choose an action from the drop-down list. The possible values are as follows:
  - Drop—Specifies that a stream is dropped on periodic reevaluation.
  - Fallback—Specifies that a stream is demoted to Best Effort class on periodic reevaluation.

The default value is **drop**.
h) Click **Apply**.

**Step 3**

Enable the media stream for multicast-direct by following these steps:

a) Choose **WLANs** > **WLAN ID** to open the **WLANs** > **Edit** page.

b) Click the **QoS** tab and select **Gold (Video)** from the Quality of Service (QoS) drop-down list.

c) Click **Apply**.

**Step 4**

Set the EDCA parameters to voice and video optimized (optional) by following these steps:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **EDCA** Parameters.

b) From the **EDCA Profile** drop-down list, choose the **Voice and Video Optimized** option.

c) Click **Apply**.

**Step 5**

Enable the admission control on a band for video (optional) by following these steps:

**Note** Keep the voice bandwidth allocation to a minimum for better performance.

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media** to open the 802.11a/n (5 GHZ) or 802.11b/g/n > **Media** page.

b) Click the **Video** tab.

c) Select the **Admission Control (ACM)** check box to enable bandwidth-based CAC for this radio band. The default value is disabled.

d) Click **Apply**.

**Step 6**

Configure the video bandwidth by following these steps:

**Note** The template bandwidth that is configured for a media stream should be more than the bandwidth for the source media stream. The voice configuration is optional. Keep the voice bandwidth allocation to a minimum for better performance.

a) Disable all WMM WLANs.

b) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media** to open the 802.11a/n/ac (5 GHZ) or 802.11b/g/n > **Media** page.

c) Click the **Video** tab.

d) Select the **Admission Control (ACM)** check box to enable the video CAC for this radio band. The default value is disabled.

e) In the Max RF Bandwidth field, enter the percentage of the maximum bandwidth allocated to clients for video applications on this radio band. Once the client reaches the value specified, the access point rejects new requests on this radio band. The range is 5 to 85%. The default value is 9%.

f) Click **Apply**.

g) Reenable all WMM WLANs and click **Apply**.

**Step 7**

Configure the media bandwidth by following these steps:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media** to open the 802.11a (or 802.11b) > **Media** > **Parameters** page.

b) Click the **Media** tab to open the Media page.

c) Select the **Unicast Video Redirect** check box to enable Unicast Video Redirect. The default value is disabled.

d) In the **Maximum Media Bandwidth (0-85%)** text box, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches a specified value, the access point rejects new calls on this radio band.
The default value is 85%; valid values are from 0% to 85%.

e) In the **Client Minimum Phyg Rate** text box, enter the minimum transmission data rate to the client. If the transmission data rate is below the phy rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

f) In the **Maximum Retry Percent (0-100%)** text box, enter the percentage of maximum retries that are allowed. The default value is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

g) Select the **Multicast Direct Enable** check box to enable the Multicast Direct Enable field. The default value is enabled.

h) From the **Max Streams per Radio** drop-down list, choose the maximum number of streams allowed per radio from the range 0 to 20. The default value is set to No-limit. If you choose No-limit, there is no limit set for the number of client subscriptions.

i) From the **Max Streams per Client** drop-down list, choose the maximum number of streams allowed per client from the range 0 to 20. The default value is set to No-limit. If you choose No-limit, there is no limit set for the number of client subscriptions.

j) Select the **Best Effort QoS Admission** check box to enable best-effort QoS admission.

k) Click **Apply**.

**Step 8**
Enable a WLAN by following these steps:

a) Choose **WLANS > WLAN ID**. The WLANs > Edit page appears.

b) Select the **Status** check box.

c) Click **Apply**.

**Step 9**
Enable the 802.11 a/n/ac or 802.11 b/g/n network by following these steps:

a) Choose **Wireless > 802.11a/n/ac or 802.11b/g/n > Network**.

b) Select the **802.11a or 802.11b/g Network Status** check box to enable the network status.

c) Click **Apply**.

**Step 10**
Verify that the clients are associated with the multicast groups and group IDs by following these steps:

a) Choose **Monitor > Clients**. The Clients page appears.

b) Check if the 802.11a/n/ac or 802.11b/g/n network clients have the associated access points.

c) Choose **Monitor > Multicast**. The Multicast Groups page appears.

d) Select the **MGID** check box for the VideoStream to the clients.

e) Click **MGID**. The Multicast Group Detail page appears. Check the Multicast Status details.
PART XIV

VLAN

• Configuring VTP, on page 1451
• VLANs, on page 1475
• VLAN Groups, on page 1495
• Configuring VLAN Trunks, on page 1503
CHAPTER 80

Configuring VTP

• Finding Feature Information, on page 1451
• Prerequisites for VTP, on page 1451
• Restrictions for VTP, on page 1452
• Information About VTP, on page 1452
• How to Configure VTP, on page 1460
• Monitoring VTP, on page 1470
• Configuration Examples for VTP, on page 1471
• Where to Go Next, on page 1471
• Additional References, on page 1471
• Feature History and Information for VTP, on page 1473

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VTP

Before you create VLANs, you must decide whether to use the VLAN Trunking Protocol (VTP) in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches.

VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.
The switch supports a total of 4094 VLANs. However, the number of configured features affects the usage of the switch hardware. If the switch is notified by VTP of a new VLAN and the switch is already using the maximum available hardware resources, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the `show vlan` user EXEC command shows the VLAN in a suspended state.

You can enable or disable VTP per port by entering the `[no] vtp` interface configuration command. When you disable VTP on trunking ports, all VTP instances for that port are disabled. You cannot set VTP to `off` for the MST database and `on` for the VLAN database on the same port.

When you globally set VTP mode to off, it applies to all the trunking ports in the system. However, you can specify on or off on a per-VTP instance basis. For example, you can configure the switch as a VTP server for the VLAN database but with VTP `off` for the MST database.

Because trunk ports send and receive VTP advertisements, you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of another switch. Otherwise, the switch cannot receive any VTP advertisements.

**Related Topics**
- VTP Advertisements, on page 1454
- Adding a VTP Client Switch to a VTP Domain (CLI), on page 1468
- VTP Domain, on page 1453
- VTP Modes, on page 1453

**Restrictions for VTP**

The following are restrictions for a VTP:

- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

**Caution**

Before adding a VTP client switch to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. If you add a switch that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain.

**Information About VTP**

**VTP**

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.
VTP Domain

A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches or switch stacks under the same administrative responsibility sharing the same VTP domain name. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain.

By default, the switch is in the VTP no-management-domain state until it receives an advertisement for a domain over a trunk link (a link that carries the traffic of multiple VLANs) or until you configure a domain name. Until the management domain name is specified or learned, you cannot create or modify VLANs on a VTP server, and VLAN information is not propagated over the network.

If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch then ignores advertisements with a different domain name or an earlier configuration revision number.

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP advertisements are sent over all IEEE trunk connections, including IEEE 802.1Q. VTP dynamically maps VLANs with unique names and internal index associates across multiple LAN types. Mapping eliminates excessive device administration required from network administrators.

If you configure a switch for VTP transparent mode, you can create and modify VLANs, but the changes are not sent to other switches in the domain, and they affect only the individual switch. However, configuration changes made when the switch is in this mode are saved in the switch running configuration and can be saved to the switch startup configuration file.

Related Topics
- Adding a VTP Client Switch to a VTP Domain (CLI), on page 1468
- Prerequisites for VTP, on page 1451

VTP Modes

Table 116: VTP Modes

<table>
<thead>
<tr>
<th>VTP Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP server</td>
<td>In VTP server mode, you can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links. VTP server is the default mode. In VTP server mode, VLAN configurations are saved in NVRAM. If the switch detects a failure while writing a configuration to NVRAM, VTP mode automatically changes from server mode to client mode. If this happens, the switch cannot be returned to VTP server mode until the NVRAM is functioning.</td>
</tr>
<tr>
<td>VTP Mode</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VTP client</td>
<td>A VTP client functions like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode. In VTP versions 1 and 2 in VTP client mode, VLAN configurations are not saved in NVRAM. In VTP version 3, VLAN configurations are saved in NVRAM in client mode.</td>
</tr>
<tr>
<td>VTP transparent</td>
<td>VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode. When the switch is in VTP transparent mode, the VTP and VLAN configurations are saved in NVRAM, but they are not advertised to other switches. In this mode, VTP mode and domain name are saved in the switch running configuration, and you can save this information in the switch startup configuration file by using the <code>copy running-config startup-config</code> privileged EXEC command.</td>
</tr>
<tr>
<td>VTP off</td>
<td>A switch in VTP off mode functions in the same manner as a VTP transparent switch, except that it does not forward VTP advertisements on trunks.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Prerequisites for VTP, on page 1451
- Configuring VTP Mode (CLI), on page 1460

**VTP Advertisements**

Each switch in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. Neighboring switches receive these advertisements and update their VTP and VLAN configurations as necessary.

VTP advertisements distribute this global domain information:

- VTP domain name
- VTP configuration revision number
• Update identity and update timestamp
• MD5 digest VLAN configuration, including maximum transmission unit (MTU) size for each VLAN
• Frame format

VTP advertisements distribute this VLAN information for each configured VLAN:
• VLAN IDs (including IEEE 802.1Q)
• VLAN name
• VLAN type
• VLAN state
• Additional VLAN configuration information specific to the VLAN type

In VTP version 3, VTP advertisements also include the primary server ID, an instance number, and a start index.

Related Topics
Prerequisites for VTP, on page 1451

VTP Version 2

If you use VTP in your network, you must decide which version of VTP to use. By default, VTP operates in version 1.

VTP version 2 supports these features that are not supported in version 1:
• Token Ring support—VTP version 2 supports Token Ring Bridge Relay Function (TrBRF) and Token Ring Concentrator Relay Function (TrCRF) VLANs.
• Unrecognized Type-Length-Value (TLV) support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM when the switch is operating in VTP server mode.
• Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent switch inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Although VTP version 2 supports only one domain, a VTP version 2 transparent switch forwards a message only when the domain name matches.
• Consistency Checks—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from NVRAM. If the MD5 digest on a received VTP message is correct, its information is accepted.

Related Topics
Enabling the VTP Version (CLI), on page 1464

VTP Version 3

VTP version 3 supports these features that are not supported in version 1 or version 2:
• Enhanced authentication—You can configure the authentication as hidden or secret. When hidden, the secret key from the password string is saved in the VLAN database file, but it does not appear in plain text in the configuration. Instead, the key associated with the password is saved in hexadecimal format in the running configuration. You must reenter the password if you enter a takeover command in the domain. When you enter the secret keyword, you can directly configure the password secret key.

• Support for extended range VLAN (VLANs 1006 to 4094) database propagation—VTP versions 1 and 2 propagate only VLANs 1 to 1005.

Note VTP pruning still applies only to VLANs 1 to 1005, and VLANs 1002 to 1005 are still reserved and cannot be modified.

• Support for any database in a domain—In addition to propagating VTP information, version 3 can propagate Multiple Spanning Tree (MST) protocol database information. A separate instance of the VTP protocol runs for each application that uses VTP.

• VTP primary server and VTP secondary servers—A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to its NVRAM.

By default, all devices come up as secondary servers. You can enter the vtp primary privileged EXEC command to specify a primary server. Primary server status is only needed for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers. Primary server status is lost if the device reloads or domain parameters change, even when a password is configured on the switch.

Related Topics
Enabling the VTP Version (CLI), on page 1464

VTP Pruning

VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices. Without VTP pruning, a switch floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even though receiving switches might discard them. VTP pruning is disabled by default.

VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in the pruning-eligible list. Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning eligible switch trunk ports. If the VLANs are configured as pruning-ineligible, the flooding continues. VTP pruning is supported in all VTP versions.

Figure 73: Flooding Traffic without VTP Pruning

VTP pruning is disabled in the switched network. Port 1 on Switch A and Port 2 on Switch D are assigned to the Red VLAN. If a broadcast is sent from the host connected to Switch A, Switch A floods the broadcast and every switch in the network receives it, even though Switches C, E, and F have no ports in the Red VLAN.
VTP pruning is disabled in the switched network. Port 1 on Switch A and Port 2 on Switch D are assigned to the Red VLAN. If a broadcast is sent from the host connected to Switch A, Switch A floods the broadcast and every switch in the network receives it, even though Switches C, E, and F have no ports in the Red VLAN.

VTP pruning is enabled in the switched network. The broadcast traffic from Switch A is not forwarded to Switches C, E, and F because traffic for the Red VLAN has been pruned on the links shown (Port 5 on Switch B and Port 4 on Switch D).

With VTP versions 1 and 2, when you enable pruning on the VTP server, it is enabled for the entire VTP domain. In VTP version 3, you must manually enable pruning on each switch in the domain. Making VLANs
pruning-eligible or pruning-ineligible affects pruning eligibility for those VLANs on that trunk only (not on all switches in the VTP domain).

VTP pruning takes effect several seconds after you enable it. VTP pruning does not prune traffic from VLANs that are pruning-ineligible. VLAN 1 and VLANs 1002 to 1005 are always pruning-ineligible; traffic from these VLANs cannot be pruned. Extended-range VLANs (VLAN IDs higher than 1005) are also pruning-ineligible.

**Related Topics**

Enabling VTP Pruning (CLI), on page 1466

---

## VTP Configuration Guidelines

### VTP Configuration Requirements

When you configure VTP, you must configure a trunk port so that the switch can send and receive VTP advertisements to and from other switches in the domain.

### VTP Settings

The VTP information is saved in the VTP VLAN database. When VTP mode is transparent, the VTP domain name and mode are also saved in the switch running configuration file, and you can save it in the switch startup configuration file by entering the `copy running-config startup-config` privileged EXEC command. You must use this command if you want to save VTP mode as transparent, even if the switch resets.

When you save VTP information in the switch startup configuration file and reboot the switch, the switch configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.

- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

**Related Topics**

Configuring VTP on a Per-Port Basis (CLI), on page 1467
Configuring a VTP Version 3 Primary Server (CLI), on page 1463

---

### Domain Names for Configuring VTP

When configuring VTP for the first time, you must always assign a domain name. You must configure all switches in the VTP domain with the same domain name. Switches in VTP transparent mode do not exchange VTP messages with other switches, and you do not need to configure a VTP domain name for them.

**Note**

If the NVRAM and DRAM storage is sufficient, all switches in a VTP domain should be in VTP server mode.
Caution

Do not configure a VTP domain if all switches are operating in VTP client mode. If you configure the domain, it is impossible to make changes to the VLAN configuration of that domain. Make sure that you configure at least one switch in the VTP domain for VTP server mode.

Related Topics

Adding a VTP Client Switch to a VTP Domain (CLI), on page 1468

Passwords for the VTP Domain

You can configure a password for the VTP domain, but it is not required. If you do configure a domain password, all domain switches must share the same password and you must configure the password on each switch in the management domain. Switches without a password or with the wrong password reject VTP advertisements.

If you configure a VTP password for a domain, a switch that is booted without a VTP configuration does not accept VTP advertisements until you configure it with the correct password. After the configuration, the switch accepts the next VTP advertisement that uses the same password and domain name in the advertisement.

If you are adding a new switch to an existing network with VTP capability, the new switch learns the domain name only after the applicable password has been configured on it.

Caution

When you configure a VTP domain password, the management domain does not function properly if you do not assign a management domain password to each switch in the domain.

Related Topics

Configuring a VTP Version 3 Password (CLI), on page 1462
Example: Configuring a Switch as the Primary Server, on page 1471

VTP Version

Follow these guidelines when deciding which VTP version to implement:

• All switches in a VTP domain must have the same domain name, but they do not need to run the same VTP version.

• A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1 if version 2 is disabled on the version 2-capable switch (version 2 is disabled by default).

• If a switch running VTP version 1, but capable of running VTP version 2, receives VTP version 3 advertisements, it automatically moves to VTP version 2.

• If a switch running VTP version 3 is connected to a switch running VTP version 1, the VTP version 1 switch moves to VTP version 2, and the VTP version 3 switch sends scaled-down versions of the VTP packets so that the VTP version 2 switch can update its database.

• A switch running VTP version 3 cannot move to version 1 or 2 if it has extended VLANs.

• Do not enable VTP version 2 on a switch unless all of the switches in the same VTP domain are version-2-capable. When you enable version 2 on a switch, all of the version-2-capable switches in the domain enable version 2. If there is a version 1-only switch, it does not exchange VTP information with switches that have version 2 enabled.
• Cisco recommends placing VTP version 1 and 2 switches at the edge of the network because they do not forward VTP version 3 advertisements.

• If there are TrBRF and TrCRF Token Ring networks in your environment, you must enable VTP version 2 or version 3 for Token Ring VLAN switching to function properly. To run Token Ring and Token Ring-Net, disable VTP version 2.

• VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must configure these VLANs manually on each device. VTP version 3 supports extended-range VLANs and support for extended range VLAN database propagation.

• When a VTP version 3 device trunk port receives messages from a VTP version 2 device, it sends a scaled-down version of the VLAN database on that particular trunk in VTP version 2 format. A VTP version 3 device does not send VTP version 2-formatted packets on a trunk unless it first receives VTP version 2 packets on that trunk port.

• When a VTP version 3 device detects a VTP version 2 device on a trunk port, it continues to send VTP version 3 packets, in addition to VTP version 2 packets, to allow both kinds of neighbors to coexist on the same trunk.

• A VTP version 3 device does not accept configuration information from a VTP version 2 or version 1 device.

• Two VTP version 3 regions can only communicate in transparent mode over a VTP version 1 or version 2 region.

• Devices that are only VTP version 1 capable cannot interoperate with VTP version 3 devices.

• VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must manually configure these VLANs on each device.

Related Topics

Enabling the VTP Version (CLI), on page 1464

How to Configure VTP

Configuring VTP Mode (CLI)

You can configure VTP mode as one of these:

• VTP server mode—In VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.

• VTP client mode—In VTP client mode, you cannot change its VLAN configuration. The client switch receives VTP updates from a VTP server in the VTP domain and then modifies its configuration accordingly.

• VTP transparent mode—In VTP transparent mode, VTP is disabled on the switch. The switch does not send VTP updates and does not act on VTP updates received from other switch. However, a VTP transparent switch running VTP version 2 does forward received VTP advertisements on its trunk links.

• VTP off mode—VTP off mode is the same as VTP transparent mode except that VTP advertisements are not forwarded.
When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>vtp domain domain-name</td>
<td>Configures the VTP administrative-domain name. The name can be 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name. This command is optional for modes other than server mode. VTP server mode requires a domain name. If the switch has a trunk connection to a VTP domain, the switch learns the domain name from the VTP server in the domain. You should configure the VTP domain before configuring other VTP parameters.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# vtp domain eng_group</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>vtp mode {client</td>
<td>server</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# vtp mode server</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>vtp password password</td>
<td>(Optional) Sets the password for the VTP domain. The password can be 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# vtp password mypassword</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a VTP Version 3 Password (CLI)

You can configure a VTP version 3 password on the switch.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vtp version 3</td>
<td>Enables VTP version 3 on the device. The default is VTP version 1.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# vtp version 3</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

VTP Modes, on page 1453
### Purpose

Command or Action | Purpose
--- | ---
Step 4 | vtp password *password [hidden | secret]*
**Example:**
```plaintext
Switch(config)# vtp password mypassword hidden
```
(Optional) Sets the password for the VTP domain. The password can be 8 to 64 characters.
- *(Optional)* **hidden**—Saves the secret key generated from the password string in the nvram: vlan.dat file. If you configure a takeover by configuring a VTP primary server, you are prompted to reenter the password.
- *(Optional)* **secret**—Directly configures the password. The secret password must contain 32 hexadecimal characters.

**Step 5**

**end**

**Example:**
```plaintext
Switch(config)# end
```
Returns to privileged EXEC mode.

**Step 6**

**show vtp password**

**Example:**
```plaintext
Switch# show vtp password
```
Verifies your entries. The output appears like this:
```
VTP password:
89914640C8D90868B6A0D8103847A733
```

**Step 7**

**copy running-config startup-config**

**Example:**
```plaintext
Switch# copy running-config startup-config
```
(Optional) Saves your entries in the configuration file.

### Related Topics
- **Passwords for the VTP Domain**, on page 1459
- **Example: Configuring a Switch as the Primary Server**, on page 1471

## Configuring a VTP Version 3 Primary Server (CLI)

When you configure a VTP server as a VTP primary server, the takeover operation starts.

### Procedure

Command or Action | Purpose
--- | ---
Step 1 | vtp version 3
**Example:**
```
Enables VTP version 3 on the device. The default is VTP version 1.
Enabling the VTP Version (CLI)

VTP version 2 and version 3 are disabled by default.

- When you enable VTP version 2 on a switch, every VTP version 2-capable switch in the VTP domain enables version 2. To enable VTP version 3, you must manually configure it on each switch.

- With VTP versions 1 and 2, you can configure the version only on switches in VTP server or transparent mode. If a switch is running VTP version 3, you can change to version 2 when the switch is in client mode if no extended VLANs exist, and no hidden password was configured.

Caution

VTP version 1 and VTP version 2 are not interoperable on switches in the same VTP domain. Do not enable VTP version 2 unless every switch in the VTP domain supports version 2.

- In TrCRF and TrBRF Token Ring environments, you must enable VTP version 2 or VTP version 3 for Token Ring VLAN switching to function properly. For Token Ring and Token Ring-Net media, disable VTP version 2.

Caution

In VTP version 3, both the primary and secondary servers can exist on an instance in the domain.
## Enabling the VTP Version (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vtp version {1</td>
<td>2</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# vtp version 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show vtp status</td>
<td>Verifies that the configured VTP version is enabled.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show vtp status</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics
- [VTP Version](#), on page 1459
- [VTP Version 2](#), on page 1455
- [VTP Version 3](#), on page 1455
Enabling VTP Pruning (CLI)

Before you begin

VTP pruning is not designed to function in VTP transparent mode. If one or more switches in the network are in VTP transparent mode, you should do one of these actions:

- Turn off VTP pruning in the entire network.
- Turn off VTP pruning by making all VLANs on the trunk of the switch upstream to the VTP transparent switch pruning ineligible.

To configure VTP pruning on an interface, use the switchport trunk pruning vlan interface configuration command. VTP pruning operates when an interface is trunking. You can set VLAN pruning-eligibility, whether or not VTP pruning is enabled for the VTP domain, whether or not any given VLAN exists, and whether or not the interface is currently trunking.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>vtp pruning</td>
<td>Enables pruning in the VTP administrative domain.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# vtp pruning</td>
<td>By default, pruning is disabled. You need to enable pruning on only one switch in VTP server mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>show vtp status</td>
<td>Verifies your entries in the VTP Pruning Mode field of the display.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# show vtp status</td>
<td></td>
</tr>
</tbody>
</table>
Configuring VTP on a Per-Port Basis (CLI)

With VTP version 3, you can enable or disable VTP on a per-port basis. You can enable VTP only on ports that are in trunk mode. Incoming and outgoing VTP traffic are blocked, not forwarded.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  Example:  
  Switch> enable |
| **Step 2** configure terminal | Enters global configuration mode.  
  Example:  
  Switch# configure terminal |
| **Step 3** interface interface-id | Identifies an interface, and enters interface configuration mode.  
  Example:  
  Switch(config)# interface gigabitethernet0/1 |
| **Step 4** vtp | Enables VTP on the specified port.  
  Example:  
  Switch(config-if)# vtp |
| **Step 5** end | Returns to privileged EXEC mode.  
  Example:  
  Switch(config)# end |
| **Step 6** show running-config interface interface-id | Verifies the change to the port.  
  Example:  
  Switch# show running-config interface gigabitethernet 1/0/1 |
Adding a VTP Client Switch to a VTP Domain (CLI)

Follow these steps to verify and reset the VTP configuration revision number on a switch before adding it to a VTP domain.

**Before you begin**

Before adding a VTP client to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. With VTP versions 1 and 2, adding a switch that has a revision number higher than the revision number in the VTP domain can erase all VLAN information from the VTP server and VTP domain. With VTP version 3, the VLAN information is not erased.

You can use the `vtp mode transparent` global configuration command to disable VTP on the switch and then to change its VLAN information without affecting the other switches in the VTP domain.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>show vtp status</code></td>
<td>Checks the VTP configuration revision number.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# show vtp status</code></td>
<td>If the number is 0, add the switch to the VTP domain.</td>
</tr>
<tr>
<td></td>
<td>If the number is greater than 0, follow these substeps:</td>
</tr>
<tr>
<td></td>
<td>• Write down the domain name.</td>
</tr>
<tr>
<td></td>
<td>• Write down the configuration revision number.</td>
</tr>
<tr>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Step 3</strong> configure terminal</td>
<td>• Continue with the next steps to reset the switch configuration revision number.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> vtp domain domain-name</td>
<td>Changes the domain name from the original one displayed in Step 1 to a new name.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# vtp domain domain123</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode. The VLAN information on the switch is updated and the configuration revision number is reset to 0.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show vtp status</td>
<td>Verifies that the configuration revision number has been reset to 0.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show vtp status</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> vtp domain domain-name</td>
<td>Enters the original domain name on the switch</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# vtp domain domain012</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> end</td>
<td>Returns to privileged EXEC mode. The VLAN information on the switch is updated.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Monitoring VTP

This section describes commands used to display and monitor the VTP configuration.

You monitor VTP by displaying VTP configuration information: the domain name, the current VTP revision, and the number of VLANs. You can also display statistics about the advertisements sent and received by the switch.

### Table 117: VTP Monitoring Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vtp counters</td>
<td>Displays counters about VTP messages that have been sent and received.</td>
</tr>
<tr>
<td>show vtp devices [conflict]</td>
<td>Displays information about all VTP version 3 devices in the domain. Conflicts are VTP version 3 devices with conflicting primary servers. The <code>show vtp devices</code> command does not display information when the switch is in transparent or off mode.</td>
</tr>
<tr>
<td>show vtp interface [interface-id]</td>
<td>Displays VTP status and configuration for all interfaces or the specified interface.</td>
</tr>
<tr>
<td>show vtp password</td>
<td>Displays the VTP password. The form of the password displayed depends on whether or not the <code>hidden</code> keyword was entered and if encryption is enabled on the switch.</td>
</tr>
<tr>
<td>show vtp status</td>
<td>Displays the VTP switch configuration information.</td>
</tr>
</tbody>
</table>
Configuration Examples for VTP

Example: Configuring a Switch as the Primary Server

This example shows how to configure a switch as the primary server for the VLAN database (the default) when a hidden or secret password was configured:

Switch# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP domain

VTP Database Conf Switch ID Primary Server Revision System Name
------------- ---- -------------- ------------- ---------- -------------------
VLANDB Yes 00d0.00b8.1400=00d0.00b8.1400 1 stp7

Do you want to continue (y/n) [n]?
y

Related Topics
Configuring a VTP Version 3 Password (CLI), on page 1462
Passwords for the VTP Domain, on page 1459

Where to Go Next

After configuring VTP, you can configure the following:

• VLANs
• VLAN groups
• VLAN groups
• VLAN trunking

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>For complete syntax and usage information for the commands used in this chapter.</td>
<td>VLAN Command Reference (Catalyst 3850 Switches) VLAN Command Reference (Cisco WLC 5700 Series) Layer 2/3 Command Reference (Catalyst 3850 Switches) Layer 2 Command Reference (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>
### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1573</td>
<td>Evolution of the Interfaces Group of MIB-II</td>
</tr>
<tr>
<td>RFC 1757</td>
<td>Remote Network Monitoring Management</td>
</tr>
<tr>
<td>RFC 2021</td>
<td>SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>
# Feature History and Information for VTP

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 81

VLANs

• Finding Feature Information, on page 1475
• Prerequisites for VLANs, on page 1475
• Restrictions for VLANs, on page 1476
• Information About VLANs, on page 1476
• How to Configure VLANs, on page 1479
• Monitoring VLANs, on page 1491
• Where to Go Next, on page 1492
• Additional References, on page 1492
• Feature History and Information for VLANs, on page 1494

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VLANs

The following are prerequisites and considerations for configuring VLANs:

• Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network.

• If you plan to configure many VLANs on the switch and to not enable routing, you can set the Switch Database Management (SDM) feature to the VLAN template, which configures system resources to support the maximum number of unicast MAC addresses.

• Switches running the LAN Base feature set support only static routing on SVIs.

• A VLAN should be present in the switch to be able to add it to the VLAN group.
Restrictions for VLANs

The following are restrictions for VLANs:

- In the Cisco Catalyst 4500E Supervisor Engine, the number of switch per-VLAN spanning-tree (PVST) or rapid PVST is based on the number of trunks on the switch multiplied by the number of active VLANs on the trunks, plus the number of non-trunking interfaces on the switch (trunks * VLANS + non-trunk ports). For MSTP, the maximum number of MST instances supported is 4094.

- The switch supports IEEE 802.1Q trunking methods for sending VLAN traffic over Ethernet ports.

- Configuring an interface VLAN router's MAC address is not supported. The interface VLAN already has an MAC address assigned by default.

- Private VLANs are not supported on the switch.

- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

Information About VLANs

Logical Networks

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a switch supporting fallback bridging. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree.

VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch is assigned manually on an interface-by-interface basis. When you assign switch interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Traffic between VLANs must be routed.

The switch can route traffic between VLANs by using switch virtual interfaces (SVIs). An SVI must be explicitly configured and assigned an IP address to route traffic between VLANs.

Supported VLANs

The switch supports VLANs in VTP client, server, and transparent modes. VLANs are identified by a number from 1 to 4094. VLAN 1 is the default VLAN and is created during system initialization. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. All of the VLANs except 1002 to 1005 are available for user configuration.

There are 3 VTP versions: VTP version 1, version 2, and version 3. All VTP versions support both normal and extended range VLANs, but only with VTP version 3, does the switch propagate extended range VLAN.
configuration information. When extended range VLANs are created in VTP versions 1 and 2, their configuration information is not propagated. Even the local VTP database entries on the switch are not updated, but the extended range VLANs configuration information is created and stored in the running configuration file.

You can configure up to 4049 VLANs on the switch.

### VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic the port carries and the number of VLANs to which it can belong.

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis.

<table>
<thead>
<tr>
<th>Membership Mode</th>
<th>VLAN Membership Characteristics</th>
<th>VTP Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static-access</td>
<td>A static-access port can belong to one VLAN and is manually assigned to that VLAN.</td>
<td>VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent. To participate in VTP, there must be at least one trunk port on the switch connected to a trunk port of a second switch.</td>
</tr>
</tbody>
</table>
| Trunk (IEEE 802.1Q) :  
  * IEEE 802.1Q—Industry-standard trunking encapsulation. | A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the list. | VTP is recommended but not required. VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other switches over trunk links. |
| Voice VLAN       | A voice VLAN port is an access port attached to a Cisco IP Phone, configured to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone. | VTP is not required; it has no effect on a voice VLAN. |

**Related Topics**

- Assigning Static-Access Ports to a VLAN (CLI), on page 1484
- Monitoring VLANs, on page 1491
VLAN Configuration Files

Configurations for VLAN IDs 1 to 1005 are written to the vlan.dat file (VLAN database), and you can display them by entering the `show vlan` privileged EXEC command. The vlan.dat file is stored in flash memory. If the VTP mode is transparent, they are also saved in the switch running configuration file.

You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the `show running-config` privileged EXEC command.

When you save VLAN and VTP information (including extended-range VLAN configuration information) in the startup configuration file and reboot the switch, the switch configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration, and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VLAN and VTP configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.

- If the VTP mode or domain name in the startup configuration does not match the VLAN database, the domain name and VTP mode and configuration for the VLAN IDs 1 to 1005 use the VLAN database information.

- In VTP versions 1 and 2, if VTP mode is server, the domain name and VLAN configuration for VLAN IDs 1 to 1005 use the VLAN database information. VTP version 3 also supports VLANs 1006 to 4094.

- From image 15.0(02)SE6, on vtp transparent and off modes, vlans get created from startup-config even if they are not applied to the interface.

---

**Note**

Ensure that you delete the vlan.dat file along with the configuration files before you reset the switch configuration using `write erase` command. This ensures that the switch reboots correctly on a reset.

---

Normal-Range VLAN Configuration Guidelines

Normal-range VLANs are VLANs with IDs from 1 to 1005.

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- Normal-range VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.

- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database. If the VTP mode is transparent, VTP and VLAN configurations are also saved in the switch running configuration file.

- If the switch is in VTP server or VTP transparent mode, you can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)

- Extended-range VLANs created in VTP transparent mode are not saved in the VLAN database and are not propagated. VTP version 3 supports extended range VLAN (VLANs 1006 to 4094) database propagation in VTP server mode.

- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. If the switch is a VTP server, you must define a VTP domain or VTP will not function.
• The switch does not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.

• The switch supports 128 spanning tree instances. If a switch has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 128 VLANs and is disabled on the remaining VLANs.

If you have already used all available spanning-tree instances on a switch, adding another VLAN anywhere in the VTP domain creates a VLAN on that switch that is not running spanning-tree. If you have the default allowed list on the trunk ports of that switch (which is to allow all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent switches that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances.

If the number of VLANs on the switch exceeds the number of supported spanning-tree instances, we recommend that you configure the IEEE 802.1s Multiple STP (MSTP) on your switch to map multiple VLANs to a single spanning-tree instance.

Related Topics
Creating or Modifying an Ethernet VLAN (CLI), on page 1480
Monitoring VLANs, on page 1491

Extended-Range VLAN Configuration Guidelines

Extended-range VLANs are VLANs with IDs from 1006 to 4094.

Follow these guidelines when creating extended-range VLANs:

• VLAN IDs in the extended range are not saved in the VLAN database and are not recognized by VTP unless the switch is running VTP version 3.

• You cannot include extended-range VLANs in the pruning eligible range.

• For VTP version 1 or 2, you can set the VTP mode to transparent in global configuration mode. You should save this configuration to the startup configuration so that the switch boots up in VTP transparent mode. Otherwise, you lose the extended-range VLAN configuration if the switch resets. If you create extended-range VLANs in VTP version 3, you cannot convert to VTP version 1 or 2.

Related Topics
Creating an Extended-Range VLAN (CLI), on page 1486
Monitoring VLANs, on page 1491

How to Configure VLANs

How to Configure Normal-Range VLANs

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

• VLAN ID
• VLAN name
• VLAN type
  • Ethernet
  • Fiber Distributed Data Interface [FDDI]
  • FDDI network entity title [NET]
  • TrBRF or TrCRF
  • Token Ring
  • Token Ring-Net
• VLAN state (active or suspended)
• Security Association Identifier (SAID)
• Bridge identification number for TrBRF VLANs
• Ring number for FDDI and TrCRF VLANs
• Parent VLAN number for TrCRF VLANs
• Spanning Tree Protocol (STP) type for TrCRF VLANs
• VLAN number to use when translating from one VLAN type to another

You can cause inconsistency in the VLAN database if you attempt to manually delete the vlan.dat file. If you want to modify the VLAN configuration, follow the procedures in this section.

**Creating or Modifying an Ethernet VLAN (CLI)**

**Before you begin**

With VTP version 1 and 2, if the switch is in VTP transparent mode, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database.

The switch supports only Ethernet interfaces. Because FDDI and Token Ring VLANs are not locally supported, you only configure FDDI and Token Ring media-specific characteristics for VTP global advertisements to other switches.

Although the switch does not support Token Ring connections, a remote device with Token Ring connections could be managed from one of the supported switches. Switches running VTP Version 2 advertise information about these Token Ring VLANs:

• Token Ring TrBRF VLANs
• Token Ring TrCRF VLANs
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 vlan vlan-id</td>
<td>Enters a VLAN ID, and enters VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN.</td>
</tr>
<tr>
<td>Example: Switch(config)# vlan 20</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The available VLAN ID range for this command is 1 to 4094.</td>
</tr>
</tbody>
</table>

Additional `vlan` command options include:

- **access-map**—Creates VLAN access-maps or enters the `vlan` access map command mode.
- **configuration**—Enters the `vlan` feature configuration mode.
- **dot1q**—Configures VLAN dot1q tag native parameters.
- **filter**—Applies a VLAN filter map to a VLAN list.
- **group**—Creates a VLAN group.

| Step 3 name vlan-name | (Optional) Enters a name for the VLAN. If no name is entered for the VLAN, the default is to append the `vlan-id` value with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4. |
| Example: Switch(config-vlan)# name test20 | |

The following additional VLAN configuration command options are available:

- **are**—Sets the maximum number of All Router Explorer (ARE) hops for the VLAN.
- **backupcrf**—Enables or disables the backup concentrator relay function (CRF) mode for the VLAN.
- **bridge**—Sets the value of the bridge number for the FDDI net or Token Ring net type VLANs.
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>exit</strong>—Applies changes, bumps the revision number, and exits.</td>
</tr>
<tr>
<td>• <strong>media</strong>—Sets the media type of the VLAN.</td>
</tr>
<tr>
<td>• <strong>no</strong>—Negates the command or default.</td>
</tr>
<tr>
<td>• <strong>parent</strong>—Sets the value of the ID for the parent VLAN for FDDI or Token Ring type VLANs.</td>
</tr>
<tr>
<td>• <strong>remote-span</strong>—Configures a remote SPAN VLAN.</td>
</tr>
<tr>
<td>• <strong>ring</strong>—Sets the ring number value for FDDI or Token Ring type VLANs.</td>
</tr>
<tr>
<td>• <strong>said</strong>—Sets the IEEE 802.10 SAID value.</td>
</tr>
<tr>
<td>• <strong>shutdown</strong>—Shuts down the VLAN switching.</td>
</tr>
<tr>
<td>• <strong>state</strong>—Sets the operational VLAN state to active or suspended.</td>
</tr>
<tr>
<td>• <strong>ste</strong>—Sets the maximum number of Spanning Tree Explorer (STE) hops for the VLAN.</td>
</tr>
<tr>
<td>• <strong>stp</strong>—Sets the Spanning Tree characteristics of the VLAN.</td>
</tr>
</tbody>
</table>

### Step 4

**media** { ethernet | fd-net | fddi | tokenring | trn-net }

**Example:**

```
Switch(config-vlan)# media ethernet
```

Configures the VLAN media type. Command options include:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet</td>
<td>Sets the VLAN media type as Ethernet.</td>
</tr>
<tr>
<td>fd-net</td>
<td>Sets the VLAN media type as FDDI net.</td>
</tr>
<tr>
<td>fddi</td>
<td>Sets the VLAN media type as FDDI.</td>
</tr>
<tr>
<td>tokenring</td>
<td>Sets the VLAN media type as Token Ring.</td>
</tr>
<tr>
<td>trn-net</td>
<td>Sets the VLAN media type as Token Ring net.</td>
</tr>
</tbody>
</table>

### Step 5

**remote-span**

**Example:**

(Optional) Configures the VLAN as the RSPAN VLAN for a remote SPAN session. For more information on remote SPAN, see the *Catalyst...*
Deleting a VLAN (CLI)

When you delete a VLAN from a switch that is in VTP server mode, the VLAN is removed from the VLAN database for all switches in the VTP domain. When you delete a VLAN from a switch that is in VTP transparent mode, the VLAN is deleted only on that specific switch.

You cannot delete the default VLANs for the different media types: Ethernet VLAN1 and FDDI or Token Ring VLANs1002 to 1005.

Caution

When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-vlan)# remote-span</td>
<td>3850 Network Management Configuration Guide.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 7 show vlan {name vlan-name</td>
<td>id vlan-id}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show vlan name test20 id 20</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

Normal-Range VLAN Configuration Guidelines, on page 1478
Monitoring VLANs, on page 1491
Assigning Static-Access Ports to a VLAN (CLI)

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information by disabling VTP (VTP transparent mode).

For the Cisco Catalyst 9500 Series Switches, if you are assigning a port on a cluster member switch to a VLAN, first use the `rcommand` privileged EXEC command to log in to the cluster member switch.

If you assign an interface to a VLAN that does not exist, the new VLAN is created.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
| | Example: |  
| | Switch> enable |  
| Step 2 | configure terminal | Enters global configuration mode  
| | Example: |  
| | Switch> configure terminal |  

Related Topics

- Monitoring VLANs, on page 1491
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Enters the interface to be added to the VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport mode access</td>
<td>Defines the VLAN membership mode for the port (Layer 2 access port).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> switchport access vlan vlan-id</td>
<td>Assigns the port to a VLAN. Valid VLAN IDs are 1 to 4094.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# switchport access vlan 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show running-config interface interface-id</td>
<td>Verifies the VLAN membership mode of the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> show interfaces interface-id switchport</td>
<td>Verifies your entries in the Administrative Mode and the Access Mode VLAN fields of the display.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show interfaces gigabitethernet2/0/1 switchport</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
How to Configure Extended-Range VLANs

Extended-range VLANs enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any `switchport` commands that allow VLAN IDs.

With VTP version 1 or 2, extended-range VLAN configurations are not stored in the VLAN database, but because VTP mode is transparent, they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file. Extended-range VLANs created in VTP version 3 are stored in the VLAN database.

You can change only the MTU size and the remote SPAN configuration state on extended-range VLANs; all other characteristics must remain at the default state.

Creating an Extended-Range VLAN (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
Example: Switch> enable  
- Enter your password if prompted. |
| Step 2 | `configure terminal` | Enters global configuration mode.  
Example: Switch# configure terminal |
| Step 3 | `vlan vlan-id` | Enters an extended-range VLAN ID and enters VLAN configuration mode. The range is 1006 to 4094.  
Example: Switch(config)# vlan 2000  
Switch(config-vlan)# |
| Step 4 | `remote-span` | (Optional) Configures the VLAN as the RSPAN VLAN.  
Example: Switch(config-vlan)# remote-span |
| Step 5 | `exit` | Returns to configuration mode.  
Example: |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Switch(config-vlan)# exit
Switch(config)# | Enters the interface configuration mode for the selected VLAN. |
| **Step 6** interface vlan
**Example:**
Switch(config)# interface vlan 200
Switch(config-if)# | (Optional) Modifies the VLAN by changing the MTU size. You can configure the MTU size between 68 to 1500 bytes. **Note** Although all VLAN commands appear in the CLI help, only the `ip mtu mtu-size` and `remote-span` commands are supported for extended-range VLANs. |
| **Step 7** ip mtu mtu-size
**Example:**
Switch(config-if)# ip mtu 1024
Switch(config-if)# | |
| **Step 8** end
**Example:**
Switch(config)# end | Returns to privileged EXEC mode. |
| **Step 9** show vlan id vlan-id
**Example:**
Switch# show vlan id 2000 | Verifies that the VLAN has been created. |
| **Step 10** copy running-config startup-config
**Example:**
Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

**Related Topics**
- Extended-Range VLAN Configuration Guidelines, on page 1479
- Monitoring VLANs, on page 1491
How to Configure VLANs (GUI)

Creating Layer2 VLAN (GUI)

To create a Layer2 VLAN using the switch web UI, you must follow the steps defined in this procedure.

Procedure

Step 1  
To create a Layer2 VLAN, choose **Configuration > Controller > System > VLAN > Layer2 VLAN.** The VLAN Layer2 page appears. You must provide values for all parameters listed in the Layer2 page.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>VLAN tag identifier, or 0 for no VLAN tag.</td>
</tr>
<tr>
<td>Name</td>
<td>VLAN name.</td>
</tr>
</tbody>
</table>
| State     | VLAN state. Values are the following:  
  • Active  
  • Suspended |

Step 2  
Click **Apply.**

Creating Layer3 Interface (GUI)

To create a Layer3 interface using the switch web UI, you must follow the steps defined in this procedure.

Procedure

Step 1  
To create a Layer3 interface, choose **Configuration > Controller > System > VLAN > Layer3 Interface.** The Layer3 interface page appears. You must provide values for all parameters listed in the window.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description for the Layer3 interface.</td>
</tr>
<tr>
<td>DHCP Relay Information</td>
<td>Information on controller built-in DHCP relay agents.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address/subnet mask of the VLAN SVI (Switch Virtual Interface).</td>
</tr>
<tr>
<td>Mask Address</td>
<td>Mask address of the DHCP server.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>IPv6 address of the DHCP server.</td>
</tr>
<tr>
<td>IPv4 DHCP Server</td>
<td>IPv4 address of the DHCP server.</td>
</tr>
<tr>
<td>IPv6 DHCP Server</td>
<td>IPv6 address of the DHCP server.</td>
</tr>
</tbody>
</table>
Step 2  Click Apply.

Viewing Layer2 VLAN (GUI)

You can view the details of the Layer2 VLANs configured in the switch interface using the web UI.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Configuration &gt; Controller &gt; System &gt; VLAN &gt; Layer2 VLAN.</td>
<td>The Layer2 VLAN page appears, listing the following details of the Layer2 VLANs in the switch.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>Displays VLAN tag identifier.</td>
</tr>
<tr>
<td>Name</td>
<td>VLAN name.</td>
</tr>
<tr>
<td>State</td>
<td>VLAN state. Values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Active</td>
</tr>
<tr>
<td></td>
<td>• Suspended</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit.</td>
</tr>
</tbody>
</table>

Viewing Layer3 Interface (GUI)

You can view the details of the Layer3 interfaces configured in the switch interface using the web UI.

Procedure

Choose Configuration > Controller > System > VLAN > Layer3 Interface.  
The Layer2 VLAN page appears, listing the following details of the Layer3 interfaces in the switch.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Layer3 interface name.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the Layer3 interface. Values are the following:</td>
</tr>
<tr>
<td></td>
<td>• Up</td>
</tr>
<tr>
<td></td>
<td>• Down</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol used for Layer3 interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address used for Layer3 security and mobility managers.</td>
</tr>
</tbody>
</table>
Removing Layer2 VLAN (GUI)

To remove a Layer2 VLANs using the switch web UI, you must:

**Procedure**

**Step 1** Choose **Configuration > Controller > System > VLAN > Layer2 VLAN**.

The Layer2 VLAN page appears, listing the following details of the Layer2 VLANs associated with the switch.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>Displays VLAN tag identifier.</td>
</tr>
<tr>
<td>Name</td>
<td>VLAN name.</td>
</tr>
<tr>
<td>State</td>
<td>VLAN state. Values as follows:</td>
</tr>
<tr>
<td></td>
<td>• Active</td>
</tr>
<tr>
<td></td>
<td>• Suspended</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit.</td>
</tr>
</tbody>
</table>

**Step 2** Check the checkbox of the Layer2 VLAN you need to delete from the Layer2 VLANs displayed in the Layer2 VLAN list.

You will receive a confirmation message confirming deletion of the selected Layer2 VLAN.

**Step 3** Click **Ok**.

---

Removing Layer3 Interface (GUI)

To remove a Layer3 interface using the switch web UI, you must:

**Procedure**

**Step 1** Choose **Configuration > Controller > System > VLAN > Layer3 Interface**.

The Layer3 interface page appears, listing the following details of the Layer3 interfaces associated with the switch.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Layer3 interface name.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the Layer3 interface. Values are the following:</td>
</tr>
<tr>
<td></td>
<td>• Up</td>
</tr>
<tr>
<td></td>
<td>• Down</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol used for Layer3 interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address used for Layer3 security and mobility managers.</td>
</tr>
</tbody>
</table>
Step 2  
Check the checkbox of the Layer3 interfaces you need to delete from the Layer3 interfaces displayed in the Layer3 interfaces.
You will receive a confirmation message confirming deletion of the selected Layer3 interface.

Step 3  
Click Ok.

## Monitoring VLANs

**Table 119: Privileged EXEC show Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces [vlan vlan-id]</code></td>
<td>Displays characteristics for all interfaces or for the specified VLAN configured on the switch.</td>
</tr>
</tbody>
</table>
| `show vlan [ access-map name ] | brief | dot1q | [ tag native ] | [ filter [ access-map | vlan ] | group [ group-name name ] | id vlan-id | ifindex | mtu | name name | remote-span | summary ]` | Displays parameters for all VLANs or the specified VLAN on the switch. The following command options are available: 
  - `access-map`—Displays the VLAN access-maps.
  - `brief`—Displays VTP VLAN status in brief.
  - `dot1q`—Displays the dot1q parameters.
  - `filter`—Displays VLAN filter information.
  - `group`—Displays the VLAN group with its name and the connected VLANs that are available.
  - `id`—Displays VTP VLAN status by identification number.
  - `ifindex`—Displays SNMP ifIndex.
  - `mtu`—Displays VLAN MTU information.
  - `name`—Displays the VTP VLAN information by specified name.
  - `remote-span`—Displays the remote SPAN VLANs.
  - `summary`—Displays a summary of VLAN information. |

**Related Topics**

- [Creating or Modifying an Ethernet VLAN (CLI)], on page 1480
- [Normal-Range VLAN Configuration Guidelines], on page 1478
- [Deleting a VLAN (CLI)], on page 1483
- [Assigning Static-Access Ports to a VLAN (CLI)], on page 1484
- [VLAN Port Membership Modes], on page 1477
- [Creating an Extended-Range VLAN (CLI)], on page 1486
- [Extended-Range VLAN Configuration Guidelines], on page 1479

---

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
Where to Go Next

After configuring VLANs, you can configure the following:

- VLAN groups
- VLAN Trunking Protocol (VTP)
- VLAN trunks

Additional References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>For complete syntax and usage information for the commands used in this chapter.</td>
<td>VLAN Command Reference (Catalyst 3850 Switches) VLAN Command Reference (Cisco WLC 5700 Series) Layer 2/3 Command Reference (Catalyst 3850 Switches) Layer 2 Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>VLAN and Mobility Agents</td>
<td>Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Related Topic</td>
<td>Document Title</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SPAN</td>
<td>Network Management Command Reference (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>Network Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td></td>
<td>Network Management Configuration Guide (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>Network Management Configuration Guide (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Platform-independent configuration</td>
<td>Identity Based Networking Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>information</td>
<td></td>
</tr>
</tbody>
</table>

**Error Message Decoder**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
<tr>
<td>the Error Message Decoder tool.</td>
<td></td>
</tr>
</tbody>
</table>

**Standards and RFCs**

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1573</td>
<td>Evolution of the Interfaces Group of MIB-II</td>
</tr>
<tr>
<td>RFC 1757</td>
<td>Remote Network Monitoring Management</td>
</tr>
<tr>
<td>RFC 2021</td>
<td>SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2</td>
</tr>
</tbody>
</table>

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use</td>
</tr>
<tr>
<td></td>
<td>Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/">http://www.cisco.com/</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td>support</td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Feature History and Information for VLANs

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>VLAN GUI support.</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
VLAN Groups

- Finding Feature Information, on page 1495
- Prerequisites for VLAN Groups, on page 1495
- Restrictions for VLAN Groups, on page 1495
- Information About VLAN Groups, on page 1496
- How to Configure VLAN Groups, on page 1496
- Where to Go Next, on page 1500
- Additional References, on page 1500
- Feature History and Information for VLAN Groups, on page 1502

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VLAN Groups

- A VLAN should be present in the switch for it to be added to the VLAN group.

- For a VLAN group to function properly, in addition to enabling DHCP snooping globally, you must ensure that DHCP snooping is enabled in all the VLANs.

Restrictions for VLAN Groups

- The number of VLANs mapped to a VLAN group is not limited by Cisco IOS XE software release. However, if the number of VLANs in a VLAN group exceeds the recommended value of 32, the mobility functionality might not work as expected and in the VLAN group, L2 multicast breaks for some VLANs. Therefore, it is the responsibility of network administrators to configure feasible number of VLANs in...
Information About VLAN Groups

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

The VLAN Groups feature uses a single WLAN that can support multiple VLANs. The clients can get assigned to one of the configured VLANs. This feature maps a WLAN to a single VLAN or multiple VLANs using the VLAN groups. When a wireless client associates to the WLAN, the VLAN is derived by an algorithm based on the MAC address of the wireless client. A VLAN is assigned to the client and the client gets the IP address from the assigned VLAN. This feature also extends the current AP group architecture and AAA override architecture, where the AP groups and AAA override can override a VLAN or a VLAN group to which the WLAN is mapped.

When a client associates with a WLAN and the WLAN is applied to a VLAN group, an index is calculated based on the MAC address of the client and the number of VLANs in the VLAN group using a hash algorithm. Based on this index, a VLAN is assigned to the client. If the index is "dirty," another index is generated in a round-robin manner and the VLAN is assigned to the client based on the newly generated index.

The system marks VLAN as Dirty for 30 minutes when the clients are unable to receive IP addresses using DHCP. The system might not clear the Dirty flag from the VLAN even after 30 minutes for a VLAN group. After 30 minutes, when the VLAN is marked non-dirty, new clients in the IP Learn state can get assigned with IP addresses from the VLAN if free IPs are available in the pool and DHCP scope is defined correctly. This is the expected behavior because the timestamp of each interface has to be checked to see if it is greater than 30 minutes, due to which there is a lag of 5 minutes for the global timer to expire.

Related Topics
   Creating a VLAN Group (CLI), on page 1496

How to Configure VLAN Groups

Creating a VLAN Group (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>


Removing a VLAN Group (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td><code>Switch(config)#configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>vlan group WORD vlan-list vlan-ID</code></td>
<td>Creates a VLAN group with the given group name (vlangrp1) and adds all the VLANs listed in the command. The VLAN list ranges from 1 to 4096 and the recommended number of VLANs in a group is 32.</td>
</tr>
<tr>
<td><code>Switch(config)#vlan group vlangrp1 vlan-list 91-95</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>no vlan group WORD vlan-list vlan-ID</code></td>
<td>Removes the VLAN group with the given group name (vlangrp1).</td>
</tr>
<tr>
<td><code>Switch(config)#no vlan group vlangrp1 vlan-list 91-95</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Exits global configuration mode and returns to privileged EXEC mode. Alternatively, press <code>CTRL-Z</code> to exit the global configuration mode.</td>
</tr>
<tr>
<td><code>Switch(config)#end</code></td>
<td></td>
</tr>
</tbody>
</table>

Creating VLAN Groups (GUI)

To create a VLAN group using the switch web UI, you must:
Procedure

**Step 1** Choose **Configuration > Controller > System > VLAN > VLAN Group.**

The VLAN Group page appears. You must provide values for all parameters listed in the VLAN Group window.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Group Name</td>
<td>Group name for the VLANs.</td>
</tr>
<tr>
<td>VLAN List</td>
<td>The VLAN list to configure the mesh access point (MAP) access port.</td>
</tr>
</tbody>
</table>

**Step 2** Click **Apply.**

---

**Adding a VLAN Group to a WLAN (CLI)**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global command mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wlan WORD number</td>
<td>Enables the WLAN to map a VLAN group using an identifier. The WLAN identifier values range from 1 to 512.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)#wlan wlanname 512</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> client vlan WORD</td>
<td>Maps the VLAN group to the WLAN by entering the VLAN identifier, VLAN group, or the VLAN name.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-wlan)#client vlan vlangrp1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits global configuration mode and returns to privileged EXEC mode. Alternatively, press CTRL-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-wlan)#end</td>
<td></td>
</tr>
</tbody>
</table>

---

**Adding a VLAN Group to WLAN (GUI)**

To add a VLAN group to WLAN using the switch web UI, you must follow the steps defined in this procedure.

**Procedure**

**Step 1** To add a VLAN group to a WLAN, choose **Configuration > Wireless > WLANs > WLAN Profile > General.**
The general parameter page of the WLAN group appears.

**Step 2** Select the VLAN group values listed in the **Interface/Interface Group** drop-down list to associate the selected WLAN profile to a VLAN group.

**Step 3** Click **Apply**.

---

### Removing VLAN Groups (GUI)

To remove a VLAN groups using the switch web UI, you must:

**Procedure**

**Step 1** Choose **Configuration > Controller > System > VLAN > VLAN Group**.

The VLAN Group page appears, listing the following details of the VLAN groups associated with the switch.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Group Name</td>
<td>Group name for the VLANs.</td>
</tr>
<tr>
<td>VLAN List</td>
<td>The VLAN list to configure the mesh access point (MAP) access port.</td>
</tr>
</tbody>
</table>

**Step 2** Check the checkbox of the VLAN group you need to delete from the VLAN group names displayed in the VLAN group list.

You will receive a confirmation message confirming deletion of the selected VLAN group.

**Step 3** Click **Ok**.

---

### Viewing the VLANs in a VLAN Group (CLI)

**Command** | **Description**                |
-------------|--------------------------------|
show vlan group | Displays the list of VLAN groups with name and the VLANs that are available. |
show vlan group group-name group_name | Displays the specified VLAN group details. |
show wireless vlan group group_name | Displays the specified wireless VLAN group details. |

---

### Viewing VLAN Groups (GUI)

To view a VLAN groups using the switch web UI, you must:

**Procedure**

**Step 1** Choose **Configuration > Controller > System > VLAN > VLAN Group**.
The VLAN Group page appears, listing the following details of the VLAN groups associated with the switch.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Group Name</td>
<td>Group name for the VLANs.</td>
</tr>
<tr>
<td>VLAN List</td>
<td>The VLAN list to configure the mesh access point (MAP) access port.</td>
</tr>
</tbody>
</table>

**Step 2** Click **Apply**.

**Where to Go Next**

After configuring VLAN groups, you can configure the following:

- VLANs
- VLAN Trunking Protocol (VTP)
- VLAN trunks

**Additional References**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>
| For complete syntax and usage information for the commands used in this chapter. | *VLAN Command Reference (Catalyst 3850 Switches)*  *VLAN Command Reference (Cisco WLC 5700 Series)*  
|                             | *Layer 2/3 Command Reference (Catalyst 3850 Switches)*  *Layer 2 Command Reference (Cisco WLC 5700 Series)* |
| VLAN access-maps            | *Security Configuration Guide (Catalyst 3850 Switches)*  *Security Configuration Guide (Cisco WLC 5700 Series)*  
|                             | *Security Command Reference (Catalyst 3850 Switches)*  *Security Command Reference (Cisco WLC 5700 Series)* |
| VLAN and Mobility Agents    | *Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* |
|                             | *Flexible Netflow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* |
### Related Topic | Document Title
--- | ---
IGMP Snooping | IP Multicast Routing Command Reference (Catalyst 3850 Switches)Cisco 5760 Multicast Command Reference (Cisco WLC 5700 Series)
| IP Multicast Routing Configuration Guide (Catalyst 3850 Switches)Routing Configuration Guide (Cisco WLC 5700 Series)
| IPv6 Command Reference (Catalyst 3850 Switches)IPv6 Command Reference (Cisco WLC 5700 Series)
SPAN | Network Management Command Reference (Catalyst 3850 Switches)Network Management Command Reference (Cisco WLC 5700 Series)
| Network Management Configuration Guide (Catalyst 3850 Switches)Network Management Configuration Guide (Cisco WLC 5700 Series)
Platform-independent configuration information | Identity Based Networking Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

### Error Message Decoder

| Description | Link |
--- | ---|
To help you research and resolve system error messages in this release, use the Error Message Decoder tool. | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

### Standards and RFCs

| Standard/RFC | Title |
--- | ---|
RFC 1573 | Evolution of the Interfaces Group of MIB-II |
RFC 1757 | Remote Network Monitoring Management |
RFC 2021 | SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2 |

### MIBs

| MIB | MI Bs Link |
--- | ---|
All the supported MIBs for this release. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information for VLAN Groups

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2E</td>
<td>This feature was introduced</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>VLAN GUI support.</td>
</tr>
</tbody>
</table>
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VLAN Trunks

The IEEE 802.1Q trunks impose these limitations on the trunking strategy for a network:

- In a network of Cisco switches connected through IEEE 802.1Q trunks, the switches maintain one spanning-tree instance for each VLAN allowed on the trunks. Non-Cisco devices might support one spanning-tree instance for all VLANs.

When you connect a Cisco switch to a non-Cisco device through an IEEE 802.1Q trunk, the Cisco switch combines the spanning-tree instance of the VLAN of the trunk with the spanning-tree instance of the non-Cisco IEEE 802.1Q switch. However, spanning-tree information for each VLAN is maintained by Cisco switches separated by a cloud of non-Cisco IEEE 802.1Q switches. The non-Cisco IEEE 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.
• Make sure the native VLAN for an IEEE 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.

• Disabling spanning tree on the native VLAN of an IEEE 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an IEEE 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure your network is loop-free before disabling spanning tree.

Restrictions for VLAN Trunks

The following are restrictions for VLAN trunks:

• A trunk port cannot be a secure port.

• Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch propagates the setting that you entered to all ports in the group:
  • Allowed-VLAN list.
  • STP port priority for each VLAN.
  • STP Port Fast setting.
  • Trunk status:
    If one port in a port group ceases to be a trunk, all ports cease to be trunks.

• We recommend that you configure no more than 24 trunk ports in Per VLAN Spanning Tree (PVST) mode and no more than 40 trunk ports in Multiple Spanning Tree (MST) mode.

• If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.

• A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable IEEE 802.1x on a dynamic port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, the port mode is not changed.

• Dynamic Trunking Protocol (DTP) is not supported on tunnel ports.

• The switch does not support Layer 3 trunks; you cannot configure subinterfaces or use the encapsulation keyword on Layer 3 interfaces. The switch does support Layer 2 trunks and Layer 3 VLAN interfaces, which provide equivalent capabilities.

• You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.
Information About VLAN Trunks

Trunking Overview

A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

The following trunking encapsulations are available on all Ethernet interfaces:

- IEEE 802.1Q — Industry-standard trunking encapsulation.

Trunking Modes

Ethernet trunk interfaces support different trunking modes. You can set an interface as trunking or nontrunking or to negotiate trunking with the neighboring interface. To autonegotiate trunking, the interfaces must be in the same VTP domain.

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a Point-to-Point Protocol (PPP). However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations.

Related Topics

- Configuring a Trunk Port (CLI), on page 1508
- Layer 2 Interface Modes, on page 1505

Layer 2 Interface Modes

Table 120: Layer 2 Interface Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport mode access</td>
<td>Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface regardless of whether or not the neighboring interface is a trunk interface.</td>
</tr>
<tr>
<td>switchport mode dynamic auto</td>
<td>Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. The default switchport mode for all Ethernet interfaces is dynamic auto.</td>
</tr>
<tr>
<td>switchport mode dynamic desirable</td>
<td>Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode.</td>
</tr>
<tr>
<td>switchport mode trunk</td>
<td>Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.</td>
</tr>
</tbody>
</table>
Function Mode

PreventstheinterfacefromgeneratingDTPframes. You can use this command only when the interface switchport mode is *access* or *trunk*. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport nonegotiate</td>
<td>Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is <em>access</em> or <em>trunk</em>. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring a Trunk Port (CLI), on page 1508
- Trunking Modes, on page 1505

### Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk.

To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), DTP, and VTP in VLAN 1.

If a trunk port with VLAN 1 disabled is converted to a nontrunk port, it is added to the access VLAN. If the access VLAN is set to 1, the port will be added to VLAN 1, regardless of the *switchport trunk allowed* setting. The same is true for any VLAN that has been disabled on the port.

A trunk port can become a member of a VLAN if the VLAN is enabled, if VTP knows of the VLAN, and if the VLAN is in the allowed list for the port. When VTP detects a newly enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of the enabled VLAN. When VTP detects a new VLAN and the VLAN is not in the allowed list for a trunk port, the trunk port does not become a member of the new VLAN.

**Related Topics**

- Defining the Allowed VLANs on a Trunk (CLI), on page 1510

### Load Sharing on Trunk Ports

Load sharing divides the bandwidth supplied by parallel trunks connecting switches. To avoid loops, STP normally blocks all but one parallel link between switches. Using load sharing, you divide the traffic between the links according to which VLAN the traffic belongs.

You configure load sharing on trunk ports by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same switch. For load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches.

### Network Load Sharing Using STP Priorities

When two ports on the same switch form a loop, the switch uses the STP port priority to decide which port is enabled and which port is in a blocking state. You can set the priorities on a parallel trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port sends or receives all traffic for the VLAN.
Network Load Sharing Using STP Path Cost

You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs, blocking different ports for different VLANs. The VLANs keep the traffic separate and maintain redundancy in the event of a lost link.

Feature Interactions

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port.
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch propagates the setting that you entered to all ports in the group:
  - Allowed-VLAN list.
  - STP port priority for each VLAN.
  - STP Port Fast setting.
  - Trunk status:
    If one port in a port group ceases to be a trunk, all ports cease to be trunks.

- We recommend that you configure no more than 24 trunk ports in Per VLAN Spanning Tree (PVST) mode and no more than 40 trunk ports in Multiple Spanning Tree (MST) mode.
- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable IEEE 802.1x on a dynamic port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, the port mode is not changed.

How to Configure VLAN Trunks

To avoid trunking misconfigurations, configure interfaces connected to devices that do not support DTP to not forward DTP frames, that is, to turn off DTP:

- If you do not intend to trunk across those links, use the `switchport mode access` interface configuration command to disable trunking.
To enable trunking to a device that does not support DTP, use the `switchport mode trunk` and `switchport nonegotiate` interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Configuring an Ethernet Interface as a Trunk Port

Configuring a Trunk Port (CLI)

Because trunk ports send and receive VTP advertisements, to use VTP you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of a second switch. Otherwise, the switch cannot receive any VTP advertisements.

Before you begin

By default, an interface is in Layer 2 mode. The default mode for Layer 2 interfaces is `switchport mode dynamic auto`. If the neighboring interface supports trunking and is configured to allow trunking, the link is a Layer 2 trunk or, if the interface is in Layer 3 mode, it becomes a Layer 2 trunk when you enter the `switchport` interface configuration command.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
<td>Specifies the port to be configured for trunking, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface gigabitethernet 1/0/2</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport mode {dynamic {auto</td>
<td>desirable}</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# switchport mode dynamic desirable</td>
<td>• <code>dynamic auto</code>—Sets the interface to a trunk link if the neighboring interface is set to trunk or desirable mode. This is the default.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• dynamic desirable</td>
<td>Sets the interface to a trunk link if the neighboring interface is set to trunk, desirable, or auto mode.</td>
</tr>
<tr>
<td>• trunk</td>
<td>Sets the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.</td>
</tr>
</tbody>
</table>

#### Step 5

**switchport access vlan** *vlan-id*

**Example:**

Switch(config-if)# switchport access vlan 200

(Optional) Specifies the default VLAN, which is used if the interface stops trunking.

#### Step 6

**switchport trunk native vlan** *vlan-id*

**Example:**

Switch(config-if)# switchport trunk native vlan 200

Specifies the native VLAN for IEEE 802.1Q trunks.

#### Step 7

**end**

**Example:**

Switch(config)# end

Returns to privileged EXEC mode.

#### Step 8

**show interfaces interface-id switchport**

**Example:**

Switch# show interfaces gigabitethernet 1/0/2 switchport

Displays the switch port configuration of the interface in the Administrative Mode and the Administrative Trunking Encapsulation fields of the display.

#### Step 9

**show interfaces interface-id trunk**

**Example:**

Switch# show interfaces gigabitethernet 1/0/2 trunk

Displays the trunk configuration of the interface.

#### Step 10

**copy running-config startup-config**

**Example:**

Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.
Defining the Allowed VLANs on a Trunk (CLI)

VLAN 1 is the default VLAN on all trunk ports in all Cisco switches, and it has previously been a requirement that VLAN 1 always be enabled on every trunk link. You can use the VLAN 1 minimization feature to disable VLAN 1 on any individual VLAN trunk link so that no user traffic (including spanning-tree advertisements) is sent or received on VLAN 1.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 1/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport mode trunk</td>
<td>Configures the interface as a VLAN trunk port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# switchport mode trunk</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> switchport trunk allowed vlan { word</td>
<td>add</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# switchport trunk allowed vlan remove 2</td>
<td></td>
</tr>
</tbody>
</table>

The *vlan-list* parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. All VLANs are allowed by default.
### Command or Action | Purpose
--- | ---
**Step 6** | **end**
  **Example:**
  
  Switch(config)# end
  
  **Purpose:**
  Returns to privileged EXEC mode.

**Step 7** | **show interfaces interface-id switchport**
  **Example:**
  
  Switch# show interfaces gigabitethernet 1/0/1 switchport
  
  **Purpose:**
  Verifies your entries in the Trunking VLANs Enabled field of the display.

**Step 8** | **copy running-config startup-config**
  **Example:**
  
  Switch# copy running-config startup-config
  
  **Purpose:**
  (Optional) Saves your entries in the configuration file.

---

## Related Topics

**Allowed VLANs on a Trunk**, on page 1506

### Changing the Pruning-Eligible List (CLI)

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. VTP pruning must be enabled for this procedure to take effect.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **enable**
  **Example:**
  
  Switch> enable
  
  **Purpose:**
  Enables privileged EXEC mode.
  - Enter your password if prompted.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2** | **configure terminal**
  **Example:**
  
  Switch# configure terminal
  
  **Purpose:**
  Enters global configuration mode.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3** | **interface interface-id**
  **Example:**
  
  Switch(config)# interface
  
  **Purpose:**
  Selects the trunk port for which VLANs should be pruned, and enters interface configuration mode.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>gigabitethernet0/1</td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**

`switchport trunk pruning vlan {add | except | none | remove} vlan-list [vlan [,vlan [...]]]`

- **Purpose**: Configures the list of VLANs allowed to be pruned from the trunk.
- **Details**: For explanations about using the `add`, `except`, `none`, and `remove` keywords, see the command reference for this release.
- **Separate non-consecutive VLAN IDs** with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are 2 to 1001. Extended-range VLANs (VLAN IDs 1006 to 4094) cannot be pruned.
- **VLANs** that are pruning-ineligible receive flooded traffic.
- **Default list**: The default list of VLANs allowed to be pruned contains VLANs 2 to 1001.

**Step 5**

`end`

- **Purpose**: Returns to privileged EXEC mode.

**Example:**

Switch(config)# end

**Step 6**

`show interfaces interface-id switchport`

- **Purpose**: Verifies your entries in the **Pruning VLANs Enabled** field of the display.

**Example:**

Switch# show interfaces gigabitethernet 1/0/1 switchport

**Step 7**

`copy running-config startup-config`

- **Purpose**: (Optional) Saves your entries in the configuration file.

**Example:**

Switch# copy running-config startup-config

---

**Configuring the Native VLAN for Untagged Traffic (CLI)**

A trunk port configured with IEEE 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

The native VLAN can be assigned any VLAN ID.

If a packet has a VLAN ID that is the same as the outgoing port native VLAN ID, the packet is sent untagged; otherwise, the switch sends the packet with a tag.
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt;</code></td>
<td><code>enable</code></td>
</tr>
</tbody>
</table>

| **Step 2**        | Enters global configuration mode. |
| `configure terminal` | |
| **Example:**      | |
| `Switch#`         | `configure terminal` |

| **Step 3**        | Defines the interface that is configured as the IEEE 802.1Q trunk, and enters interface configuration mode. |
| `interface interface-id` | |
| **Example:**      | |
| `Switch(config)#`  | `interface gigabitethernet 1/0/2` |

| **Step 4**        | Configures the VLAN that is sending and receiving untagged traffic on the trunk port. For `vlan-id`, the range is 1 to 4094. |
| `switchport trunk native vlan vlan-id` | |
| **Example:**      | |
| `Switch(config-if)#` | `switchport trunk native vlan 12` |

| **Step 5**        | Returns to privileged EXEC mode. |
| `end`             | |
| **Example:**      | |
| `Switch(config-if)#` | `end` |

| **Step 6**        | Verifies your entries in the Trunking Native Mode VLAN field. |
| `show interfaces interface-id switchport` | |
| **Example:**      | |
| `Switch#`         | `show interfaces gigabitethernet 1/0/2 switchport` |

| **Step 7**        | (Optional) Saves your entries in the configuration file. |
| `copy running-config startup-config` | |
| **Example:**      | |
| `Switch#`         | `copy running-config startup-config` |
## Configuring Trunk Ports for Load Sharing

### Configuring Load Sharing Using STP Port Priorities (CLI)

These steps describe how to configure a network with load sharing using STP port priorities.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code>&lt;br&gt;Example: <code>Switch&gt; enable</code></td>
<td>Enables privileged EXEC mode.&lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code>&lt;br&gt;Example: <code>Switch# configure terminal</code></td>
<td>Enters global configuration mode on Switch A.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>vtp domain domain-name</code>&lt;br&gt;Example: <code>Switch(config)# vtp domain workdomain</code></td>
<td>Configures a VTP administrative domain.&lt;br&gt;The domain name can be 1 to 32 characters.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>vtp mode server</code>&lt;br&gt;Example: <code>Switch(config)# vtp mode server</code></td>
<td>Configures Switch A as the VTP server.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code>&lt;br&gt;Example: <code>Switch(config)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>show vtp status</code>&lt;br&gt;Example: <code>Switch# show vtp status</code></td>
<td>Verifies the VTP configuration on both Switch A and Switch B.&lt;br&gt;In the display, check the <strong>VTP Operating Mode</strong> and the <strong>VTP Domain Name</strong> fields.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>show vlan</code>&lt;br&gt;Example: <code>Switch# show vlan</code></td>
<td>Verifies that the VLANs exist in the database on Switch A.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>8</td>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>interface interface-id</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface gigabitethernet1/0/1</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>switchport mode trunk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# switchport mode trunk</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>end</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>show interfaces interface-id switchport</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show interfaces gigabitethernet1/0/1 switchport</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Repeat the above steps on Switch A for a second port in the switch.</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Repeat the above steps on Switch B to configure the trunk ports that connect to the trunk ports configured on Switch A.</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>show vlan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show vlan</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode on Switch A.</td>
<td></td>
</tr>
</tbody>
</table>

**Purpose Command or Action**

- Enters global configuration mode.
- Defines the interface to be configured as a trunk, and enters interface configuration mode.
- Configures the port as a trunk port.
- Returns to privileged EXEC mode.
- Verifies the VLAN configuration.
- When the trunk links come up, VTP passes the VTP and VLAN information to Switch B. This command verifies that Switch B has learned the VLAN configuration.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong> interface interface-id</td>
<td>Defines the interface to set the STP port priority, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 1/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 18</strong> spanning-tree vlan vlan-range port-priority priority-value</td>
<td>Assigns the port priority for the VLAN range specified. Enter a port priority value from 0 to 240. Port priority values increment by 16.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# spanning-tree vlan 8-10 port-priority 16</td>
<td></td>
</tr>
<tr>
<td><strong>Step 19</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 20</strong> interface interface-id</td>
<td>Defines the interface to set the STP port priority, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 1/0/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 21</strong> spanning-tree vlan vlan-range port-priority priority-value</td>
<td>Assigns the port priority for the VLAN range specified. Enter a port priority value from 0 to 240. Port priority values increment by 16.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# spanning-tree vlan 3-6 port-priority 16</td>
<td></td>
</tr>
<tr>
<td><strong>Step 22</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 23</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example: Switch# show running-config</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Load Sharing Using STP Path Cost (CLI)

These steps describe how to configure a network with load sharing using STP path costs.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Enters global configuration mode on Switch A.</td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Defines the interface to be configured as a trunk, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 1/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>switchport mode trunk</td>
</tr>
<tr>
<td>Example:</td>
<td>Configures the port as a trunk port.</td>
</tr>
<tr>
<td>Switch(config-if)# switchport mode trunk</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Switch(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>Step 6</td>
<td>Repeat Steps 2 through 4 on a second interface in Switch A.</td>
</tr>
<tr>
<td>Step 7</td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td>Step 8</td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show running-config</td>
</tr>
<tr>
<td>Step 9</td>
<td>show vlan</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show vlan</td>
</tr>
<tr>
<td>Step 10</td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>Step 11</td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# interface gigabitethernet 1/0/1</td>
</tr>
<tr>
<td>Step 12</td>
<td>spanning-tree vlan vlan-range cost cost-value</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# spanning-tree vlan 2-4 cost 30</td>
</tr>
<tr>
<td>Step 13</td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# end</td>
</tr>
<tr>
<td>Step 14</td>
<td>Repeat Steps 9 through 13 on the other configured trunk interface on Switch A, and</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 15**

**exit**

Example:

Switch(config)# exit

Returns to privileged EXEC mode.

**Step 16**

**show running-config**

Example:

Switch# show running-config

Verifies your entries. In the display, verify that the path costs are set correctly for both trunk interfaces.

**Step 17**

**copy running-config startup-config**

Example:

Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.

**Related Topics**

[Network Load Sharing Using STP Path Cost](#), on page 1507

**Where to Go Next**

After configuring VLAN trunks, you can configure the following:

- VLANs
- VLAN groups
- VLAN groups
# Additional References

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>For complete syntax and usage information for the commands used in this chapter.</td>
<td>VLAN Command Reference (Catalyst 3850 Switches) VLAN Command Reference (Cisco WLC 5700 Series) Layer 2/3 Command Reference (Catalyst 3850 Switches) Layer 2 Command Reference (Cisco WLC 5700 Series) Command Reference (Catalyst 9300 Series Switches) Command Reference (Catalyst 9500 Series Switches)</td>
</tr>
</tbody>
</table>

## Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

## Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1573</td>
<td>Evolution of the Interfaces Group of MIB-II</td>
</tr>
<tr>
<td>RFC 1757</td>
<td>Remote Network Monitoring Management</td>
</tr>
<tr>
<td>RFC 2021</td>
<td>SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information for VLAN Trunks

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
PART XV

WLAN

- WLANs, on page 1525
- DHCP for WLANs, on page 1551
- WLAN Security, on page 1561
- Setting Client Count Per WLAN, on page 1573
- 802.11w, on page 1579
- Configuring Wi-Fi Direct Client Policy, on page 1587
- Configuring 802.11r BSS Fast Transition, on page 1593
- Assisted Roaming, on page 1605
- Configuring Access Point Groups, on page 1611
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About WLANs

This feature enables you to control up to 512 WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All switches publish up to 16 WLANs to each connected access point, but you can create up to the maximum number of WLANs supported and then selectively publish these WLANs (using access point groups) to different access points to better manage your wireless network.

You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the switch to access.
Band Selection

Band selection enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of 3 nonoverlapping channels. To prevent these sources of interference and improve overall network performance, configure band selection on the switch.

Related Topics
- Configuring Advanced WLAN Properties (CLI), on page 1540
- Configuring Advanced WLAN Properties (GUI), on page 1543
- Prerequisites for WLANs, on page 1529
- Restrictions for WLANs, on page 1529

Off-Channel Scanning Defer

In deployments with certain power-save clients, you sometimes need to defer the Radio Resource Management's (RRM) normal off-channel scanning to avoid missing critical information from low-volume clients (for example, medical devices that use power-save mode and periodically send telemetry information). This feature improves the way that Quality of Service (QoS) interacts with the RRM scan defer feature.

You can use a client's Wi-Fi Multimedia (WMM) UP marking to configure the access point to defer off-channel scanning for a configurable period of time if it receives a packet marked UP.

Off-Channel Scanning Defer is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off-Channel Scanning Defer is responsible for rogue detection. Devices that need to defer Off-Channel Scanning Defer should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that Off-Channel Defer scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP Off-Channel Scanning Defer, such as monitoring access points, or other access points in the same location that do not have this WLAN assigned.

You can assign a QoS policy (bronze, silver, gold, and platinum) to a WLAN to affect how packets are marked on the downlink connection from the access point regardless of how they were received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. The marking results of each QoS policy are as follows:

- Bronze marks all downlink traffic to UP=1.
- Silver marks all downlink traffic to UP=0.
- Gold marks all downlink traffic to UP=4.
- Platinum marks all downlink traffic to UP=6.

DTIM Period

In the 802.11 networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.
Typically, the DTIM value is set to 1 (to transmit broadcast and multicast frames after every beacon) or 2 (to transmit after every other beacon). For instance, if the beacon period of the 802.11 network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames 5 times per second. Either of these settings are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon) if all 802.11 clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently which results in a longer battery life. For example, if the beacon period is 100 ms and you set the DTIM value to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds. This rate allows the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, which results in a longer battery life.

A beacon period, which is specified in milliseconds on the switch, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. On Cisco’s 802.11n access points, this value is rounded to the nearest multiple of 17 TUs. For example, a configured beacon period of 100 ms results in an actual beacon period of 104 ms.

Many applications cannot tolerate a long time between broadcast and multicast messages, which results in poor protocol and application performance. We recommend that you set a low DTIM value for 802.11 networks that support such clients.

Session Timeouts

You can configure a WLAN with a session timeout. The session timeout is the maximum time for a client session to remain active before requiring reauthorization.

Cisco Client Extensions

The Cisco Client Extensions (CCX) software is licensed to manufacturers and vendors of third-party client devices. The CCX code resident on these clients enables them to communicate wirelessly with Cisco access points and to support Cisco features that other client devices do not, including those features that are related to increased security, enhanced performance, fast roaming, and power management.

- The software supports CCX versions 1 through 5, which enables switches and their access points to communicate wirelessly with third-party client devices that support CCX. CCX support is enabled automatically for every WLAN on the switch and cannot be disabled. However, you can configure Aironet information elements (IEs).

- If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the switch sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the switch and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 1540
Peer-to-Peer Blocking

Peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. Peer-to-Peer enables you to have more control over how traffic is directed. For example, you can choose to have traffic bridged locally within the switch, dropped by the switch, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with the local switching WLAN.

Related Topics
- Configuring Advanced WLAN Properties (CLI), on page 1540
- Configuring Advanced WLAN Properties (GUI), on page 1543
- Prerequisites for WLANs, on page 1529
- Restrictions for WLANs, on page 1529

Diagnostic Channel

You can choose a diagnostic channel to troubleshoot why the client is having communication problems with a WLAN. You can test the client and access points to identify the difficulties that the client is experiencing and allow corrective measures to be taken to make the client operational on the network. You can use the switch GUI or CLI to enable the diagnostic channel, and you can use the switch CLI to run the diagnostic tests.

Note
We recommend that you enable the diagnostic channel feature only for nonanchored SSIDs that use the management interface. CCX Diagnostic feature has been tested only with clients having Cisco ADU card

Per-WLAN Radius Source Support

The switch sources RADIUS traffic from the IP address of its management interface unless the configured RADIUS server exists on a VLAN accessible via one of the switch Dynamic interfaces. If a RADIUS server is reachable via a switch Dynamic interface, RADIUS requests to this specific RADIUS server will be sourced from the controller via the corresponding Dynamic interface.

By default, RADIUS packets sourced from the switch will set the NAS-IP-Address attribute to that of the management interface's IP Address, regardless of the packet's source IP Address (Management or Dynamic, depending on topology).

When you enable per-WLAN RADIUS source support (Radius Server Overwrite interface) the NAS-IP-Address attribute is overwritten by the switch to reflect the sourced interface. Also, RADIUS attributes are modified accordingly to match the identity. This feature virtualizes the switch on the per-WLAN RADIUS traffic, where each WLAN can have a separate layer 3 identity. This feature is useful in deployments that integrate with ACS Network Access Restrictions and Network Access Profiles.
To filter WLANs, use the callStationID that is set by RFC 3580 to be in the APMAC:SSID format. You can also extend the filtering on the authentication server to be on a per-WLAN source interface by using the NAS-IP-Address attribute.

You can combine per-WLAN RADIUS source support with the normal RADIUS traffic source and some WLANs that use the management interface and others using the per-WLAN dynamic interface as the address source.

### Prerequisites for WLANs

- You can associate up to 16 WLANs with each access point group and assign specific access points to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point (AP) does not advertise disabled WLANs in its access point group or WLANs that belong to another group.

- We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that switches properly route VLAN traffic.

### Related Topics

- Creating WLANs (CLI), on page 1532
- Creating WLANs (GUI), on page 1533
- Configuring General WLAN Properties (CLI), on page 1537
- Configuring General WLAN Properties (GUI), on page 1539
- Deleting WLANs (CLI), on page 1534
- Configuring Advanced WLAN Properties (CLI), on page 1540
- Configuring Advanced WLAN Properties (GUI), on page 1543
- Band Selection, on page 1526
- DTIM Period
- Session Timeout
- Cisco Client Extensions, on page 1527
- Peer-to-Peer Blocking, on page 1528
- Diagnostic Channel
- Client Count Per WLAN
- Enabling WLANs (CLI), on page 1536
- Disabling WLANs (CLI), on page 1536

### Restrictions for WLANs

- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are properly configured, the VLAN mapping will become Group-specific.

- Do not enable IEEE 802.1X Fast Transition on Flex Local Authentication enabled WLAN, as client association is not supported with Fast Transition 802.1X key management.

- Peer-to-peer blocking does not apply to multicast traffic.

- You can configure a maximum of up to 12000 clients.
• You can configure a maximum up to of 2000 clients.

• The WLAN name and SSID can have up to 32 characters.

• Special characters are not supported for the WLAN name.

• WLAN name cannot be a keyword; for example, if you try to create a WLAN with the name as 's' by entering the `wlan s` command, it results in shutting down all WLANs because 's' is used as a keyword for shutdown.

• You cannot map a WLAN to VLAN0, and you cannot map VLANs 1002 to 1006.

• Dual stack clients with a static-IPv4 address is not supported.

• When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.

• When multiple WLANs with the same SSID get assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between them.

• When AAA override is enabled on WLAN with flex local switching, the client must receive the IPv6 address from the VLAN returned by the AAA server. This implies that if a WLAN with both local switching and AAA override enabled is mapped to VLAN X and the AAA server returns a VLAN Y; then, the client must receive an address from VLAN Y. However, this is not supported in this controller release.

• When WLAN is local switching, associate the client to local-switching WLAN where AVC is enabled. Send some traffic from client, when you check the AVC stats after 90 sec. Cisco WLC shows stats under top-apps but does not show under client. There is timer issue so for the first slot Cisco WLC might not show stats for the clients. Earlier, only 1 sec stats for a client is seen if the timers at AP and at WLC are off by 89 seconds. Now, clearing of the stats is after 180 seconds so stats from 91 seconds to 179 seconds for a client is seen. This is done because two copies of the stats per client cannot be kept due to memory constraint in Cisco 5508 WLC.

• RADIUS Server Overwrite interface per wlan feature is not supported. However, you can achieve the same using the following configuration:
  • Configure a RADIUS Authentication Server
  • Configure a RADIUS Authentication Server Group
  • Create 802.1x WLAN
  • Configure Wireless Profile Policy and Attach it to the VLAN

**Configure a RADIUS Authentication Server**

• Device (config)# radius server server-name

• Device (config-radius-server)# address ipv4 address auth-port auth_port_number acct-port acct_port_number

• Device (config-radius-server)# key key

**Configure a RADIUS Authentication Server Group**

• Device(config)# aaa group server radius server-name

• Device(config)# server name server-name
• Device(config)# ip radius source-interface vlan vlan-name
• Device(config)# aaa authentication dot1x dot1x_name group server-name

Create 802.1x WLAN
• Device(config)# wlan wlan-name id ssid
• Device(config-wlan)# security dot1x authentication-list list-name
• Device(config-wlan)# no shutdown

Configure Wireless Profile Policy and Attach it to VLAN
• Device(config)# wireless profile policy profile-name
• Device(config-wireless-policy)# vlan vlan-name
• Device(config-wireless-policy)# no shutdown

A sample configuration on the Cisco Wireless Controller is given below:

radius server RAD_EXT_3
    address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
    key cisco

aaa group server radius AAA_EXT_3
    server name RAD_EXT_3
    ip radius source-interface vlan 50
    aaa authentication dot1x test_ext group AAA_EXT_3

wlan test_wpa2_dot1x 2 test_wpa2_dot1x
    security dot1x authentication-list test_ext
    no shutdown

wireless profile policy pp-1
    vlan 50
    no shutdown

radius server RAD_EXT_3
    address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
    key cisco

aaa group server radius AAA_EXT_2
    server name RAD_EXT_3
    ip radius source-interface vlan 51
    aaa authentication dot1x test_ext_2 group AAA_EXT_2

wlan test_wpa2 3 test_wpa3
    security dot1x authentication-list test_ext_2
    no shutdown
wireless profile policy pp-1
vlan 51
no shutdown

Caution
Some clients might not be able to connect to WLANs properly if they detect the same SSID with multiple security policies. Use this feature with care.

Related Topics
Creating WLANs (CLI), on page 1532
Creating WLANs (GUI), on page 1533
Configuring General WLAN Properties (CLI), on page 1537
Configuring General WLAN Properties (GUI), on page 1539
Deleting WLANs (CLI), on page 1534
Configuring Advanced WLAN Properties (CLI), on page 1540
Configuring Advanced WLAN Properties (GUI), on page 1543
Band Selection, on page 1526
DTIM Period
Session Timeout
Cisco Client Extensions, on page 1527
Peer-to-Peer Blocking, on page 1528
Diagnostic Channel
Client Count Per WLAN
Enabling WLANs (CLI), on page 1536
Disabling WLANs (CLI), on page 1536

How to Configure WLANs

Creating WLANs (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>wlan profile-name wlan-id [ssid]</td>
<td>Specifies the WLAN name and ID:</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# wlan mywlan 34</td>
<td>For the profile-name, enter the profile name. The range is from 1 to 32</td>
</tr>
<tr>
<td>mywlan-ssid</td>
<td>alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>For the wlan-id, enter the WLAN ID. The range is from 1 to 512.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For the <code>ssid</code>, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**: By default, the WLAN is disabled.

### Step 3

**Example:**

```
Switch(config)# end
```

Returns to privileged EXEC mode. Alternatively, you can also press `Ctrl-Z` to exit global configuration mode.

### Related Topics

- Prerequisites for WLANs, on page 1529
- Restrictions for WLANs, on page 1529

---

## Creating WLANs (GUI)

### Procedure

#### Step 1

Click **Configuration > Wireless**.

The **WLANs** page is displayed.

#### Step 2

Click **New** to create a WLAN.

The **WLANs > Create New** page is displayed.

#### Step 3

Enter the following parameters:

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN ID</td>
<td>WLAN identifier. The value ranges from 1 to 512.</td>
</tr>
<tr>
<td>SSID</td>
<td>Broadcast name of the WLAN.</td>
</tr>
<tr>
<td>Profile</td>
<td>WLAN profile name.</td>
</tr>
</tbody>
</table>

#### Step 4

Click **Apply**.

### Related Topics

- Prerequisites for WLANs, on page 1529
- Restrictions for WLANs, on page 1529
Deleting WLANs (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>no wlan wlan-name wlan-id ssid</code></td>
<td>Deletes the WLAN. The arguments are as follows:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>no wlan test2</code></td>
<td>• The <code>wlan-name</code> is the WLAN profile name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <code>wlan-id</code> is the WLAN ID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <code>ssid</code> is the WLAN SSID name configured for the WLAN.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you delete a WLAN that is part of an AP group, the WLAN is removed from the AP group and from the AP's radio.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Prerequisites for WLANs, on page 1529
- Restrictions for WLANs, on page 1529

Deleting WLANs (GUI)

### Procedure

- **Step 1** Click **Configuration > Wireless**. The **WLANs** page is displayed.

- **Step 2** Select the checkbox corresponding to the WLAN you want to delete.

  **Note** If you delete a WLAN that is part of an AP group, the WLAN is removed from the AP group and from the AP's radio.
Step 3  Click Remove.

Searching WLANs (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 show wlan summary</td>
<td>Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.</td>
</tr>
</tbody>
</table>

Example

Switch# show wlan summary
Number of WLANs: 4

<table>
<thead>
<tr>
<th>WLAN Profile Name</th>
<th>SSID</th>
<th>VLAN Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 test1</td>
<td>test1-ssid</td>
<td>137 UP</td>
</tr>
<tr>
<td>3 test2</td>
<td>test2-ssid</td>
<td>136 UP</td>
</tr>
<tr>
<td>2 test3</td>
<td>test3-ssid</td>
<td>1 UP</td>
</tr>
<tr>
<td>45 test4</td>
<td>test4-ssid</td>
<td>1 DOWN</td>
</tr>
</tbody>
</table>

You can also use wild cards to search WLANs. For example show wlan summary include | variable. Where variable is any search string in the output.

Switch# show wlan summary | include test-wlan-ssid
1 test-wlan | test-wlan-ssid | 137 UP |

Searching WLANs (GUI)

Procedure

Step 1 Click Configuration > Wireless.
The WLANs page is displayed.

Step 2 Type the first few characters in the text box above the column you are searching. For example, to search the WLAN based on the Profile, type the first few characters of the profile name.

You can search a WLAN based on the following criteria:

- Profile
- ID
- SSID
- VLAN
If a WLAN exists, it would appear based on the accuracy of the match.

---

### Enabling WLANs (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  * configure terminal  
  * Example: Switch# configure terminal | Enters global configuration mode. |
| **Step 2**
  * wlan profile-name  
  * Example: Switch# wlan test4 | Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN. |
| **Step 3**
  * no shutdown  
  * Example: Switch(config-wlan)# no shutdown | Enables the WLAN. |
| **Step 4**
  * end  
  * Example: Switch(config)# end | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode. |

**Related Topics**
- Prerequisites for WLANs, on page 1529
- Restrictions for WLANs, on page 1529

---

### Disabling WLANs (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  * configure terminal  
  * Example: Switch# configure terminal | Enters global configuration mode. |
| **Step 2**
  * wlan profile-name  
  * Example: Switch# wlan test4 | Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN. |
### Purpose

Command or Action | Purpose
--- | ---
**Step 3** shutdown  
*Example:*  
Switch(config-wlan)# shutdown | Disables the WLAN.

**Step 4** end  
*Example:*  
Switch(config)# end | Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

**Step 5** show wlan summary  
*Example:*  
Switch# show wlan summary | Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.

### Related Topics

- [Prerequisites for WLANs](#)
- [Restrictions for WLANs](#)

### Configuring General WLAN Properties (CLI)

You can configure the following properties:

- Media stream
- Broadcast SSID
- Call Snooping
- Radio
- Interface
- Status

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** configure terminal  
*Example:*  
Switch# configure terminal | Enters global configuration mode. |
| **Step 2** wlan *profile-name*  
*Example:*  
Switch# wlan test4 | Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN. |
| **Step 3** shutdown  
*Example:*  
Switch# shutdown | Disables the WLAN before configuring the parameters. |
<table>
<thead>
<tr>
<th><strong>Step</strong></th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td><code>broadcast-ssid</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; <code>Switch (config-wlan)# broadcast-ssid</code></td>
<td>Broadcasts the SSID for this WLAN. This field is enabled by default.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>`radio {all</td>
<td>dot11a</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>client vlan vlan-identifier</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; <code>Switch# client vlan test-vlan</code></td>
<td>Enables an interface group on the WLAN.  &lt;br&gt; <code>vlan-identifier</code>—Specifies the VLAN identifier. This can be the VLAN name, VLAN ID, or VLAN group name.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>ip multicast vlan vlan-name</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; <code>Switch(config-wlan)# ip multicast vlan test</code></td>
<td>Enables IP multicast on a WLAN. The keywords are as follows:  &lt;br&gt; - <code>vlan</code>—Specifies the VLAN ID.  &lt;br&gt; - <code>vlan-name</code>—Specifies the VLAN name.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>media-stream multicast-direct</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; <code>Switch(config-wlan)# media-stream multicast-direct</code></td>
<td>Enables multicast VLANs on this WLAN.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>call-snoop</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; <code>Switch(config-wlan)# call-snoop</code></td>
<td>Enables call-snooping support.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>no shutdown</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; <code>Switch(config-wlan)# no shutdown</code></td>
<td>Enables the WLAN.</td>
</tr>
</tbody>
</table>
### Configuring General WLAN Properties (GUI)

Use this procedure to perform the following actions on a WLAN:

- Set WLAN Status
- Configure Radio Policies
- Assign Interface/Interface Groups
- Enable or Disable Multicast VLAN Feature
- Enable or Disable Broadcast SSID Feature

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Click <strong>Configuration &gt; Wireless</strong>.</td>
</tr>
<tr>
<td></td>
<td>The <strong>WLANs</strong> page is displayed.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Locate the WLAN you want to configure by using the search mechanisms on the page.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click on the <strong>WLAN Profile</strong> of the WLAN.</td>
</tr>
<tr>
<td></td>
<td>The <strong>WLAN &gt; Edit</strong> page is displayed.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the <strong>General</strong> tab. This tab is displayed by default.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure the <strong>General</strong> parameters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Displays the configured profile name of the WLAN.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the configured LAN type.</td>
</tr>
<tr>
<td>SSID</td>
<td>Displays the configured SSID of the WLAN.</td>
</tr>
<tr>
<td>Status</td>
<td>Check box to enable the WLAN. The default value is enabled.</td>
</tr>
</tbody>
</table>
### Parameter | Description
---|---
Radio Policy | WLAN radio policy to enable radios on the WLAN. Values are the following:
  - All
  - 802.11a only
  - 802.11g only
  - 802.11a/g only
  - 802.11b/g only

Interface/Interface Group | Interface or interface group that you want this WLAN to be mapped. Displays the non-service port and non-virtual interface names configured on the Interfaces page.
**Note** | This field displays a drop down box only when the VLAN for a WLAN is mapped using a existing VLAN name on the switch.

Broadcast SSID | Check box to broadcast this SSID. The default is enabled.

Multicast VLAN Feature | Check box to enable the multicast VLAN. The default is disabled.
**Note** | The Multicast Interface field appears only after you enable the Multicast VLAN feature text box.
**Note** | You have to configure the multicast VLAN feature only once if you want to use the multicast feature.

### Step 6
Click **Apply**.

### What to do next
Proceed to configure the Security, QoS, and Advanced Properties.

### Related Topics
- Prerequisites for WLANs, on page 1529
- Restrictions for WLANs, on page 1529

### Configuring Advanced WLAN Properties (CLI)

You can configure the following advanced properties:

- AAA Override
- Coverage Hole Detection
- Session Timeout
- Cisco Client Extensions
- Diagnostic Channels
- Interface Override ACLs
• P2P Blocking
• Client Exclusion
• Maximum Clients Per WLAN
• Off Channel Scan Defer

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wlan profile-name</code></td>
<td>Enters WLAN configuration submode. The <code>profile-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Switch# wlan test4</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>aaa-override</code></td>
<td>Enables AAA override.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Switch(config-wlan)# aaa-override</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>chd</code></td>
<td>Enables coverage hole detection for this WLAN. This field is enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Switch(config-wlan)# chd</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>session-timeout time-in-seconds</code></td>
<td>Sets the session timeout in seconds. The range and default values vary according to the security configuration. If the WLAN security is configured to dot1x, the range is 300 to 86400 seconds and the default value is 1800 seconds. For all other WLAN security configurations, the range is 1 to 65535 seconds and the default value is 0 seconds. A value of 0 indicates no session timeout.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Switch(config-wlan)# session-timeout 450</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>ccx aironet-iesupport</code></td>
<td>Enables support for Aironet IEs for this WLAN. This field is enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Switch(config-wlan)# ccx aironet-iesupport</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>diag-channel</code></td>
<td>Enables diagnostic channel support to troubleshoot client communication issues on a WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Switch(config-wlan)# diag-channel</code></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>ip access-group [web] acl-name</code></td>
<td>Configures the WLAN ACL group. The variable <code>acl-name</code> specifies the user-defined</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# ip access-group test-acl-name</td>
<td>IPv4 ACL name. The keyword web specifies the IPv4 web ACL.</td>
</tr>
</tbody>
</table>

**Step 9**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| peer-blocking [drop | Configures peer to peer blocking parameters. The keywords are as follows:
| forward-upstream] | • drop—Enables peer-to-peer blocking on the drop action.
| Example: | • forward-upstream—Enables peer-to-peer blocking on the forward upstream action. |

**Example:**

Switch(config)# peer-blocking drop

### Step 10

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclusionlist time-in-seconds</td>
<td>Specifies the timeout in seconds. The valid range is from 0 to 2147483647. Enter 0 for no timeout. A zero (0) timeout indicates that the client is permanently added to the exclusion list.</td>
</tr>
</tbody>
</table>

**Example:**

Switch(config)# exclusionlist 10

### Step 11

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>client association limit max-number-of-clients</td>
<td>Sets the maximum number of clients that can be configured on a WLAN.</td>
</tr>
</tbody>
</table>

**Example:**

Switch(config)# client association limit 200

### Step 12

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| channel-scan defer-priority {defer-priority {0-7} | Sets the channel scan defer priority and defer time. The arguments are as follows:
| defer-time {0 - 6000}} | • defer-priority—Specifies the priority markings for packets that can defer off-channel scanning. The range is from 0 to 7. The default is 3.
| Example: | • defer-time—Deferral time in milliseconds. The range is from 0 to 6000. The default is 100. |

Switch(config)# channel-scan defer-priority 6

### Step 13

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

Switch(config)# end

### Related Topics

- Band Selection, on page 1526
- DTIM Period
- Session Timeout
- Cisco Client Extensions, on page 1527
- Peer-to-Peer Blocking, on page 1528
- Diagnostic Channel
- Client Count Per WLAN
- Prerequisites for WLANs, on page 1529
Configuring Advanced WLAN Properties (GUI)

**Procedure**

**Step 1** Click Configuration > Wireless.
The WLANs page is displayed.

**Step 2** Locate the WLAN you want to configure by using the search mechanisms on the page.

**Step 3** Click on the WLAN Profile of the WLAN.
The WLAN > Edit page is displayed.

**Step 4** Click on the Advanced Properties tab.

**Step 5** Configure the Advanced properties.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow AAA Override</td>
<td>AAA override for global WLAN parameters that you can enable or disable. When AAA Override is enabled, and a client has conflicting AAA and switches WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco WLAN Solution WLAN VLAN to a VLAN returned by the AAA server and predefined in the switches interface configuration. In all cases, the operating system also uses QoS, DSCP, 802.1p priority tag values, and ACLs provided by the AAA server, if they are predefined in the switches interface configuration. (This VLAN switching by AAA Override is also referred to as Identity Networking.) If the Corporate WLAN primarily uses a Management Interface assigned to VLAN 2, and if AAA Override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned. When AAA Override is disabled, all client authentication defaults to the switches authentication parameter settings, and authentication is performed only by the AAA server if the switches WLAN does not contain any client-specific authentication parameters. The AAA override values might come from a RADIUS server, for example.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Coverage Hole Detection</td>
<td>Coverage hole detection (CHD) on this WLAN that you can enable or disable. By default, CHD is enabled on all WLANs on the switches. You can disable CHD on a WLAN. When you disable CHD on a WLAN, a coverage hole alert is still sent to the Switch, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where guests are connected to your network for short periods of time and are likely to be highly mobile.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Configure a WLAN with a session timeout in seconds. The session timeout is the maximum time for a client session to remain active before requiring reauthorization. The minimum session timeout allowed is 1 second and the maximum timeout allowed is 65535 seconds. Enter zero denotes the session will never expire.</td>
</tr>
<tr>
<td>Aironet IE</td>
<td>Support of Aironet IEs per WLAN that you can enable or disable. The default is disabled.</td>
</tr>
<tr>
<td>Diagnostic Channel</td>
<td>Diagnostic channel support on the WLAN that you can enable or disable. The default is disabled.</td>
</tr>
<tr>
<td>P2P Blocking Action</td>
<td>Peer-to-peer blocking settings that you can choose from the following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—(Default) Disables peer-to-peer blocking and bridges traffic locally within the switch whenever possible.</td>
</tr>
<tr>
<td></td>
<td>• Drop—Causes the switches to discard the packets.</td>
</tr>
<tr>
<td></td>
<td>• Forward-UpStream—Causes the packets to be forwarded on the upstream VLAN. The device above the switches decides what action to take regarding the packets.</td>
</tr>
<tr>
<td>Client Exclusion</td>
<td>Timeout in seconds for disabled client machines that you can enable or disable. Client machines are disabled by their MAC address and their status can be observed on the Clients &gt; Details page. A timeout setting of 0 indicates that the client is disabled permanently. Administrative control is required to reenable the client. The default is enabled and the timeout setting is configured as 60 seconds.</td>
</tr>
<tr>
<td>Timeout Value (secs)</td>
<td>The minimum timeout value allowed is 0 seconds and the maximum timeout value allowed is 2147483647 seconds.</td>
</tr>
<tr>
<td>Max Allowed Client</td>
<td>Maximum clients allowed per Switch.</td>
</tr>
<tr>
<td></td>
<td>You can set a limit to the number of clients that can connect to a WLAN. This feature is useful in scenarios where you have a limited number of clients that can connect to a Switch. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure per WLAN depends on the platform that you are using. A maximum of up to 12000 clients are supported.</td>
</tr>
<tr>
<td></td>
<td>Note: The maximum number of clients per WLAN feature is supported only for access points that are in connected mode.</td>
</tr>
<tr>
<td>DHCP</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>DHCP Server IP Address</strong></td>
<td>Enter the DHCP server on the WLAN that overrides the DHCP server address on the interface assigned to the WLAN.</td>
</tr>
<tr>
<td><strong>DHCP Address Assignment Required</strong></td>
<td>Enables the DHCP address assignment and makes it mandatory for clients to get their IP address from the DHCP server.</td>
</tr>
<tr>
<td><strong>DHCP Option 82</strong></td>
<td>Enables the DHCP82 payload on the WLAN.</td>
</tr>
</tbody>
</table>
| **DHCP option 82 Format** | Specifies the DHCP option 82 format. Values are as follows:  
  - add-ssid—Set RemoteID format that is the AP radio MAC address and SSID.  
  - ap-ethmac—Set RemoteID format that is the AP Ethernet MAC address.  
  **Note** If the format option is not configured, only the AP radio MAC address is used. |
| **DHCP Option ASCII Mode** | Configures ASCII for DHCP Option 82. If this is not configured, the option 82 format is set to ASCII format. |
| **DHCP Option 82 RID Mode** | Adds the Cisco 2 Byte RID for DHCP option 82. |
| **NAC** | Enables the NAC on the WLAN. |

### Off Channel Scanning Defer

| Scan Differ Priority | Defer priority for the channel scan that you can assign by clicking on the priority argument. The valid range for the priority is 0 to 7. The priority is 0 to 7 (this value should be set to 6 on the client and on the WLAN).  
  Multiple values can be set. The default values are 4, 5 and 6. |
| Scan Differ Time | Channel scan defer time in milliseconds that you can assign. The valid range is 100 (default) to 60000 (60 seconds). This setting should match the requirements of the equipment on your wireless LAN. |

### Override Interface ACL

| IPv4 ACL | The WLANs IPv4 ACL group. Values are as follows:  
  - Un-configured  
  - Pre-auth_ipv4_acl |
| IPv6 ACL | The WLANs IPv6 ACL group. Values are as follows:  
  - Un-configured  
  - Pre-auth_ipv6_acl |

---

**Step 6** Click **Apply**.

**Related Topics**  
[Band Selection](#), on page 1526
Applying a QoS Policy on a WLAN (GUI)

Procedure

Step 1 Choose **Configuration > Wireless**.

Step 2 Expand the **WLAN** node by clicking on the left pane and choose **WLANs**. The **WLANs page** is displayed.

Step 3 Select the WLAN for which you want to configure the QoS policies by clicking on the WLAN **Profile**.

Step 4 Click the QoS tab to configure the QoS policies on the WLAN.

You can also configure precious metal policies for the WLAN.

The following options are available:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>QoS SSID Policy</strong></td>
<td></td>
</tr>
<tr>
<td>Egress Policy</td>
<td>QoS downstream policy configuration. The <strong>Existing Policy</strong> column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the <strong>Assign Policy</strong> column. If a policy is not selected, NONE is displayed.</td>
</tr>
<tr>
<td>Ingress Policy</td>
<td>QoS upstream policy configuration. The <strong>Existing Policy</strong> column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the <strong>Assign Policy</strong> column. If a policy is not selected, NONE is displayed.</td>
</tr>
<tr>
<td><strong>QoS Client Policy</strong></td>
<td></td>
</tr>
<tr>
<td>Egress Policy</td>
<td>QoS downstream policy configuration. The <strong>Existing Policy</strong> column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the <strong>Assign Policy</strong> column. If a policy is not selected, NONE is displayed.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Policy</td>
<td>QoS upstream policy configuration.</td>
</tr>
<tr>
<td></td>
<td>The Existing Policy column displays the current applied policy. To change</td>
</tr>
<tr>
<td></td>
<td>the existing policy, select the policy from the drop-down list in the Assign</td>
</tr>
<tr>
<td></td>
<td>Policy column. If a policy is not selected, NONE is displayed.</td>
</tr>
</tbody>
</table>

### WMM

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WMM Policy</td>
<td>WMM Policy. This parameter has the following values:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—Disables this WMM policy.</td>
</tr>
<tr>
<td></td>
<td>• Allowed—Allows the clients to communicate with the WLAN.</td>
</tr>
<tr>
<td></td>
<td>• Require—Ensures that it is mandatory for the clients to have WMM features</td>
</tr>
<tr>
<td></td>
<td>enabled on them to communicate with the WLAN.</td>
</tr>
</tbody>
</table>

### Step 5

Click **Apply**.

### Related Topics

- Port Policies, on page 596
- Port Policy Format, on page 596
- Restrictions for QoS on Wireless Targets, on page 632
- Supported QoS Features on Wireless Targets, on page 594
- Examples: Wireless QoS Policy Classified by Voice, Video, and Multicast Traffic, on page 696
- SSID Policies, on page 598
- Examples: SSID Policy
- Examples: Configuring Downstream SSID Policy, on page 697
- Client Policies, on page 599
- Examples: Client Policies, on page 699

### Monitoring WLAN Properties (CLI)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wlan id wlan-id</td>
<td>Displays WLAN properties based on the WLAN ID.</td>
</tr>
<tr>
<td>show wlan name wlan-name</td>
<td>Displays WLAN properties based on the WLAN name.</td>
</tr>
<tr>
<td>show wlan all</td>
<td>Displays WLAN properties of all configured WLANs.</td>
</tr>
</tbody>
</table>
### Viewing WLAN Properties (GUI)

**Before you begin**
- You must have administrator privileges.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select <strong>Configuration &gt; WLAN</strong>&lt;br&gt;The WLANs page is displayed.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the <strong>WLAN Profile</strong> link.&lt;br&gt;The <strong>WLANs &gt; Edit</strong> page is displayed. The WLANs page contains the following tabs:&lt;br&gt;  - <strong>General</strong>: Displays the WLAN general properties.&lt;br&gt;  - <strong>Security</strong>: Displays the security properties. The properties include Layer 2, Layer 3, and AAA properties.&lt;br&gt;  - <strong>QoS</strong>: Displays the QoS configuration properties.&lt;br&gt;  - <strong>Advanced</strong>: Displays the advanced properties.</td>
</tr>
</tbody>
</table>

**Where to Go Next**
Proceed to configure DHCP for WLANs.

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wlan summary</code></td>
<td>Displays a summary of all WLANs. The summary details includes the following information:&lt;br&gt;  - WLAN ID&lt;br&gt;  - Profile name&lt;br&gt;  - SSID&lt;br&gt;  - VLAN&lt;br&gt;  - Status</td>
</tr>
<tr>
<td><code>show running-config wlan wlan-name</code></td>
<td>Displays the running configuration of a WLAN based on the WLAN name.</td>
</tr>
<tr>
<td><code>show running-config wlan</code></td>
<td>Displays the running configuration of all WLANs.</td>
</tr>
</tbody>
</table>
# Additional References

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN command reference</td>
<td><em>WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em></td>
</tr>
<tr>
<td>Mobility Anchor configuration</td>
<td><em>Mobility Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em></td>
</tr>
<tr>
<td>WebAuth Configuration</td>
<td><em>Security Configuration Guide (Catalyst 3850 Switches)</em></td>
</tr>
</tbody>
</table>

## Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
Feature Information for WLANs

This table lists the features in this module and provides links to specific configuration information:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN Functionality</td>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 85

DHCP for WLANs

- Finding Feature Information, on page 1551
- Information About the Dynamic Host Configuration Protocol, on page 1551
- Prerequisites for Configuring DHCP for WLANs, on page 1554
- Restrictions for Configuring DHCP for WLANs, on page 1555
- How to Configure DHCP for WLANs, on page 1555
- Additional References, on page 1558
- Feature Information for DHCP for WLANs, on page 1559

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About the Dynamic Host Configuration Protocol

You can configure WLANs to use the same or different Dynamic Host Configuration Protocol (DHCP) servers or no DHCP server. Two types of DHCP servers are available: internal and external.

Internal DHCP Servers

The switches contain an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server. The wireless network generally contains a maximum of 10 access points or fewer, with the access points on the same IP subnet as the switch. The internal server provides DHCP addresses to wireless clients, direct-connect access points, and DHCP requests that are relayed from access points. Only lightweight access points are supported. When you want to use the internal DHCP server, you must set the management interface IP address of the switch as the DHCP server IP address.
DHCP option 43 is not supported on the internal server. Therefore, the access point must use an alternative method to locate the management interface IP address of the switch, such as local subnet broadcast, Domain Name System (DNS), or priming.

An internal DHCP server pool only serves the wireless clients of that switch, not clients of other switches. Also, an internal DHCP server can serve only wireless clients, not wired clients.

When clients use the internal DHCP server of the switch, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned with the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one. Wired guest clients are always on a Layer 2 network connected to a local or foreign switch.

---

**Note**

- VRF is not supported for the internal DHCP server.
- DHCPv6 is not supported in the internal DHCP servers.

---

**General Guidelines**

### External DHCP Servers

The operating system is designed to appear as a DHCP Relay to the network and as a DHCP server to clients with industry-standard external DHCP servers that support DHCP Relay, which means that each switch appears as a DHCP Relay agent to the DHCP server and as a DHCP server at the virtual IP address to wireless clients.

Because the switch captures the client IP address that is obtained from a DHCP server, it maintains the same IP address for that client during intra switch, inter switch, and inter-subnet client roaming.

---

**Note**

External DHCP servers can support DHCPv6.

---

### DHCP Assignments

You can configure DHCP on a per-interface or per-WLAN basis. We recommend that you use the primary DHCP server address that is assigned to a particular interface.

You can assign DHCP servers for individual interfaces. You can configure the management interface, AP-manager interface, and dynamic interface for a primary and secondary DHCP server, and you can configure the service-port interface to enable or disable DHCP servers. You can also define a DHCP server on a WLAN. In this case, the server overrides the DHCP server address on the interface assigned to the WLAN.

### Security Considerations

For enhanced security, we recommend that you require all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, you can configure all WLANs with a DHCP Addr. Assignment Required setting, which disallows client static IP addresses. If DHCP Addr. Assignment Required is selected, clients must obtain an IP address via DHCP. Any client with a static IP address is not allowed on the network. The switch monitors DHCP traffic because it acts as a DHCP proxy for the clients.
• WLANs that support management over wireless must allow management (device-servicing) clients to obtain an IP address from a DHCP server.

If slightly less security is tolerable, you can create WLANs with DHCP Addr. Assignment Required disabled. Clients then have the option of using a static IP address or obtaining an IP address from a designated DHCP server.

Note

DHCP Addr. Assignment Required is not supported for wired guest LANs.

You can create separate WLANs with DHCP Addr. Assignment Required configured as disabled. This is applicable only if DHCP proxy is enabled for the switch. You must not define the primary/secondary configuration DHCP server you should disable the DHCP proxy. These WLANs drop all DHCP requests and force clients to use a static IP address. These WLANs do not support management over wireless connections.

Information About DHCP Option 82

DHCP option 82 provides additional security when DHCP is used to allocate network addresses. It enables the switch to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. You can configure the switch to add option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.

Figure 76: DHCP Option 82

The access point forwards all DHCP requests from a client to the switch. The switch adds the DHCP option 82 payload and forwards the request to the DHCP server. The payload can contain the MAC address or the MAC address and SSID of the access point, depending on how you configure this option.

Note

Any DHCP packets that already include a relay agent option are dropped at the switch.

For DHCP option 82 to operate correctly, DHCP proxy must be enabled.
Configuring DHCP Scopes

Information About Internal DHCP Server

Switches have built-in DHCP relay agents. However, when you desire network segments that do not have a separate DHCP server, the switches can have built-in internal DHCP server that assign IP addresses and subnet masks to wireless clients. Typically, one switch can have one or more internal DHCP server that each provide a range of IP addresses.

Internal DHCP server are needed for internal DHCP to work. Once DHCP is defined on the switch, you can then point the primary DHCP server IP address on the management, AP-manager, and dynamic interfaces to the switch’s management interface.

Note

The controller has the ability to provide internal DHCP server. This feature is very limited and considered as convenience that is often used simple demonstration or proof-of-concept, for example in a lab environment. The best practice is NOT to use this feature in an enterprise production network.


Prerequisites for Configuring DHCP for WLANs

- To be able to use the DHCP option 82, you must configure DHCP on Cisco IOS software. By default, DHCP option 82 is enabled for all clients. You can control the wireless client behavior using the WLAN suboptions.

- The Cisco converged access platforms support internal DHCP server functionality. However, as a general deployment guideline to build large enterprise-class networks, we recommend that you use external DHCP server to provide dynamic IP addressing to wireless clients. Such distributed function reduces processing and configuration load on network devices and allows them to operate efficiently in large scale deployments.

- DHCP Snooping Configuration—DHCP snooping configuration is the required best practices configuration on switch for rapid client join function. DHCP snooping needs to be enabled on each client VLAN including the override VLAN if override is applied on the WLAN.

Example of DHCP snooping configuration

1. Global DHCP snooping configuration:

   1. `Switch(config)#ip dhcp snooping`
   
   `Switch(config)#ip dhcp snooping vlan 100`

   2. `Enable bootp-broadcast` command. This is required for clients that send DHCP messages with broadcast addresses and broadcast bit is set in the DHCP message:

   `Switch(config)#ip dhcp snooping wireless bootp-broadcast enable`

   3. To not append DHCP Option information, enter this command:

   `Switch(config)#no ip dhcp snooping information option`
2. On the interface:

Note: IP DHCP snooping trust is required on Port-Channel interface in addition to member link of the Port-Channel interface.

```
Switch(config)#interface range TenGigabitEthernet 1/0/1 – 2
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 100
Switch(config-if)#ip dhcp snooping trust

Switch(config)#interface port-channel 1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 100
Switch(config-if)#ip dhcp snooping trust
```

Note: DHCP snooping must be configured on the Guest Anchor switch for guest access similar to the Config above.

**Restrictions for Configuring DHCP for WLANs**

- If you override the DHCP server in a WLAN, you must ensure that you configure the underlying Cisco IOS configuration to make sure that the DHCP server is reachable.

- WLAN DHCP override works only if DHCP service is enabled on the switch.

You can configure DHCP service in the following ways:

- Configuring the DHCP pool on the switch.

- Configuring a DHCP relay agent on the SVI. Note: the VLAN of the SVI must be mapped to the WLAN where DHCP override is configured.

**How to Configure DHCP for WLANs**

**Configuring DHCP for WLANs (CLI)**

Use this procedure to configure the following DHCP parameters on a WLAN:

- DHCP Option 82 Payload
• DHCP Required
• DHCP Override

Before you begin
• You must have admin privileges for configuring the WLAN.
• To configure the DHCP override, you must have the IP address of the DHCP server.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>shutdown</td>
<td>Shut down the WLAN.</td>
</tr>
<tr>
<td>Example: Switch(config)# shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>wlan profile-name</td>
<td>Enters WLAN configuration submode. The</td>
</tr>
<tr>
<td>Example: Switch# wlan test4</td>
<td>profile-name is the profile name of the</td>
</tr>
<tr>
<td></td>
<td>configured WLAN.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>ip dhcp opt82 {ascii</td>
<td>format {add-ssid</td>
</tr>
<tr>
<td>Example: Switch(config)# ip dhcp opt82 format</td>
<td>The keyword and arguments are as follows:</td>
</tr>
<tr>
<td>add-ssid</td>
<td>• ascii—Configures ASCII for DHCP</td>
</tr>
<tr>
<td></td>
<td>Option 82. If this is not configured, the</td>
</tr>
<tr>
<td></td>
<td>option 82 format is set to ASCII format.</td>
</tr>
<tr>
<td></td>
<td>• format—Specifies the DHCP option 82</td>
</tr>
<tr>
<td></td>
<td>format. The following options are available:</td>
</tr>
<tr>
<td></td>
<td>• add-ssid—Set RemoteID format that</td>
</tr>
<tr>
<td></td>
<td>is the AP radio MAC address and SSID.</td>
</tr>
<tr>
<td></td>
<td>• ap-ethmac—Set RemoteID format that is the</td>
</tr>
<tr>
<td></td>
<td>AP Ethernet MAC address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the format option is not</td>
</tr>
<tr>
<td></td>
<td>configured, only the AP radio MAC address</td>
</tr>
<tr>
<td></td>
<td>is used.</td>
</tr>
<tr>
<td></td>
<td>• rid—Adds the Cisco 2 byte RID for DHCP</td>
</tr>
<tr>
<td></td>
<td>option 82.</td>
</tr>
</tbody>
</table>

### Command or Action | Purpose
--- | ---
**Step 5** | ip dhcp required
Example: Switch(config-wlan)# ip dhcp required
Makes it mandatory for clients to get their IP address from the DHCP server. Static clients are not allowed.

**Step 6** | ip dhcp server *ip-address*
Example: Switch(config-wlan)# ip dhcp server 200.1.1.2
Defines a DHCP server on the WLAN that overrides the DHCP server address on the interface assigned to the WLAN.

**Step 7** | no shutdown
Example: Switch(config-wlan)# no shutdown
Restarts the WLAN.

**Step 8** | end
Example: Switch(config)# end
Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

**Step 9** | show wlan *wlan-name*
Example: Switch(config-wlan)# show wlan test-wlan
Verifies the DHCP configuration.

### Configuring DHCP Scopes (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | configure terminal
Example: Switch# configure terminal
Enters global configuration mode. |
| **Step 2** | ip dhcp pool *pool-name*
Example: Switch(config)# ip dhcp pool test-pool
Configures the DHCP pool address. |
| **Step 3** | network *network-name* mask-address
Example: Switch(dhcp-config)#network 209.165.200.224 255.255.255.0
Specifies the network number in dotted-decimal notation and the mask address. |
| **Step 4** | dns-server *hostname*
Example: Switch(dhcp-config)#dns-server example.com
Specifies the DNS name server. You can specify an IP address or a hostname. |
### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Management</td>
<td>System Management Configuration Guide (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>System Management Configuration Guide (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

#### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/ErrorDecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/ErrorDecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://cisco.com/go/mibs">http://cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
### Feature Information for DHCP for WLANs

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP functionality for WLAN</td>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
Feature Information for DHCP for WLANs
WLAN Security

• Finding Feature Information, on page 1561
• Prerequisites for Layer 2 Security, on page 1561
• Information About AAA Override, on page 1562
• How to Configure WLAN Security, on page 1562
• Additional References, on page 1570
• Feature Information about WLAN Layer 2 Security, on page 1571

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Layer 2 Security

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on the information advertised in beacon and probe responses. The available Layer 2 security policies are as follows:

• None (open WLAN)
• Static WEP or 802.1X

Note

• Because static WEP and 802.1X are both advertised by the same bit in beacon and probe responses, they cannot be differentiated by clients. Therefore, they cannot both be used by multiple WLANs with the same SSID.
• WLAN WEP is not supported in 1810w Access Point.
• WPA/WPA2

Note
• Although WPA and WPA2 cannot be used by multiple WLANs with the same SSID, you can configure two WLANs with the same SSID with WPA/TKIP with PSK and Wi-Fi Protected Access (WPA) / Temporal Key Integrity Protocol (TKIP) with 802.1X, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X.

• A WLAN configured with TKIP support will not be enabled on an RM3000AC module.

Related Topics
Configuring Static WEP + 802.1X Layer 2 Security Parameters (CLI), on page 1562
Configuring Layer 2 Parameters (GUI), on page 1566
Configuring Static WEP Layer 2 Security Parameters (CLI), on page 1563
Configuring WPA + WPA2 Layer 2 Security Parameters (CLI), on page 1564
Configuring 802.1X Layer 2 Security Parameters (CLI), on page 1566
Configuring Advanced WLAN Properties (CLI), on page 1540
Information About AAA Override, on page 1562

Information About AAA Override

The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

Related Topics
Configuring Advanced WLAN Properties (CLI), on page 1540
Prerequisites for Layer 2 Security, on page 1561

How to Configure WLAN Security

Configuring Static WEP + 802.1X Layer 2 Security Parameters (CLI)

Before you begin
You must have administrator privileges.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wlan profile-name</td>
<td>Enters WLAN configuration submode. The profile-name is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# wlan test4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> security static-wep-key { authentication { open</td>
<td>sharedkey } encryption { 104</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-wlan)# security static-wep-key encryption 40 hex 0 test2</td>
<td>• <strong>authentication</strong>—Configures 802.11 authentication.</td>
</tr>
<tr>
<td></td>
<td>• <strong>encryption</strong>—Sets the static WEP keys and indices.</td>
</tr>
<tr>
<td></td>
<td>• <strong>open</strong>—Configures open system authentication.</td>
</tr>
<tr>
<td></td>
<td>• <strong>sharedkey</strong>—Configures shared key authentication.</td>
</tr>
<tr>
<td></td>
<td>• <strong>104, 40</strong>—Specifies the WEP key size.</td>
</tr>
<tr>
<td></td>
<td>• <strong>hex, ascii</strong>—Specifies the input format of the key.</td>
</tr>
<tr>
<td></td>
<td>• <strong>wep-key-index, wep-key-index1-4</strong>—Type of password that follows. A value of 0 indicates that an unencrypted password follows. A value of 8 indicates that an AES encrypted follows.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- [Prerequisites for Layer 2 Security](#), on page 1561

### Configuring Static WEP Layer 2 Security Parameters (CLI)

#### Before you begin

You must have administrator privileges.
## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wlan profile-name</td>
<td>Enters WLAN configuration submode. The <em>profile-name</em> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch# wlan test4</td>
<td></td>
</tr>
</tbody>
</table>
| Step 3 | security static-wep-key [authentication {open | shared}] [encryption {104 | 40}] {ascii | hex} [0 | 8]] | The keywords are as follows:  
- **static-wep-key**—Configures Static WEP Key authentication.  
- **authentication**—Specifies the authentication type you can set. The values are open and shared.  
- **encryption**—Specifies the encryption type that you can set. The valid values are 104 and 40. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.  
- **ascii**—Specifies the key format as ASCII.  
- **hex**—Specifies the key format as HEX. |
|      | **Example:** Switch(config-wlan)# security static-wep-key authentication open | |
| Step 4 | end | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode. |
|      | **Example:** Switch(config)# end | |

### Related Topics

- Prerequisites for Layer 2 Security, on page 1561

---

## Configuring WPA + WPA2 Layer 2 Security Parameters (CLI)

### Note

The default security policy is WPA2.

### Before you begin

You must have administrator privileges.
## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wlan profile-name</code></td>
<td>Enters WLAN configuration submode. The <code>profile-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch# wlan test4</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>security wpa</code></td>
<td>Enables WPA.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-wlan)# security wpa</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>security wpa wpa1</code></td>
<td>Enables WPA1.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-wlan)# security wpa wpa1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>`security wpa wpa1 ciphers [aes</td>
<td>tkip]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-wlan)# security wpa wpa1 ciphers aes</code></td>
<td>- <code>aes</code>—Specifies WPA/AES support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>tkip</code>—Specifies WPA/TKIP support.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>security wpa wpa2</code></td>
<td>Enables WPA2.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-wlan)# security wpa wpa2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>`security wpa wpa2 ciphers [aes</td>
<td>tkip]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config-wlan)# security wpa wpa2 ciphers tkip</code></td>
<td>- <code>aes</code>—Specifies WPA/AES support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>tkip</code>—Specifies WPA/TKIP support.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

## Related Topics

- [Prerequisites for Layer 2 Security](#), on page 1561
Configuring 802.1X Layer 2 Security Parameters (CLI)

Before you begin

You must have administrator privileges.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wlan profile-name</td>
<td>Enters WLAN configurations submode. The profile-name is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# wlan test4</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>security dot1x</td>
<td>Specifies 802.1X security.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-wlan)# security dot1x</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>security [authentication-list auth-list-name</td>
<td>The keywords and arguments are as follows:</td>
</tr>
<tr>
<td>Example:</td>
<td>encryption {0</td>
<td>104</td>
</tr>
<tr>
<td>Switch(config-wlan)# security encryption</td>
<td>• encryption—Specifies the length of the CKIP encryption key. The valid values are 0, 40, and 104. Zero (0) signifies no encryption. This is the default.</td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>Note All keys in a WLAN must be of the same size.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press \texttt{Ctrl-Z} to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

Prerequisites for Layer 2 Security, on page 1561

Configuring Layer 2 Parameters (GUI)

Before you begin

• You must have administrator privileges.
Procedure

Step 1  Click **Configuration > WLAN >**. The **WLANs** page appears.

Step 2  Click the WLANs profile of the WLAN you want to configure. The **WLANs > Edit >** page appears.

Step 3  Click the **Security > Layer 2 >** tab.

**Note**  WLAN WEP is not supported in 1810w Access Point.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer2 Security</td>
<td>Layer 2 security for the selected WLAN. Values are the following:</td>
</tr>
<tr>
<td></td>
<td>• None—No Layer 2 security selected.</td>
</tr>
<tr>
<td></td>
<td>• WPA+WPA2—Wi-Fi Protected Access.</td>
</tr>
<tr>
<td></td>
<td>• 802.1X—WEP 802.1X data encryption type. For information on these settings,</td>
</tr>
<tr>
<td></td>
<td>see the Layer 2 802.1X Parameters topic.</td>
</tr>
<tr>
<td></td>
<td>• Static WEP—Static WEP encryption parameters.</td>
</tr>
<tr>
<td></td>
<td>• Static WEP + 802.1x—Both Static WEP and 802.1X parameters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC Filtering</th>
<th>MAC address filtering. You can locally configure clients by their MAC addresses in the <strong>MAC Filters &gt; New page</strong>. You can add a maximum of 12000 local net users. Otherwise, configure the clients on a RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note</strong>  MAC Filtering is also known as MAC Authentication By Pass (MAB).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fast Transition</th>
<th>Check box to enable or disable a fast transition between access points.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over the DS</td>
<td>Check box to enable or disable a fast transition over a distributed system.</td>
</tr>
<tr>
<td>Reassociation</td>
<td>Time in seconds after which a fast transition reassociation times out.</td>
</tr>
<tr>
<td>Timeout</td>
<td></td>
</tr>
</tbody>
</table>

To configure the **WPA + WPA2** parameters, provide the following details:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA Policy</td>
<td>Check box to enable or disable WPA policy.</td>
</tr>
<tr>
<td>WPA Encryption</td>
<td>WPA2 encryption type: TKIP or AES. Available only if the WPA policy is enabled.</td>
</tr>
<tr>
<td>WPA2 Policy</td>
<td>Check box to enable or disable WPA2 policy.</td>
</tr>
<tr>
<td>WPA2 Encryption</td>
<td>WPA2 encryption type: TKIP or AES. Available only if the WPA2 policy is enabled.</td>
</tr>
</tbody>
</table>
### Authentication Key Management

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The rekeying mechanism parameter. Values are the following:</td>
</tr>
<tr>
<td></td>
<td>• 802.1X</td>
</tr>
<tr>
<td></td>
<td>• CCKM</td>
</tr>
<tr>
<td></td>
<td>• PSK</td>
</tr>
<tr>
<td></td>
<td>• 802.1x + CCKM</td>
</tr>
</tbody>
</table>

**PSK Format**

Enabled when you select the PSK value for Authentication Key Management. Choose ASCII or the HEX format and enter the preshared key.

To configure **802.1x** parameters, provide the following details:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 data encryption</td>
<td>WEP 802.11 data encryption type.</td>
</tr>
</tbody>
</table>

**Type**

Security type.

**Key size**

Key size. Values are the following:

- None
- 40 bits
- 104 bits

The third-party AP WLAN (17) can only be configured with 802.1X encryption. Drop-down configurable 802.1X parameters are not available for this WLAN.

To specify **Static WEP**, configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 Data Encryption</td>
<td>Static WEP encryption type.</td>
</tr>
</tbody>
</table>

**Current Key**

Displays the current selected key details.

**Type**

Security type.

**Key size**

Key size. Values are the following:

- Not set
- 40 bits
- 104 bits
### Key Index
- **Description**: Key index from 1 to 4.
  - One unique WEP key index can be applied to each WLAN. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption.
  - Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption.

### Encryption Key
- **Description**: Encryption key.

### Key Format
- **Description**: Encryption key format in ASCII or HEX.

### Allow Shared Key Authentication
- **Description**: Key authentication that you can enable or disable.

To configure Static WEP + 802.1X Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Static WEP Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>802.11 Data Encryption</td>
<td>Static WEP encryption type.</td>
</tr>
<tr>
<td>Current Key</td>
<td>Displays the current selected key details.</td>
</tr>
<tr>
<td>Type</td>
<td>Security type.</td>
</tr>
<tr>
<td>Key size</td>
<td>Key size. Values are the following:</td>
</tr>
<tr>
<td></td>
<td>• Not set</td>
</tr>
<tr>
<td></td>
<td>• 40 bits</td>
</tr>
<tr>
<td></td>
<td>• 104 bits</td>
</tr>
<tr>
<td>Key Index</td>
<td>Key index from 1 to 4.</td>
</tr>
<tr>
<td></td>
<td>The key index is unique per WLAN. You can only have one &quot;key 1&quot; on a given WLAN. You can define up to 4 keys per WLAN, and the switch will announce the key index, to allow clients configured the same way to know what key to use. This is per WLAN. You can configure all your WLANs (up to 512) as WEP if you want, each with up to 4 keys.</td>
</tr>
<tr>
<td>Encryption Key</td>
<td>Encryption key.</td>
</tr>
<tr>
<td>Key Format</td>
<td>Encryption key format in ASCII or HEX.</td>
</tr>
<tr>
<td>Allow Shared Key Authentication</td>
<td>Key authentication that you can enable or disable.</td>
</tr>
</tbody>
</table>

<p>| <strong>802.1x Parameters</strong> |                                                 |
| 802.11 Data Encryption | Static WEP encryption type.                     |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Security type.</td>
</tr>
<tr>
<td>Key size</td>
<td>Key size. Values are the following:</td>
</tr>
<tr>
<td></td>
<td>• Not set</td>
</tr>
<tr>
<td></td>
<td>• 40 bits</td>
</tr>
<tr>
<td></td>
<td>• 104 bits</td>
</tr>
</tbody>
</table>

**Step 4**
Click **Apply**.

**Related Topics**
*Prerequisites for Layer 2 Security*, on page 1561

**Additional References**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN command reference</td>
<td><em>WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em></td>
</tr>
<tr>
<td>Security configuration guide</td>
<td><em>Security Configuration Guide (Catalyst 3850 Switches)</em></td>
</tr>
</tbody>
</table>

**Error Message Decoder**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information about WLAN Layer 2 Security

This table lists the features in this module and provides links to specific configuration information.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN Security functionality</td>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Feature Information about WLAN Layer 2 Security
CHAPTER 87

Setting Client Count Per WLAN

- Finding Feature Information, on page 1573
- Restrictions for Setting Client Count for WLANs, on page 1573
- Information About Setting the Client Count per WLAN, on page 1574
- How to Configure Client Count Per WLAN, on page 1574
- Monitoring Client Connections (CLI), on page 1576
- Additional References for Client Connections, on page 1577
- Feature Information about Client Connections Per WLAN, on page 1577

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Setting Client Count for WLANs

- When a WLAN has reached the limit on the maximum number of clients connected to it or an AP radio and a new client tries to join the WLAN, the client cannot connect to the WLAN until an existing client gets disconnected.

- Roaming clients are considered as new clients. The new client can connect to a WLAN, which has reached the maximum limit on the number of connected clients, only when an existing client gets disconnected.

Note

For more information about the number of clients that are supported, see the product data sheet of your switch.

Related Topics

Configuring Client Count per WLAN (CLI), on page 1574
Information About Setting the Client Count per WLAN

You can set a limit to the number of clients that can connect to a WLAN, which is useful in scenarios where you have a limited number of clients that can connect to a switch. For example, consider a scenario where the switch can serve up to 256 clients on a WLAN and these clients can be shared between enterprise users (employees) and guest users. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure for each WLAN depends on the platform that you are using.

Related Topics
- Configuring Client Count per WLAN (CLI), on page 1574
- Configuring Client Count Per AP Per WLAN (CLI), on page 1575
- Configuring Client Count per AP Radio per WLAN (CLI), on page 1575
- Restrictions for Setting Client Count for WLANs, on page 1573
- Monitoring Client Connections (CLI), on page 1576

How to Configure Client Count Per WLAN

Configuring Client Count per WLAN (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>wlan profile-name</code></td>
<td>Enters WLAN configuration submode. The <code>profile-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# wlan test4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>client association limit limit</code></td>
<td>Configures the maximum number of client associations per WLAN. The range is 0 to 200012000. A default value is 0 (no limit).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-wlan)# client association limit 2000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileded EXEC mode. Alternatively, you can also press Ctrl-z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(wlan-config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Client Count Per AP Per WLAN (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters WLAN configuration submode. The <code>profile-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td><code>wlan profile-name</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# wlan test4</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the maximum number of clients per AP per WLAN. The range is 1 - 400.</td>
</tr>
<tr>
<td><code>client association limit ap ap-limit</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-wlan)# client association limit ap 250</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-z to exit global configuration mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(wlan-config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Information About Setting the Client Count per WLAN, on page 1574
- Restrictions for Setting Client Count for WLANs, on page 1573
- Monitoring Client Connections (CLI), on page 1576

Configuring Client Count per AP Radio per WLAN (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters WLAN configuration submode. The <code>profile-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td><code>wlan profile-name</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# wlan test4</code></td>
<td></td>
</tr>
</tbody>
</table>
### Monitoring Client Connections (CLI)

The following commands can be used to monitor client connections on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wlan name wlan-name</code></td>
<td>Displays the WLAN properties. Here is an example:</td>
</tr>
</tbody>
</table>
| | `. . . .
Max Associated Clients per WLAN :0
Max Associated Clients per AP per WLAN :0
Max Associated Clients per AP Radio per WLAN :0 . . . . |
| `show wlan id wlan-id` | Displays the WLAN properties. Here is an example: |
| | `. . . .
Max Associated Clients per WLAN :0
Max Associated Clients per AP per WLAN :0
Max Associated Clients per AP Radio per WLAN :0 . . . . |

**Related Topics**

- Configuring Client Count per WLAN (CLI), on page 1574
- Configuring Client Count Per AP Per WLAN (CLI), on page 1575
- Configuring Client Count per AP Radio per WLAN (CLI), on page 1575
- Information About Setting the Client Count per WLAN, on page 1574
Additional References for Client Connections

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN Command References</td>
<td>WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td></td>
<td>WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature Information about Client Connections Per WLAN

This table lists the features in this module and provides links to specific configuration information:
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Connections Per WLAN, Per AP, and per AP Radio</td>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for 802.11w

• To configure 802.11w feature for optional and mandatory, you must have WPA and AKM configured.

  Note

  The RNS (Robust Secure Network) IE must be enabled with an AES Cipher.

• To configure 802.11w as mandatory, you must enable PMF AKM in addition to WPA AKM.

Related Topics

Configuring 802.11w (CLI), on page 1581
Disabling 802.11w (CLI), on page 1582
Restrictions for 802.11w

- 802.11w cannot be applied on an open WLAN, WEP-encrypted WLAN, or a TKIP-encrypted WLAN.
- The WLAN on which 802.11w is configured must have either WPA2-PSK or WPA2-802.1x security configured.

Related Topics
- Configuring 802.11w (CLI), on page 1581
- Disabling 802.11w (CLI), on page 1582
- Information About 802.11w, on page 1580

Information About 802.11w

Wi-Fi is a broadcast medium that enables any device to eavesdrop and participate either as a legitimate or rogue device. Control and management frames such as authentication/deauthentication, association/disassociation, beacons, and probes are used by wireless clients to select an AP and to initiate a session for network services.

Unlike data traffic which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to tear down a session between a client and AP.

The 802.11w protocol applies only to a set of robust management frames that are protected by the Management Frame Protection (PMF) service. These include Disassociation, Deauthentication, and Robust Action frames.

Management frames that are considered as robust action and therefore protected are the following:
- Spectrum Management
- QoS
- Block Ack
- SA Query
- Vendor-specific Protected

When 802.11w is implemented in the wireless medium, the following occur:
- Client protection is added by the AP adding cryptographic protection (by including the MIC information element) to deauthentication and disassociation frames preventing them from being spoofed in a DOS attack.
- Infrastructure protection is added by adding a Security Association (SA) teardown protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.
Related Topics
Configuring 802.11w (CLI), on page 1581
Disabling 802.11w (CLI), on page 1582
Prerequisites for 802.11w, on page 1579
Restrictions for 802.11w, on page 1580
Monitoring 802.11w (CLI), on page 1583

How to Configure 802.11w

Configuring 802.11w (CLI)

Before you begin
WPA and AKM must be configured.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wlan profile-name</td>
<td>Enters WLAN configuration submode. The profile-name is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# wlan test4</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>shutdown</td>
<td>Shutdown the WLAN before configuring the PMF.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch shutdown</td>
<td></td>
</tr>
</tbody>
</table>
| Step 4 | security pmf {association-check association-comeback-time-in-seconds | Configures the PMF parameters with the following options:
| | mandatory | • association-comeback—Configures the 802.11w association comeback time.
| | optional | The range is from 1 to 20 seconds.
| | saquery saquery-time-in-milliseconds} | • mandatory—Requires clients to negotiate 802.11w PMF protection on a WLAN.
| | Example: Switch(config-wlan)# security pmf saquery-retry-time 200 | • optional—Enables 802.11w PMF protection on a WLAN.
| | | • saquery—Time interval identified in milliseconds before which the SA query response is expected. If the switch does |
### Disabling 802.11w (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** wlan profile-name  | Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN. |
| Example:                      |                                                                         |
| Switch# wlan test4            |                                                                         |

| **Step 3** shutdown           | Shutdown the WLAN before configuring the PMF.                           |
| Example:                      |                                                                         |
| Switch shutdown               |                                                                         |

| **Step 4** no security pmf    | Disables PMF on the WLAN. The following attributes are available:       |
| [association-comeback         | • association-comeback—Disables the 802.11w association comeback time.  |
| association-check-comback-interval-seconds |                                                                         |
| mandatory | optional | saquery          |
| saquery-time-interval-milliseconds] |                                                                         |
| Example:                      |                                                                         |

---

**Related Topics**

- Information About 802.11w, on page 1580
- Prerequisites for 802.11w, on page 1579
- Restrictions for 802.11w, on page 1580
- Monitoring 802.11w (CLI), on page 1583

---

**Purpose**

**Command or Action**

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>not get a response, another SQ query is tried.</td>
</tr>
<tr>
<td>The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.</td>
</tr>
</tbody>
</table>

**Step 5** no shutdown

Example:

Switch no shutdown

**Step 6** end

Example:

Switch(config-wlan)# end

**Restart the WLAN for the changes to take effect.**

**Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-z to exit global configuration mode.**
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Switch(config-wlan)# no security pmf | • **mandatory**—Disables client to negotiate 802.11w PMF protection on a WLAN.  
• **optional**—Disables 802.11w PMF protection on a WLAN.  
• **saquery**—Time interval identified in the association response to an already associated client before the association can be tried again. This time interval checks if the client is a real client and not a rogue client during the association comeback time. If the client does not respond within this time, the client association is deleted from the switch.  
The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds. |

**Step 5**  
**Example:**  
Switch no shutdown  
**Purpose:** Restart the WLAN for the changes to take effect.

**Step 6**  
**Example:**  
Switch(config-wlan)# end  
**Purpose:** Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-z to exit global configuration mode.

**Related Topics**  
[Information About 802.11w](#), on page 1580  
[Prerequisites for 802.11w](#), on page 1579  
[Restrictions for 802.11w](#), on page 1580  
[Monitoring 802.11w (CLI)](#), on page 1583

**Monitoring 802.11w (CLI)**

The following command can be used to monitor 802.11w:
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wlan name wlan-profile-name</code></td>
<td>Displays the WLAN parameters on the WLAN. The PMF parameters are displayed. Here is an example:</td>
</tr>
</tbody>
</table>
|                                              | . . . .  
|                                              | Auth Key Management  
|                                              | 802.1x : Disabled  
|                                              | PSK : Enabled  
|                                              | CCKM : Disabled  
|                                              | FT dot1x : Disabled  
|                                              | FT PSK : Disabled  
|                                              | PMF dot1x : Disabled  
|                                              | PMF PSK : Enabled  
|                                              | FT Support : Disabled  
|                                              | FT Reassociation Timeout : 20  
|                                              | FT Over-The-DS mode : Disabled  
|                                              | PMF Support : Required  
|                                              | PMF Association Comeback Timeout : 9  
|                                              | PMF SA Query Time : 200  
|                                              | . . . .  

**Related Topics**

- Configuring 802.11w (CLI), on page 1581
- Disabling 802.11w (CLI), on page 1582
- Information About 802.11w, on page 1580

**Additional References for 802.11w**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN Command Reference</td>
<td>WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>
Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11w</td>
<td>IEEE 802.11w Protected Management Frames</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature Information for 802.11w

This table lists the features in this module and provides links to specific configuration information:

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11w</td>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 89

Configuring Wi-Fi Direct Client Policy

- Finding Feature Information, on page 1587
- Restrictions for the Wi-Fi Direct Client Policy, on page 1587
- Information About the Wi-Fi Direct Client Policy, on page 1588
- How to Configure Wi-Fi Direct Client Policy, on page 1588
- Additional References for Wi-Fi Direct Client Policy, on page 1590
- Feature Information about Wi-Fi Direct Client Policy, on page 1591

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for the Wi-Fi Direct Client Policy

- Wi-Fi Direct Client Policy is applicable to WLANs that have APs in local mode only.
- Cisco APs in FlexConnect mode (even in central authentication and central switching) is not supported.
- We do not recommend enabling this feature in a mixed AP mode deployment (some APs in FlexConnect mode and some APs in local mode). Such types of deployment is not supported or tested in FlexConnect mode.
- If WLAN applied client policy is invalid, the client is excluded with the exclusion reason being 'Client QoS Policy failure'.
### Information About the Wi-Fi Direct Client Policy

Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices may associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently. You can use the switch to configure the Wi-Fi Direct Client Policy, on a per WLAN basis, where you can allow or disallow association of Wi-Fi devices with infrastructure WLANs, or disable Wi-Fi Direct Client Policy altogether for WLANs.

**Related Topics**
- Configuring the Wi-Fi Direct Client Policy (CLI), on page 1588
- Disabling Wi-Fi Direct Client Policy (CLI), on page 1589
- Monitoring Wi-Fi Direct Client Policy (CLI), on page 1590

### How to Configure Wi-Fi Direct Client Policy

#### Configuring the Wi-Fi Direct Client Policy (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters WLAN configuration submode. The <code>profile-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td>wlan profile-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# wlan test4</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the Wi-Fi Direct client policy on the WLAN using one of the following:</td>
</tr>
<tr>
<td>wifidirect policy {permit</td>
<td>deny }</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-wlan)# wifidirect policy permit</td>
</tr>
</tbody>
</table>

- `permit`—Enables Wi-Fi Direct clients to associate with the WLAN.
- `deny`—When the Wi-Fi Direct policy is configured as "deny," the switch permits or denies Wi-Fi Direct devices based on the device capabilities. A Wi-Fi Direct device reports these capabilities in its association request to the switch and these are based on the Wi-Fi capabilities of the device. These include:
  - Concurrent operation
  - Cross connection
The command **no wifidirect policy** ignores the client’s Wi-Fi direct status. Additionally, the access point also does not advertise any beacons and probes. Effectively, the **no** form of the command disables the Wi-Fi direct feature on the WLAN.

If the Wi-Fi device supports either concurrent operations or cross connections or both, the client association is denied. The client can associate if the device does not support concurrent operations and cross connections.

**Step 4**

```
end
Example:
Switch(config-wlan)# end
```

Returns to privileged EXEC mode. Alternatively, you can also press `Ctrl-z` to exit global configuration mode.

**Related Topics**

- Information About the Wi-Fi Direct Client Policy, on page 1588
- Monitoring Wi-Fi Direct Client Policy (CLI), on page 1590

## Disabling Wi-Fi Direct Client Policy (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>wlan profile-name</code></td>
<td>Enters WLAN configuration submode. The <code>profile-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# wlan test4</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>no wifidirect policy</code></td>
<td>Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# no wifidirect policy</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 4**

End

Example:

Switch(config-wlan)# end

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless client wifidirect stats</td>
<td>Displays the total number of clients associated and the number of association requests rejected if the Wi-Fi Direct Client Policy is enabled.</td>
</tr>
<tr>
<td>show wlan summary</td>
<td>Displays status of the Wi-Fi Direct on the WLAN.</td>
</tr>
<tr>
<td>show wireless cli mac-address mac-address</td>
<td>Displays the detail information of a client.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Information About the Wi-Fi Direct Client Policy, on page 1588
- Monitoring Wi-Fi Direct Client Policy (CLI), on page 1590

**Monitoring Wi-Fi Direct Client Policy (CLI)**

The following commands can be used to monitor Wi-Fi Direct Client Policy:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless client wifidirect stats</td>
<td>Displays the total number of clients associated and the number of association requests rejected if the Wi-Fi Direct Client Policy is enabled.</td>
</tr>
<tr>
<td>show wlan summary</td>
<td>Displays status of the Wi-Fi Direct on the WLAN.</td>
</tr>
<tr>
<td>show wireless cli mac-address mac-address</td>
<td>Displays the detail information of a client.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring the Wi-Fi Direct Client Policy (CLI), on page 1588
- Disabling Wi-Fi Direct Client Policy (CLI), on page 1589
- Information About the Wi-Fi Direct Client Policy, on page 1588

**Additional References for Wi-Fi Direct Client Policy**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN Command reference</td>
<td>WLAN Command Reference, Cisco IOS XE Release 3 SE (Cisco WLC 5700 Series) WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

**Error Message Decoder**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>
### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases,</td>
</tr>
<tr>
<td></td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

### Feature Information about Wi-Fi Direct Client Policy

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wi-Fi Direct Feature</td>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Feature Information about Wi-Fi Direct Client Policy
CHAPTER 90

Configuring 802.11r BSS Fast Transition

- Finding Feature Information, on page 1593
- Restrictions for 802.11r Fast Transition, on page 1593
- Information About 802.11r Fast Transition, on page 1594
- How to Configure 802.11r Fast Transition, on page 1596
- Additional References for 802.11r Fast Transition, on page 1603
- Feature Information for 802.11r Fast Transition, on page 1604

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for 802.11r Fast Transition

- In 8.1 and earlier releases, this feature is not supported on access points in FlexConnect mode. In Release 8.2, this restriction is removed.

- For APs in FlexConnect mode:
  - 802.11r Fast Transition is supported in central and locally switched WLANs.
  - This feature is not supported for the WLANs enabled for local authentication.
  - 802.11r client association is not supported on access points in standalone mode.
  - 802.11r fast roaming is not supported on access points in standalone mode.
  - 802.11r fast roaming between local authentication and central authentication WLAN is not supported.
  - 802.11r fast roaming works only if the APs are in the same FlexConnect group.
• EAP LEAP method is not supported.

• TSPEC is not supported for 802.11r fast roaming. Therefore, RIC IE handling is not supported.

• If WAN link latency exists, fast roaming is also delayed. Voice or data maximum latency should be verified. The Cisco WLC handles 802.11r Fast Transition authentication request during roaming for both Over-the-Air and Over-the-DS methods.

• This feature is supported on open and WPA2 configured WLANs.

• Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r enabled WLANs.

Another workaround is to have two SSIDs with the same name but with different security settings (FT and non-FT).

• Fast Transition resource request protocol is not supported because clients do not support this protocol. Also, the resource request protocol is an optional protocol.

• To avoid any Denial of Service (DoS) attack, each Cisco WLC allows a maximum of three Fast Transition handshakes with different APs.

• Non-802.11r capable devices will not be able to associate with FT-enabled WLAN.

• 802.11r FT + PMF is not recommended.

• 802.11r FT Over-the-Air roaming is recommended for FlexConnect deployments.

• In a default FlexGroup scenario, fast roaming is not supported.

• As part of a fix for CSCvk64674, Adaptive mode for 802.11r Fast Transition is not supported for open WLANs. That is, if you choose Layer 2 security as None for a WLAN, ensure that you disable the Adaptive mode for 802.11r Fast Transition; else, WLAN cannot be enabled.

Related Topics
Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 1596
Disabling 802.11r Fast Transition (CLI), on page 1601
Configuring 802.11r BSS Fast Transition on a 802.1x Security Enabled WLAN (CLI), on page 1598
Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI), on page 1599
Configuring 802.11 Fast Transition (GUI), on page 1600
Information About 802.11r Fast Transition, on page 1594

Information About 802.11r Fast Transition

802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP, which is called Fast Transition (FT). The initial handshake allows the client and APs to do the Pairwise Transient Key (PTK) calculation in
advance. These PTK keys are applied to the client and AP after the client does the reassociation request or response exchange with new target AP.

802.11r provides two methods of roaming:

- Over-the-Air
- Over-the-DS (Distribution System)

The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without requiring reauthentication at every AP. WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

From Release 3E, you can create an 802.11r WLAN that is also an WPAv2 WLAN. In earlier releases, you had to create separate WLANs for 802.11r and for normal security. Non-802.11r clients can now join 802.11-r-enabled WLANs as the 802.11r WLANs can accept non-802.11r associations. If clients do not support mixed mode or 802.11r join, they can join non-802.11r WLANs. When you configure FT PSK and later define PSK, clients that can join only PSK can now join the WLAN in mixed mode.

**How a Client Roams**

For a client to move from its current AP to a target AP using the FT protocols, the message exchanges are performed using one of the following two methods:

- Over-the-Air — The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- Over-the-DS — The client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the switch.

*Figure 77: Message Exchanges when Over the Air client roaming is configured*

This figure shows the sequence of message exchanges that occur when Over the Air client roaming is configured.

```
MOBILITY DOMAIN - M1
```

- **Controller - 1**
  - Mobility update for C1
- **Controller - 2**
  - **AP1**
  - **Client C1**
  - Roaming direction
  - **AP2**
  - 802.11 auth request
  - 802.11 auth response

- **Actual communication path**
Figure 78: Message Exchanges when Over the DS client roaming is configured

This figure shows the sequence of message exchanges that occur when Over the DS client roaming is configured.

Related Topics
- Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 1596
- Disabling 802.11r Fast Transition (CLI), on page 1601
- Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI), on page 1598
- Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI), on page 1599
- Configuring 802.11 Fast Transition (GUI), on page 1600
- Monitoring 802.11r Fast Transition (CLI), on page 1601
- Restrictions for 802.11r Fast Transition, on page 1593

How to Configure 802.11r Fast Transition

Configuring 802.11r Fast Transition in an Open WLAN (CLI)

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

Example:

Switch# configure terminal
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td><code>wlan profile-name</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch# wlan test4</code></td>
<td>Enters WLAN configuration submode. The <em>profile-name</em> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>client vlan vlan-id</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config-wlan)# client vlan 0120</code></td>
<td>Associate the client VLAN to the WLAN.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>no security wpa</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config-wlan)# no security wpa</code></td>
<td>Disable WPA security.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>no security wpa akm dot1x</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config-wlan)# no security wpa akm dot1x</code></td>
<td>Disable security AKM for dot1x.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>no security wpa wpa2</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config-wlan)# no security wpa wpa2</code></td>
<td>Disables WPA2 security.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>no wpa wpa2 ciphers aes</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config-wlan)# no security wpa wpa2 ciphers aes</code></td>
<td>Disables WPA2 ciphers for AES.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>security ft</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config-wlan)# security ft</code></td>
<td>Specifies the 802.11r fast transition parameters.</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>no shutdown</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config-wlan)# shutdown</code></td>
<td>Shutdown the WLAN.</td>
</tr>
<tr>
<td>Step 10</td>
<td><code>end</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config-wlan)# end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-z</strong> to exit global configuration mode.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Information About 802.11r Fast Transition, on page 1594
- Monitoring 802.11r Fast Transition (CLI), on page 1601
- Restrictions for 802.11r Fast Transition, on page 1593
## Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wlan profile-name</code></td>
<td>Enters WLAN configuration submode. The <code>profile-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# <code>wlan test4</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>client vlan vlan-name</code></td>
<td>Associate the client VLAN to this WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-wlan)# <code>client vlan 0120</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>local-auth/local-auth-profile-eap</code></td>
<td>Enable the local auth EAP profile.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-wlan)# <code>local-auth</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>security dot1x authentication-list default</code></td>
<td>Enable security authentication list for dot1x security. The configuration is similar for any dot1x security WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-wlan)# <code>security dot1x authentication-list default</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>security ft</code></td>
<td>Enables 802.11r Fast Transition on this WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-wlan)# <code>security ft</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>security wpa akm ft dot1x</code></td>
<td>Enables 802.1x security on the WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-wlan)# <code>security wpa akm ft dot1x</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>no shutdown</code></td>
<td>Enable the WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-wlan)# <code>no shutdown</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-z</code> to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-wlan)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wlan profile-name</td>
<td>Enters WLAN configuration submode. The <em>profile-name</em> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# wlan test4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> client vlan vlan-name</td>
<td>Associates the client VLAN to this WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-wlan)# client vlan 0120</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-wlan)# no security wpa akm dot1x</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> security wpa akm ft psk</td>
<td>Configures FT PSK support.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-wlan)# security wpa akm ft psk</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> security wpa akm psk set-key {ascii {0 8}</td>
<td>hex {0 8}}</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-wlan)# security wpa akm psk set-key ascii 0 test</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> security ft</td>
<td>Configures 802.11r Fast Transition.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-wlan)# security ft</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> no shutdown</td>
<td>Enables the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-wlan)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring 802.11 Fast Transition (GUI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 9</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

| Example: | Switch(config-wlan)# end |

**Related Topics**
- Information About 802.11r Fast Transition, on page 1594
- Monitoring 802.11r Fast Transition (CLI), on page 1601
- Restrictions for 802.11r Fast Transition, on page 1593

---

**Configuring 802.11 Fast Transition (GUI)**

**Procedure**

**Step 1**
- Click **Configuration > Wireless > WLANs**
- The **WLANs** page is displayed.

**Step 2**
- Locate the WLAN you want to configure by using the search mechanism on the page.

**Step 3**
- Click on the **WLAN Profile** of the WLAN.
- The **WLAN > Edit** page is displayed.

**Step 4**
- Click the **Security** and **Layer 2** tab.

**Step 5**
- Enable the **Fast Transition** check box to enable BSS Fast Transition.
- Uncheck the **Fast Transition** check box to disable BSS Fast Transition.

**Step 6**
- To enable BSS Fast Transition over the distributed system, enable the **Over the DS** checkbox. This is enabled by default.

**Note**
- Disabling over the DS enables over the air fast transition.

**Step 7**
- (Optional) Specify a reassociation timeout value in seconds in the **Reassociation Timeout** text box. The range is 1 to 100 seconds. The default value is 20 seconds.

**Step 8**
- Click **Apply**.

**Step 9**
- To configure the WLAN in 802.11r mixed-mode, choose one of the following options from the **Auth Key Mgmt** drop-down list:
  - **FT + 802.1x**
  - **FT + PSK**
  - **FT + 802.1x +CCKM**

**Related Topics**
- Information About 802.11r Fast Transition, on page 1594
- Monitoring 802.11r Fast Transition (CLI), on page 1601
Disabling 802.11r Fast Transition (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Example: Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters WLAN configuration submode. The <code>profile-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td><code>wlan profile-name</code></td>
<td>Example: Switch# wlan test4</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Disables 802.11r Fast Transition on the WLAN. <strong>Note</strong>: Disabling 802.11r Fast Transition for over the data source enables over the air fast transition.</td>
</tr>
<tr>
<td>`no security ft [over-the-ds</td>
<td>reassociation-timeout <code>timeout-in-seconds</code>]`</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Example: Switch(config)# end</td>
</tr>
</tbody>
</table>

**Related Topics**
- Information About 802.11r Fast Transition, on page 1594
- Monitoring 802.11r Fast Transition (CLI), on page 1601
- Restrictions for 802.11r Fast Transition, on page 1593

**Monitoring 802.11r Fast Transition (GUI)**

You can view the Authentication Key Management details of a client.

Choose **Monitor > Client**. The Clients page appears. Click the corresponding client to view the client details. In the **General** tab, you can view the Authentication Key Management for the client such as FT, PSK, 802.1x, CCKM, 802.1x + CCKM. If the AKM is for 802.11r mixed mode, then FT-802.1x, FT-802.1x-CCKM, or FT-PSK appears.

**Monitoring 802.11r Fast Transition (CLI)**

The following command can be used to monitor 802.11r Fast Transition:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wlan name wlan-name</code></td>
<td>Displays a summary of the configured parameters on the WLAN.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless client mac-address mac-address</code></td>
<td>Displays the summary of the 802.11r authentication key management configuration on a client.</td>
</tr>
</tbody>
</table>

```
. . .
. . .
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 15
  Fast BSS Transition : Implemented
Fast BSS Transition Details :
Client Statistics:
  Number of Bytes Received : 9019
  Number of Bytes Sent : 3765
  Number of Packets Received : 130
  Number of Packets Sent : 36
  Number of EAP Id Request Msg Timeouts : 0
  Number of EAP Request Msg Timeouts : 0
  Number of EAP Key Msg Timeouts : 0
  Number of Data Retries : 1
  Number of RTS Retries : 0
  Number of Duplicate Received Packets : 1
  Number of Decrypt Failed Packets : 0
  Number of Mic Failed Packets : 0
  Number of Mic Missing Packets : 0
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -48 dBm
  Signal to Noise Ratio : 40 dB
. . .
. . .
If the AKM for the client is 802.11r mixed mode, the following information appears in the output:

```
. . .
. . .
Authentication Key Management : FT-PSK
. . .
. . .
```

### Related Topics
- Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 1596
- Disabling 802.11r Fast Transition (CLI), on page 1601
- Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI), on page 1598
- Configuring 802.11r Fast Transition on a PSK Security Enabled WLAN (CLI), on page 1599
- Configuring 802.11 Fast Transition (GUI), on page 1600
- Information About 802.11r Fast Transition, on page 1594
# Additional References for 802.11r Fast Transition

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN Command Reference</td>
<td><em>WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em> <em>WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</em></td>
</tr>
</tbody>
</table>

## Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

## Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11r from IEEE</td>
<td>IEEE Standard for 802.11r</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All MIBs supported for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
# Feature Information for 802.11r Fast Transition

This table lists the features in this module and provides links to specific configuration information:

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11r Fast Transition</td>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Assisted Roaming

- Finding Feature Information, on page 1605
- Information About Assisted Roaming, on page 1605
- Restrictions for Assisted Roaming, on page 1606
- How to Configure Assisted Roaming, on page 1607
- Monitoring Assisted Roaming, on page 1608
- Configuration Examples for Assisted Roaming, on page 1608
- Additional References for Assisted Roaming, on page 1609
- Feature History and Information For Performing Assisted Roaming Configuration, on page 1610

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Assisted Roaming

The 802.11k standard allows clients to request neighbor reports containing information about known neighbor access points that are candidates for a service set transition. The use of the 802.11k neighbor list can limit the need for active and passive scanning.

The assisted roaming feature is based on an intelligent and client optimized neighbor list.

Unlike the Cisco Client Extension (CCX) neighbor list, the 802.11k neighbor list is generated dynamically on-demand and is not maintained on the switch. The 802.11k neighbor list is based on the location of the clients without requiring the mobility services engine (MSE). Two clients on the same switch but different APs can have different neighbor lists delivered depending on their individual relationship with the surrounding APs.

By default, the neighbor list contains only neighbors in the same band with which the client is associated. However, a switch exists that allows 802.11k to return neighbors in both bands.
Clients send requests for neighbor lists only after associating with the APs that advertise the RRM (Radio Resource Management) capability information element (IE) in the beacon. The neighbor list includes information about BSSID, channel, and operation details of the neighboring radios.

**Assembling and Optimizing the Neighbor List**

When the switch receives a request for an 802.11k neighbor list, the following occurs:

1. The switch searches the RRM neighbor table for a list of neighbors on the same band as the AP with which the client is currently associated with.

2. The switch checks the neighbors according to the RSSI (Received Signal Strength Indication) between the APs, the current location of the present AP, the floor information of the neighboring AP from Cisco Prime Infrastructure, and roaming history information on the switch to reduce the list of neighbors to six per band. The list is optimized for APs on the same floor.

**Assisted Roaming for Non-802.11k Clients**

It is also possible to optimize roaming for non-802.11k clients. You can generate a prediction neighbor list for each client without the client requiring to send an 802.11k neighbor list request. When this is enabled on a WLAN, after each successful client association/reassociation, the same neighbor list optimization is applied on the non-802.11k client to generate the neighbor list and store the list in the mobile station software data structure. Clients at different locations have different lists because the client probes are seen with different RSSI values by different neighbors. Because clients usually probe before any association or reassociation, this list is constructed with the most updated probe data and predicts the next AP that the client is likely to roam to.

We discourage clients from roaming to those less desirable neighbors by denying association if the association request to an AP does not match the entries on the stored prediction neighbor list.

Similar to aggressive load balancing, there is a switch to turn on the assisted roaming feature both on a per-WLAN basis and globally. The following options are available:

- Denial count—Maximum number of times a client is refused association.
- Prediction threshold—Minimum number of entries required in the prediction list for the assisted roaming feature to be activated.

Because both load balancing and assisted roaming are designed to influence the AP that a client associates with, it is not possible to enable both the options at the same time on a WLAN.

**Restrictions for Assisted Roaming**

- The assisted roaming feature is supported across multiple switches.
- This feature is supported only on 802.11n capable indoor access points. For a single band configuration, a maximum of 6 neighbors are visible in a neighbor list. For dual band configuration, a maximum of 12 neighbors are visible.
- You can configure assisted roaming only using the switch CLI.
# How to Configure Assisted Roaming

## Configuring Assisted Roaming (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wireless assisted-roaming floor-bias dBm</code></td>
<td>Configures neighbor floor label bias. The valid range is from 5 to 25 dBm, and the default value is 15 dBm.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# wireless assisted-roaming floor-bias 20</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>wlan wlan-id</code></td>
<td>Enters the WLAN configuration submode. The <code>wlan-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>assisted-roaming neighbor-list</code></td>
<td>Configures an 802.11k neighbor list for a WLAN. By default, assisted roaming is enabled on the neighbor list when you create a WLAN. The <code>no</code> form of the command disables assisted roaming neighbor list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(wlan)# assisted-roaming neighbor-list</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>assisted-roaming dual-list</code></td>
<td>Configures a dual-band 802.11k dual list for a WLAN. By default, assisted roaming is enabled on the dual list when you create a WLAN. The <code>no</code> form of the command disables assisted roaming dual list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(wlan)# assisted-roaming dual-list</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>assisted-roaming prediction</code></td>
<td>Configures assisted roaming prediction list feature for a WLAN. By default, the assisted roaming prediction list is disabled.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(wlan)# assisted-roaming prediction</td>
<td><strong>Note</strong> A warning message is displayed and load balancing is disabled for the WLAN if load balancing is already enabled for the WLAN.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 7</th>
<th>wireless assisted-roaming prediction-minimum count</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch# wireless assisted-roaming prediction-minimum</code></td>
</tr>
</tbody>
</table>

**Purpose:** Configures the minimum number of predicted APs required for the prediction list feature to be activated. The default value is 3.

**Note:** If the number of the AP in the prediction assigned to the client is less than the number that you specify, the assisted roaming feature will not apply on this roam.

<table>
<thead>
<tr>
<th>Step 8</th>
<th>wireless assisted-roaming denial-maximum count</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch# wireless assisted-roaming denial-maximum 8</code></td>
</tr>
</tbody>
</table>

**Purpose:** Configures the maximum number of times a client can be denied association if the association request is sent to an AP does not match any AP on the prediction. The valid range is from 1 to 10, and the default value is 5.

<table>
<thead>
<tr>
<th>Step 9</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# end</code></td>
</tr>
</tbody>
</table>

**Purpose:** Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

### Monitoring Assisted Roaming

The following command can be used to monitor assisted roaming configured on a WLAN.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wlan id wlan-id</code></td>
<td>Displays the WLAN parameters on the WLAN.</td>
</tr>
</tbody>
</table>

### Configuration Examples for Assisted Roaming

This example shows how to configure the neighbor floor label bias:

```
Switch# configure terminal
Switch(config)# wireless assisted-roaming floor-bias 10
Switch(config)# end
Switch# show wlan id 23
```

This example shows how to disable neighbor list on a specific WLAN:

```
Switch# configure terminal
Switch(config)# wlan test1
Switch(config (wlan)# no assisted-roaming neighbor-list
Switch(config (wlan)# end
Switch# show wlan id 23
```

This example shows how to configure the prediction list on a specific WLAN:
Switch# configure terminal
Switch(config)# wlan test1
Switch(config)(wlan)# assisted-roaming prediction
Switch(config)(wlan)# end
Switch# show wlan id 23

This example shows how to configure the prediction list based on assisted roaming prediction threshold and maximum denial count on a specific WLAN:

Switch# configure terminal
Switch(config)# wireless assisted-roaming prediction-minimum 4
Switch(config)# wireless assisted-roaming denial-maximum 4
Switch(config)(wlan)# end
Switch# show wlan id 23

### Additional References for Assisted Roaming

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td>System Management Command Reference (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>System Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

**Error Message Decoder**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
<tr>
<td>the Error Message Decoder tool.</td>
<td></td>
</tr>
</tbody>
</table>

**Standards and RFCs**

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11k</td>
<td></td>
</tr>
</tbody>
</table>

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information For Performing Assisted Roaming Configuration

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assisted Roaming</td>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring AP Groups

The following are the prerequisites for creating access point groups on a switch:

- The required access control list (ACL) must be defined on the router that serves the VLAN or subnet.
- Multicast traffic is supported with access point group VLANs. However, if the client roams from one access point to another, the client might stop receiving multicast traffic, unless IGMP snooping is enabled.

Related Topics

Information About Access Point Groups, on page 1612
Restrictions on Configuring Access Point Groups, on page 1612
Restrictions on Configuring Access Point Groups

- Suppose that the interface mapping for a WLAN in the AP group table is the same as the WLAN interface. If the WLAN interface is changed, the interface mapping for the WLAN in the AP group table also changes to the new WLAN interface.

Suppose that the interface mapping for a WLAN in the AP group table is different from the one defined for the WLAN. If the WLAN interface is changed, then the interface mapping for the WLAN in the AP group table does not change to the new WLAN interface.

- If you clear the configuration on the switch, all of the access point groups disappear except for the default access point group “default-group,” which is created automatically.

- The default access point group can have up to 16 WLANs associated with it. The WLAN IDs for the default access point group must be less than or equal to 16. If a WLAN with an ID greater than 16 is created in the default access point group, the WLAN SSID will not be broadcasted. All WLAN IDs in the default access point group must have an ID that is less than or equal to 16. WLANs with IDs greater than 16 can be assigned to custom access point groups.

- We recommend that you configure all Flex+Bridge APs in a mesh tree (in the same sector) in the same AP group and the same FlexConnect group, to inherit the WLAN-VLAN mappings properly.

- Whenever you add a new WLAN to an AP group, radio reset occurs and if any client is in connected state, the client is deauthenticated and is required to reconnect. We recommend that you add or modify the WLAN configuration of an AP group only during maintenance windows to avoid outages.

- The number of AP groups that you can configure cannot be more than the number of ap-count licenses on Cisco WLC. For example, if your Cisco WLC has 5 ap-count licenses, the maximum number of AP groups that you can configure is 5, including the default AP group.

Related Topics

- Information About Access Point Groups, on page 1612
- Prerequisites for Configuring AP Groups, on page 1611

Information About Access Point Groups

After you create up to 512 WLANs on the switch, you can selectively publish them (using access point groups) to different access points to better manage your wireless network. In a typical deployment, all users on a WLAN are mapped to a single interface on the switch. Therefore, all users that are associated with that WLAN are on the same subnet or VLAN. However, you can choose to distribute the load among several interfaces or to a group of users based on specific criteria such as individual departments (such as Marketing) by creating access point groups. Additionally, these access point groups can be configured in separate VLANs to simplify network administration.

Related Topics

- Creating Access Point Groups, on page 1613
- Viewing Access Point Group, on page 1614
- Assigning an Access Point to an AP Group, on page 1614
- Prerequisites for Configuring AP Groups, on page 1611
- Restrictions on Configuring Access Point Groups, on page 1612
How to Configure Access Point Groups

Creating Access Point Groups

Before you begin

You must have administrator privileges to perform this operation.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap group ap-group-name</td>
<td>Creates an access point group.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ap group my-ap-group</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>wlan wlan-name</td>
<td>Associates the AP group to a WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-apgroup)# wlan wlan-name</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) vlan vlan-name</td>
<td>Assigns the access point group to a VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-apgroup)# vlan test-vlan</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Example

This example shows how to create an AP group:

Switch# configure terminal
Switch(config-apgroup)# ap group test-ap-group-16
Switch(config-wlan-apgroup)# wlan test-ap-group-16
Switch(config-wlan-apgroup)# vlan VLAN1300

Related Topics

Information About Access Point Groups, on page 1612
Assigning an Access Point to an AP Group

Before you begin
You must have administrator privileges to perform this operation.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> ap name ap-name ap-group-name ap-group</td>
<td>Assigns the access point to the access point group. The keywords and arguments are as follows:</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# ap name 1240-101 ap-groupname apgroup_16</td>
<td>• <strong>name</strong>—Specifies that the argument following this keyword is the name of an AP that is associated to the switch.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ap-name</strong>—AP that you want to associate to the AP group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ap-group-name</strong>—Specifies that the argument following this keyword is the name of the AP group that is configured on the switch.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ap-group</strong>—Name of the access point group that is configured on the switch.</td>
</tr>
</tbody>
</table>

Related Topics

Information About Access Point Groups, on page 1612

Viewing Access Point Group

Before you begin
You must have administrator privileges to perform this operation.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show ap groups [extended ]</td>
<td>Displays the AP groups configured on the switch. The <strong>extended</strong> keyword displays all AP Groups information defined in the system in detail.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show ap groups</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

Information About Access Point Groups, on page 1612
### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN commands</td>
<td>WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td></td>
<td>WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td></td>
<td>(Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td></td>
<td>Lightweight Access Point Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Lightweight Access Point commands</td>
<td>Lightweight Access Point Command Reference, Cisco IOS XE Release 3SE</td>
</tr>
<tr>
<td></td>
<td>(Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td></td>
<td>Lightweight Access Point Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

#### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
<tr>
<td>the Error Message Decoder tool.</td>
<td></td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases,</td>
</tr>
<tr>
<td></td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>
Feature History and Information for Access Point Groups

This table lists the features in this module and provides links to specific configuration information.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Groups</td>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
INDEX

<$nopage>HTTP over SSL 851
  see HTTPS 851
<$nopage>IEEE 802.3ad 140
  See EtherChannel 140
<$nopage>PAgP 138
  See EtherChannel 138
<$nopage>Port Aggregation Protocol 138
  See EtherChannel 138
<$nopage>Secure Copy Protocol 844

11n Mode parameter 1269
802.11a (or 802.11b/g) Global Parameters page 1265
802.11a (or 802.11b/g) Network Status parameter 1265, 1271
802.11g Support parameter 1265
802.11h Global Parameters page 1271
802.11h, described 1262
802.11n 1261
  devices 1261
802.11r 1600
  configuring using GUI 1600
802.1x 953
802.1X authentication for access points 228
  described 228

A

access control entries 867
  See ACEs 867
access groups 879
  Layer 3 879
access groups, applying IPv4 ACLs to interfaces 890
access lists 873
  See ACLs 873
Access Point Authentication 228
Access Point Communication Protocols 205
access point core dumps, uploading 237
  using the GUI 237
Access Point Retransmission Interval 216
Access Point Retry Count 216
access points 204, 205, 244, 1289
  assisted roaming 1289
  priming 204
  supporting oversized images 244
access points (continued)
  viewing join information 205
    using the GUI 205
accounting 771, 780, 818
  with RADIUS 818
  with TACACS+ 771, 780
accounting, defined 771
ACEs 868
  Ethernet 868
  IP 868
ACLs 607, 868, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 887, 889,
  890, 894, 900, 901, 903, 913, 914, 915
  applying 607, 867, 890, 913, 914, 915
    on bridged packets 914
    on multicast packets 915
    on routed packets 914
    on switched packets 913
    time ranges to 887
    to an interface 890
    to QoS 607
    comments in 901
    compiling 903
    defined 872
    examples of 903
    extended IPv4 873, 881
      creating 881
      matching criteria 873
      interface 879
      IP 873, 874, 879, 887
        implicit deny 887
        implicit masks 874
        matching criteria 873
        undefined 879
IPv4 872, 873, 879, 889, 890
  applying to interfaces 890
    creating 872
    interfaces 879
    matching criteria 873
    numbers 873
    terminal lines, setting on 889
    unsupported features 873
Layer 4 information in 878
logging messages 875
  matching 879
  monitoring 900
ACLS (continued)
- port 868
- precedence of 868
- QoS 607
- router 868
- router ACLs and VLAN map configuration guidelines 878
- standard IPv4 873, 880
- creating 880
- matching criteria 873
- support in hardware 876
- time ranges to 878
- types supported 868
- unsupported features 873
- IPv4 873
- using router ACLs with VLAN maps 877
- VLAN maps 877, 894
- configuration guidelines 877
- configuring 894
- acronyms 5
- ACS 92
- activation, AP-count 1245
- activation, base 1243
- active link 177, 191
- active links 174
- adding 953, 955
- Additional References 1471, 1492, 1500, 1520
- VLAN trunks 1520
- VLANs 1492, 1500
- VTP 1471
- address aliasing 323
- address resolution 1190
- addresses 1189, 1190, 1207
- dynamic 1189
- defined 1189
- learning 1189
- MAC, discovering 1190
- static 1207
- adding and removing 1207
- aggregate-port learners 158
- aging time 1200
- MAC address table 1200
- All APs page 742
- AnchorTime parameter 733
- and ARP 1408
- and CPD 1408
- and SSH 844
- AP Mode parameter 742
- Apply Port Policy QoS GUI 687
- ARP 1190
- defined 1190
- table 1190
- address resolution 1190
- attributes 821
- vendor-specific 821
- attributes, RADIUS 821
- vendor-specific 821
- authenticating to 834, 835
- boundary switch 834
- KDC 834
- network services 835
- authentication 771, 776, 813, 837
- local mode with AAA 837
- RADIUS 813
- login 813
- TACACS+ 771, 776
- defined 771
- login 776
- authentication, defined 771
- authoritative time source, described 1184
- authorization 771, 779, 817
- with RADIUS 817
- with TACACS+ 771, 779
- authorization, defined 771
- automatic 951
- automatic creation of 138, 140
- autonegotiation 1422
- mismatches 1422
- Autonomous Access Points Converted to Lightweight Mode 236
- average rate shaping 615, 616
- Avoid Cisco AP Load parameter 733
- Avoid Foreign AP Interference parameter 733
- Avoid Non-802.11a (802.11b) Noise parameter 733

B
- backup interfaces 174
  See Flex Links 174
- bandwidth 617, 671
- bandwidth percent 617
- banners 1188, 1198, 1199
- configuring 1198, 1199
- login 1199
- message-of-the-day login 1198
- default configuration 1188
- Beacon Period parameter 1265
- Berkeley r-tools replacement 844
- binding configuration 951
- automatic 951
- manual 951
- binding database 934
- address, DHCP server 934
  See DHCP, Cisco IOS server database 934
- binding physical and logical interfaces 137
- binding table 951
- bindings 934, 951
- address, Cisco IOS DHCP server 934
- IP source guard 951
- boundary switch 834
- bridged packets, ACLs on 914
- broadcast traffic 1408
C

CA trustpoint 852, 855
  configuring 855
  defined 852
Call Admission Control 664
CCX 264, 1527
  described 1527
  link test 264
CCX Layer 2 client roaming 1289
  described 1289
CDP 623
  and trusted boundary 623
Change Rules Priority parameter 1165
changing the default for lines 765
Channel Announcement parameter 1271
Channel Assignment Leader parameter 735
Channel Assignment Method parameter 733
channel groups 137
  binding physical and logical interfaces 137
  numbering 137
Channel Scan Duration parameter 723
Channel Width Parameter 734
CipherSuites 853
Cisco 3300 Series Mobility Services Engine (MSE), using with wIPS 1171
Cisco IOS DHCP server 934
  See DHCP, Cisco IOS DHCP server 934
Cisco IOS IP SLAs 462
Cisco Networking Services 406
Cisco Workgroup Bridges 247
  class 635
  class maps for QoS 608
  described 608
  class-based unconditional packet marking 645
  classification 604, 605, 607
    device specific 605
    Layer 2 604
    Layer 3 604
CleanAir 3
  components 3
  client policies 644
    methods of configuring 644
  Client policies 642
    configuring using GUI 642
  clock 1184
    See system clock 1184
CNS 406
CoA Request Commands 793
commands, setting privilege levels 763
communication, global 820
configurable leave timer, IGMP 325
Configuration Engine 403
  restrictions 403
configuration examples 832
Configuration Examples 24
Configuration Examples for Configuring EtherChannels command 168
Configuration Examples for Setting Passwords and Privilege Levels command 767
configuration files 759, 1478
  password recovery disable considerations 759
configuration guidelines 854, 953
Configure RF Group Mode 724
  Using GUI 724
  configuring 151, 776, 780, 813, 817, 818, 820, 835, 844, 855, 857, 860
  accounting 780, 818
  authentication 813
  authorization 779, 817
  communication, global 820
  Layer 2 interfaces 151
  login authentication 776
  on Layer 2 interfaces 151
  configuring a secure HTTP client 860
  configuring a secure HTTP server 857
Configuring a static IP address 237
Configuring CleanAir 15
  Using the GUI 15
Configuring Interference Reporting for a 10, 13
  2.4-GHz Device 10
  5-GHz Device 13
Configuring LACP Hot-Standby Ports: Example 170
Configuring Layer 2 EtherChannels: Examples command 168
Configuring Layer 3 EtherChannels: Examples command 169
Configuring Spectrum Expert 18
  Using the GUI 18
  Configuring the Switch to Use Vendor-Specific RADIUS Attributes: Examples command 827
Configuring VAACL Logging 898
Control and Provisioning of Wireless Access Points protocol (CAPWAP) 205
  described 205
  controllers 204, 209
  AP Pass Through 209
  discovery process 204
  corrupted software, recovery steps with xmodem 1414
CoS 603
  in Layer 2 frames 603
  CoS-to-DSCP map for QoS 625
country codes 258
  described 258
Country Codes 257
Coverage Exception Level per AP parameter 737
  coverage hole detection 737, 738
    configuring per controller 737, 738
    using the GUI 737, 738
  coverage hole detection and correction 721
  crashinfo file 1411
  crashinfo, description 1411
  credentials 832
  cross-stack EtherChannel 134, 135, 147, 151, 153
    configuring 151
    on Layer 2 interfaces 151
cross-stack EtherChannel (continued)
described 134
illustration 134
customizable web pages, web-based authentication 1089

D
Data Rates parameter 1266
daylight saving time 1192
DCA Channel Sensitivity parameter 733
DCA Channels parameter 735
debugging 1410, 1424, 1433
   enabling all system diagnostics 1433
   redirecting error message output 1424
   using commands 1410
default configuration 146, 180, 196, 326, 327, 512, 754, 774, 796, 854,
   1188, 1189
   banners 1188
   DNS 1188
   EtherChannel 146
   Flex Links 180
   IGMP 326
   IGMP filtering 327
   IGMP snooping 327
   IGMP throttling 327
   MAC address table 1189
   MAC address-table move update 180
   password and privilege level 754
   RADIUS 796
   RSPAN 512
   SPAN 512
   SSL 854
   TACACS+ 774
   UDLLD 196
default enable password 228
default web-based authentication configuration 1093
   802.1X 1093
default wireless QoS configuration 626
default-group access point group 1612
defined 405, 406, 771, 852
   Event Service 405
   NameSpace Mapper 406
defining AAA server groups 815
definition 1476
   VLAN 1476
   VLAN 1483
deletion 1483
   VLAN 1483
described 134, 138, 832, 851, 951, 1383, 1388, 1408, 1412
   destination-IP address-based forwarding 143
   destination-IP address-based forwarding, EtherChannel 142
   destination-MAC address forwarding 143
   destination-MAC address forwarding, EtherChannel 142
   Detect and Report Adhoc Networks parameter 1153
device stack 424
   DHCP 929, 937
      enabling 929, 937
      relay agent 937
      server 929
dhcp option 43 236
dhcp option 60 236
   DHCP option 82 931, 938, 944, 1553
      described 1553
      displaying 944
      example 1553
      forwarding address, specifying 938
      helper address 938
      overview 931
   DHCP server port-based address allocation 945, 947
default configuration 946
      enabling 947
   DHCP servers 1551
      internal 1551
   DHCP snooping 930, 931, 951
      accepting untrusted packets form edge switch 931
      option 82 data insertion 931
      trusted interface 930
      untrusted messages 930
   DHCP snooping binding database 934, 935, 940, 946
      adding bindings 946
      binding file 934, 935
      format 935
      location 934
      configuration guidelines 940
      configuring 946
described 934
      enabling 946
diagnostic channel 1528
      described 1528
   Differentiated Services (Diff-Serv) architecture 602
   Differentiated Services Code Point 603
directed roam request 1290
disabling recovery of 759
displaying 861, 1427
displaying crash information 1411
   DNS 1188, 1196
      default configuration 1188
      overview 1188
      setting up 1196
domain name server (DNS) discovery 204
   Domain Name System 1188
      See DNS 1188
domain names 1188, 1458
   DNS 1188
   DSCP 603
   DSCP maps 625
   DSCP-to-CoS map for QoS 626
   DTIM 1526
   DTLS data encryption. See <Default Para Font>data encryption 212
   DTPC Support parameter 1266
dual-rate three-color policing 615
dynamic channel assignment (DCA) 719, 734
40-MHz channelization 734
described 719
Dynamic Threshold and Scaling 620
dynamic transmit power control, configuring 1266

E
EDCA Profile parameter 1346
EDRRM 7
egress priority queues 619
enable 756, 1425
Enable Coverage Hole Detection parameter 737
Enable Low Latency MAC parameter 1347
enable password 757
enable secret 757
enable secret password 757
enabling 953, 955
enabling all system diagnostics 1433
Enabling CleanAir 8, 11
2.4-GHz 8
5-GHz 11
encrypting 757
encryption for passwords 757
encryption methods 843
encryption, CipherSuite 853
enhanced neighbor list 1289
described 1289
request (E2E) 1289
EtherChannel 134, 137, 138, 139, 140, 141, 142, 145, 146, 147, 151, 153, 155, 157, 158, 159, 160, 161, 162, 163
automatic creation of 138, 140
channel groups 137
binding physical and logical interfaces 137
numbering of 137
configuration guidelines 147
configuring 151, 153
Layer 2 interfaces 151
Layer 3 153
default configuration 146
extended load balancing 157
forwarding methods 142, 155, 157
IEEE 802.3ad, described 140
interaction 147
with STP 147
LACP 141, 142, 159, 160, 161, 162, 163
hot-standby ports 159
interaction with other features 142
max bundles 160
min links 161
modes 141
port priority 163
system priority 162
load balancing 142, 155
logical interfaces, described 137
EtherChannel (continued)
PAgP 138, 139, 140, 158
about aggregate-port learners 139
about learn method and priority 139
aggregate-port learners 158
described 138
interaction with other features 140
learn method and priority configuration 158
modes 138
port-channel interfaces 137
numbering of 137
stack changes, effects of 145
EtherChannel | interaction 147
with VLANs 147
EtherChannel failover 137
EtherChannels 134, 151, 953
Ethernet VLAN 1480
Event Service 405
Example for Performing a Traceroute to an IP Host command 1432
Example for Pinging an IP Host command 1431
Examples 692, 693, 694, 695, 701, 702, 703, 704, 705, 706
acl classification 692
average rate shaping 701
CoS Layer 2 classification 692
DSCP classification 693
hierarchical classification 694
IP precedence classification 693
policing 703
policing supported units 704
queue-limit policy 702
single-rate two-color policing 705
table map marking 706
VLAN ID Layer 2 classification 693
voice and video classification 695
Examples for controlling switch access with RADIUS 827
executing 1423, 1424
exiting 766
Expiration Timeout for Rogue AP and Rogue Client Entries parameter 1153
extended crashinfo file 1411
extended load balancing 157
extended-range VLAN 1486
extended-range VLAN configuration guidelines 1479
extended-range VLANs 1486

F
FAQ 25
feature information 367, 1473, 1494, 1521
IGMP 367
VLAN trunks 1521
VLANs 1494
VTP 1473
fiber-optic, detecting unidirectional links 194
files 1411

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
filtering 891
  non-IP traffic 891
filters, IP 867
  See ACLs, IP [filters 867
    IP 867
      zzz] 867
flash memory 1412
Flex Links 174, 175, 180, 181, 183, 186, 187
  configuring 180, 181
  configuring VLAN load balancing 183
  default configuration 180
  description 174
  link load balancing 175
  monitoring 186
  preemption scheme 181
  preferred VLAN example 187
  switchport backup example 186
  forced preemption mode example 186
  VLAN load balancing examples 187
Flex Links failover 176
forwarding methods 142, 155, 157
Fragmentation Threshold parameter 1266

G
General (controller) page 726
  configuring an RF group 726
general query 190
Generating IGMP Reports 177
global leave, IGMP 355
Group Mode parameter 744

H
hierarchical classification 606
hierarchical policies 694
Hierarchical QoS 600
hierarchical shaping 615, 616
hot-standby ports 159
HTTP secure server 851
HTTPS 851, 852, 857
  configuring 857
  described 851
  self-signed certificate 852

I
ICMP 866, 876, 1409
  time-exceeded messages 1409
  traceroute and 1409
  unreachable messages 866
  unreachables and ACLs 876
ICMP Echo operation 477
  configuring 477
  IP SLAs 477
ICMP ping 1407, 1423
  executing 1423
  overview 1407
IEEE 802.1Q tagging 1512
IEEE 802.3ad, described 140
IGMP 317, 318, 319, 321, 322, 323, 324, 325, 326, 328, 332, 334, 335, 336,
  350, 353, 354, 355, 356, 359
  configurable last member query count 353
  enabling 353
  configurable leave timer 325, 350
    described 325
    enabling 350
  configuring the switch 328, 336
    as a member of a group 328
    statically connected member 336
  default configuration 326
  flooded multicast traffic 354, 355, 356
  controlling the length of time
    disabling on an interface 356
    global leave 355
    recovering from flood mode 355
  host-query interval, modifying 332
  join messages 323
  join process 321
  leave process 322
  leaving multicast group 324
  maximum query response time value 335
  multicast addresses 318
  multicast reachability 328
  pruning groups 335
  queries 323
  query timeout 334
    query timeout 334
    report suppression
      described 325
      disabling 359
    role 317
    supported versions 318
    Version 1 318
    Version 2 319
    Version 3 319
    version differences 319
  IGMP filtering 326, 327
    default configuration 327
    described 326
  IGMP groups 340, 342
    configuring filtering 342
    setting the maximum number 340
  IGMP Immediate Leave
    enabling 349
  IGMP profile 337, 339
    applying 339
    configuration mode 337
  IGMP report suppression 317
  IGMP robustness-variable 351
<table>
<thead>
<tr>
<th>Page Numbers</th>
<th>Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>316, 318, 322, 323, 325, 327, 344, 345, 357, 361</td>
<td>IGMP snooping and address aliasing</td>
</tr>
<tr>
<td>327</td>
<td>definition</td>
</tr>
<tr>
<td>325</td>
<td>Immediate Leave method</td>
</tr>
<tr>
<td>361</td>
<td>monitoring querier</td>
</tr>
<tr>
<td>316, 357</td>
<td>configuration guidelines</td>
</tr>
<tr>
<td>318</td>
<td>supported versions</td>
</tr>
<tr>
<td>327</td>
<td>VLAN configuration</td>
</tr>
<tr>
<td>326, 327, 342, 362</td>
<td>IGMP throttling configuring</td>
</tr>
<tr>
<td>342</td>
<td>default configuration described</td>
</tr>
<tr>
<td>326</td>
<td>displaying action</td>
</tr>
<tr>
<td>317</td>
<td>IGMP Throttling Action configuration guidelines</td>
</tr>
<tr>
<td>331</td>
<td>IGMP version</td>
</tr>
<tr>
<td>357</td>
<td>Immediate Leave, IGMP described</td>
</tr>
<tr>
<td>273</td>
<td>inline power input, output parameters</td>
</tr>
<tr>
<td>654, 655</td>
<td>inter-subnet roaming described</td>
</tr>
<tr>
<td>502</td>
<td>Inter-Switch Link See ISL</td>
</tr>
<tr>
<td>140, 142</td>
<td>interaction with other features interference</td>
</tr>
<tr>
<td>720</td>
<td>Interference threshold parameter</td>
</tr>
<tr>
<td>723</td>
<td>Interval parameter</td>
</tr>
<tr>
<td>503</td>
<td>Intrusion Detection System See IDS appliances</td>
</tr>
<tr>
<td>733</td>
<td>Invoke Channel Update Now button</td>
</tr>
<tr>
<td>728</td>
<td>Invoke Power Update Now button</td>
</tr>
<tr>
<td>607, 875</td>
<td>IP ACLs for QoS classification named</td>
</tr>
<tr>
<td>875</td>
<td>IP addresses named</td>
</tr>
<tr>
<td>1190</td>
<td>discovering IP addresses and subnets</td>
</tr>
<tr>
<td>622</td>
<td>IP phones ensuring port security with QoS trusted boundary for QoS</td>
</tr>
<tr>
<td>603</td>
<td>IP precedence</td>
</tr>
<tr>
<td>464, 465, 467, 468</td>
<td>IP SLA configuration guidelines responder described enabling</td>
</tr>
<tr>
<td>468</td>
<td>threshold monitoring</td>
</tr>
<tr>
<td>462</td>
<td>IP SLAs benefits configuration ICMP echo operation</td>
</tr>
<tr>
<td>463</td>
<td>measuring network performance multi-operations scheduling response time SNMP support supported metrics UDP jitter operation</td>
</tr>
<tr>
<td>951, 953, 955</td>
<td>IP source guard 802.1x binding configuration automatic manual binding table configuration guidelines DHCP snooping enabling EtherChannels port security routed ports static bindings adding static hosts TCAM entries trunk interfaces VRF</td>
</tr>
<tr>
<td>1409, 1424</td>
<td>IP traceroute executing overview</td>
</tr>
<tr>
<td>1409</td>
<td>IP-precedence-to-DSCP map for QoS</td>
</tr>
<tr>
<td>879, 880, 881, 885, 890</td>
<td>IPv4 ACLs applying to interfaces extended, creating interfaces named standard, creating</td>
</tr>
<tr>
<td>592</td>
<td>IPv6</td>
</tr>
<tr>
<td>257</td>
<td>Japanese country codes join messages, IGMP</td>
</tr>
<tr>
<td>832, 834</td>
<td>KDC described See also Kerberos</td>
</tr>
<tr>
<td>832</td>
<td>Kerberos authenticating to boundary switch network services configuration examples</td>
</tr>
</tbody>
</table>
Kerberos (continued)
  configuring 835
credentials 832
described 832
KDC 832
operation 834
realm 832
server 832
switch as trusted third party 832
terms 832
TGT 832
tickets 832
key distribution center 832
  See KDC
  $nopage> 832

L

LACP 134, 141, 142, 151, 159, 160, 161, 162, 163
  hot-standby ports 159
  interaction with other features 142
  max bundles 160
  min links 161
  modes 141
  port priority 163
  system priority 162
Last Auto Channel Assignment parameter 735
Layer 2 605
Layer 2 EtherChannel configuration guidelines 148
Layer 2 interface modes 1505
Layer 2 interfaces 151
Layer 2 traceroute 1408
  and ARP 1408
  and CDP 1408
  broadcast traffic 1408
described 1408
  IP addresses and subnets 1408
  MAC addresses and VLANs 1408
  multicast traffic 1408
  multiple devices on a port 1408
  unicast traffic 1408
  usage guidelines 1408
Layer 3 604
Layer 3 EtherChannel configuration guidelines 149
Layer 3 packets, classification methods 603
Layer 4 604
Leaking IGMP Reports 177
learn method and priority configuration 158
license ap-count activation 1245
license base image activation 1243
lightweight mode, reverting to autonomous mode 236
limiting the services to the user 779, 817
Link Latency 264
link redundancy 174
  See Flex Links 174
link test 264
types of packets 264
load balancing 142, 155
load balancing advantages 144
load sharing 1506, 1514, 1517
  trunk ports 1506
local mode with AAA 837
local SPAN 503
logging into 766
logging messages, ACL 875
logical interfaces, described 137
login 776, 813
login authentication 776, 813
  with RADIUS 813
  with TACACS+ 776
login banners 1188
LWAPP-enabled access points 237, 239
  reverting to autonomous mode 239
  sending crash information to controller 237
M

MAC address of access point 237
  displayed on controller GUI 237
MAC address-table move update 177, 180, 184, 185
  configuration guidelines 180
  configuring 184
  default configuration 180
  description 177
  obtain and process messages 185
MAC addresses 1189, 1190, 1200, 1207
  aging time 1200
  and VLAN association 1189
  building the address table 1189
  default configuration 1189
  discovering 1190
dynamic 1189
  learning 1189
static 1207
  characteristics of 1207
MAC addresses and VLANs 1408
MAC extended access lists 866, 893
  applying to Layer 2 interfaces 866, 893
manual 951
mapping tables for QoS 625, 626
  configuring 625, 626
  CoS-to-DSCP 625
  DSCP-to-CoS 626
  IP-precedence-to-DSCP 625
marking 611, 612, 655
  action in policy map 655
  packet header 611
  router specific information 612
  table map 612
max bundles 160
MCS data rates 1269
mDNS 384
mDNS gateway 385
mDNS Gateway 385
mDNS-SD 384
mDNS-SD, wireless 384
messages, to users through banners 1188
Min Failed Client Count per AP parameter 737
min links 161
mirroring traffic for analysis 503
mismatches 1422
mismatches, autonegotiation 1422
mobility groups 716
difference from RF groups 716
modes 138, 141
Modular QoS CLI 603
monitor intervals, configuring using the GUI 723
monitoring 186, 360, 361, 362, 503, 689, 861, 900, 1423, 1470, 1601
access groups 900
Flex Links 186
IGMP 360, 361
snooping 361
IPv4 ACL configuration 900
multicast router interfaces 362
network traffic for analysis with probe 503
QoS 689
SFP status 1423
using GUI 1601
VTP 1470
Monitoring CleanAir 20, 22
Using CLI 20
Using GUI 22
Monitoring Interference Devices 23
GUI 23
monitoring status of 1423
Monitoring Worst Air Quality of Radio Bands 24
Using the GUI 24
MQC 591
mrouter Port 176
MST mode 1507
multi-operations scheduling, IP SLAs 465
Multicast Fast Convergence 176, 189
multicast groups 323, 324, 348
joining 323
leaving 324
static joins 348
multicast packets 915
ACLs on 915
multicast router interfaces, monitoring 362
multicast router ports, adding 346
multicast traffic 1408
multiple devices on a port 1408

Neighbor Packet Frequency parameter 724
NetFlow 876
Network Load Sharing 1506, 1507
STP path cost 1507
STP priorities 1506
Network Mobility Services Protocol (NMSP) 1360
modifying the notification interval for clients, RFID tags, and rogues 1360
network performance, measuring with IP SLAs 463
network services 835
Non-Cisco Workgroup Bridges 247
non-IP traffic filtering 891
nonhierarchical policy maps 655
configuring 655
normal-range 1478
VLAN configuration guidelines 1478
NTP 1184, 1186
associations 1186
defined 1186
overview 1184
time 1186
services 1186
numbering of 137

O

OBFL 1412, 1425, 1427
configuring 1425
described 1412
displaying 1427
on Layer 2 interfaces 151
on-board failure logging 1412
online diagnostics 1383
described 1383
overview 1383
operation 834
operation of 772, 788
overview 751, 755, 771, 787, 1383, 1407, 1409

P

PaGP 134
PAgP 138, 140, 151, 158
aggregate-port learners 158
described 138
interaction with other features 140
learn method and priority configuration 158
modes 138
partitioned 1421
password 1459
password and privilege level 754
password recovery disable considerations 759
passwords 751, 754, 756, 757, 759, 760, 762, 1406
default configuration 754
disabling recovery of 759

NameSpace Mapper 406
native VLAN 1512
passwords (continued)
encrypting 757
overview 751
recovery of 1406
setting 756, 757, 760, 762
enable 756
enable secret 757
Telnet 760
with usernames 762
peer-to-peer blocking 1528
described 1528
persistent self-signed certificate 852
ping 1407, 1423, 1431
executing 1423
overview 1407
ping link test 264
PoE ports 1406
police 673
policer allocation for VLAN 704
policing 606, 610, 611, 614
described 606
physical ports 611
token-bucket algorithm 611
policy 638, 651
interface attachment 651
policy map 638
Policy Map 495, 1318
policy maps 658
configuring 658
policy maps for QoS 609, 655, 658
characteristics of 609
nonhierarchal on physical ports 655
configuring 655
on SVIs 658
configuring 658
port ACLs 868, 869
defined 868
types of 869
port priority 163
port security 953
port-based authentication 1085, 1093, 1094, 1115
configuration guidelines 1093
configuring 1094
RADIUS server 1094
default configuration 1093
device roles 1085
displaying statistics 1115
switch 1085
as proxy 1085
port-channel interfaces 137
numbering of 137
Power Neighbor Count parameter 729
Power over Ethernet 273
Power Threshold parameter 729
Precious Metal Policies 684, 688, 1546
configuring using CLI 684
configuring using GUI 688, 1546
preemption delay, default configuration 180
preemption, default configuration 180
preferential treatment of traffic 591
See QoS 591
prerequisites 316, 589, 1451, 1475, 1503
IGMP snooping 316
QoS 589
VLAN trunks 1503
VLANs 1475
VTP 1451
preventing unauthorized access 751
prioritization 602
priority 675
privilege levels 755, 763, 765, 766
changing the default for lines 765
exiting 766
logging into 766
overview 755
setting a command with 763
probe request forwarding 251
probe requests, described 251
Protecting Enable and Enable Secret Passwords with Encryption:
Example command 767
Protection Type parameter 742
proxy reports 177
pruning-eligible list 1511
PVST mode 1507
QoS 603, 606, 607, 608, 609, 610, 611, 616, 618, 622, 625, 626, 655, 658,
677, 1311, 1312
basic model 606
egress port 606
ingress port 606
classification 603, 606, 607, 608
class maps, described 608
defined 606
forwarding treatment 603
IP ACLs, described 607
MAC ACLs, described 607
configuring 655, 658, 677
egress queue characteristics 677
policy maps on physical ports 655
classification 655, 658
policy maps, VLANs 658
egress queues 607
described 607
implicit deny 607
IP phones 622
detection and trusted settings 622
mapping tables 625, 626
CoS-to-DSCP 625
DSCP-to-CoS 626
QoS (continued)
mapping tables (continued)
   IP-precedence-to-DSCP  625
   marked-down actions  1312
   marking, described  606
   policers  1311
      configuring  1311
      policies, attaching to an interface  610
   policing  606, 611
      described  606
      token bucket algorithm  611
   policy maps  609
      characteristics of  609
      nonhierarchical on physical ports  609
   queues  616, 618, 677
      configuring egress characteristics  677
      location of  616
      WTD, described  618
QoS components  590
QoS Policy, WLAN  687, 1546
   configuring using GUI  687, 1546
queries, IGMP  323
queue buffer  619, 620
   allocation  620
queue buffers  678
queue limit  680

R
radio resource management (RRM)  717, 721, 723, 728, 732, 735, 737
   configuring  723
      monitor intervals using the GUI  723
   coverage hole detection  721, 737
      configuring per controller using the GUI  737
      described  721
   specifying channels  732, 735
   update interval  717
   Wireless > 802.11a/n (or 802.11b/g/n) > RRM > TPC
   parameter  728
RADIUS  787, 788, 796, 813, 815, 817, 818, 820, 821, 826
   attributes  821
      vendor-specific  821
   configuring  813, 817, 818, 820
      accounting  818
      authentication  813
      authorization  817
   communication, global  820
   default configuration  796
   defining AAA server groups  815
   limiting the services to the user
      login  813
      operation of  788
   overview  787
   server load balancing  826
   suggested network environments  787
   tracking services accessed by user  818
   RADIUS Change of Authorization  789
      realm  832
      recovery of  1406
      recovery procedures  1414
      redirecting error message output  1424
      redundancy  134
      EtherChannel  134
   references  707
      QoS  707
      remaining ratio  617
   Remote Authentication Dial-In User Service  787
      See RADIUS  787
   remote SPAN  504
   report suppression, IGMP  325, 359
      described  325
      disabling  359
   responder, IP SLA  464, 468
      described  464
      enabling  468
   response time, measuring with IP SLAs  464
   restricting access  751, 771, 787
      overview  751
      RADIUS  787
      TACACS+  771
   restrictions  316, 317, 403, 629, 1452, 1476, 1504
      Configuration Engine  403
      IGMP  316
      IGMP snooping  317
      VLAN trunks  1504
      VLANs  1476
      VTP  1452
      wired targets  629
   RF group leader  716
      described  716
   RF group name  717
      described  717
   RF groups  716, 717, 744, 745
      cascading  716
      monitoring status  744
      using the GUI  744
      overview  717
      pinning  716
      viewing status  745
      using the GUI  745
   RF-NetworkName parameter  726
   RFC  322, 1184
      1112, IP multicast and IGMP  322
      1305, NTP  1184
   RFC 5176 Compliance  790
   RFID Tracking  253
   Right-To-Use  1239, 1240, 1241, 1243, 1245
      AP-count activation  1245
      base image activation  1243
      evaluation license  1240
      image based licenses  1240
      license overview  1240

Cisco Catalyst 4500E Supervisor Engine 8-E Configuration Guide (Wireless), Cisco IOS XE Release 3.7E
Right-To-Use (continued)
  license states 1241
  permanent license 1240
  restrictions 1239
  switch stacks 1241
  term license 1240
RLPD. See <DefaultParaFont>Rogue Location Discovery Protocol (RLDP) 1149
roam reason report 1290
rogue access points 742, 1153
  alarm 742
  automatically containing 1153
  using the GUI 1153
Rogue Detection parameter 1153
Rogue Location Discovery Protocol parameter 1153
Rogue Policies page 1153
rogue states 1159
router ACLs 868, 870
  defined 868
  types of 870
RSPAN 501, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 520, 521, 523, 527
  and stack changes 511
  characteristics 510
  configuration guidelines 513
  default configuration 512
  destination ports 509
  in a device stack 504
  interaction with other features 510
  monitored ports 507
  monitoring ports 509
  overview 503
  received traffic 506
  session limits 501
  sessions 505, 520, 521, 523, 527
    creating 520, 521
    defined 505
    limiting source traffic to specific VLANs 523
    specifying monitored ports 520, 521
    with ingress traffic enabled 527
  source ports 507
  transmitted traffic 507
  VLAN-based 508
secure HTTP server 857, 861
  configuring 857
  displaying 861
Secure Shell 842
security and identification 1422
See also downloading and uploading[software images 1414
See also IP traceroute 1409
See also Kerberos<KDC 832
zzz> 832
See EtherChannel 138, 140
see HTTPS 851
See KDC<Snopage> 832
See RADIUS 787
See SCP 844
See TACACS+<Snopage> 771
self-signed certificate 852
server 832
server load balancing 826
Service Discovery Gateway 386
  filtering 386
  query 386
  service list 386
service list 387
services 406
  networking 406
Set to Factory Default button 724
Setting a Telnet Password for a Terminal Line: Example command 767
Setting or Changing a Static Enable Password: Example command 767
setting packet forwarding 1425
Setting the Privilege Level for a Command: Example command 767
SFP security and identification 1422
SFP status 1423
SFPs 1422, 1423
  monitoring status of 1423
  security and identification 1422
  status, displaying 1423
shaping 615, 683
show access-lists hw-summary command 876
show forward command 1425
show interfaces switchport 189
show platform forward command 1425
single-switch EtherChannel 135
SNMP 462, 1201, 1203, 1205
  and IP SLAs 462
  traps 1201, 1203, 1205
    enabling MAC address notification 1201, 1203, 1205
software images 1414
  recovery procedures 1414
  See also downloading and uploading[software images 1414
SCP 844
and SSH 844
configuring 844
SE-Connect 18
secure HTTP client 860, 861
  configuring 860
  displaying 861
source-and-destination MAC address forwarding, EtherChannel 142
source-and-destination-IP address based forwarding, EtherChannel 142
source-IP address based forwarding, EtherChannel 142
source-IP address-based forwarding 143
source-MAC address forwarding 143
source-MAC address forwarding, EtherChannel 142
SPAN 501, 503, 505, 506, 507, 508, 509, 510, 511, 512, 513, 516, 518, 529
and stack changes 511
configuration guidelines 512
default configuration 512
destination ports 509
interaction with other features 510
monitored ports 507
monitoring ports 509
overview 503
received traffic 506
session limits 501
sessions 505, 512, 513, 516, 518, 529
creating 513, 529
defined 505
limiting source traffic to specific VLANs 518
removing destination (monitoring) ports 512
specifying monitored ports 513, 529
with ingress traffic enabled 516
source ports 507
transmitted traffic 507
VLAN-based 508
SPAN traffic 506
Spectrum Expert 19
configuring using CLI 19
SSH 842, 843
encryption methods 843
user authentication methods, supported 843
SSH server 846
SSID 1525
described 1525
SSID and client policy statistics 691, 1324
monitoring using GUI 691, 1324
SSID policies 598, 652
configuring using GUI 652
SSID policy 654
SSL 854, 857, 860, 861
configuration guidelines 854
configuring a secure HTTP client 860
configuring a secure HTTP server 857
monitoring 861
stack changes, effects of 145
stack changes, effects on
ACL configuration 872
cross-stack EtherChannel 147
EtherChannel 145
SPAN and RSPAN 511
stacks, switch 1421
partitioned 1421
static addresses 1189
See addresses 1189
static bindings 953, 955
adding 953, 955
static hosts 955
Static IP address 237
described 237
statistics 1115
802.1X 1115
status, displaying 1423
STP path cost 1517
STP port priorities 1514
stratum, NTP 1186
subnets 385
suggested network environments 787
summer time 1192
SVIs 870
and router ACLs 870
Switch Access 766
displaying 766
switch as trusted third party 832
switch stack 1425
switch stack licenses 1241
switched packets, ACLs on 913
switchport backup interface 190
system clock 1184, 1190, 1191, 1192
configuring 1190, 1191, 1192
daylight saving time 1192
manually 1190
summer time 1192
time zones 1191
overview 1184
system name 1195
manual configuration 1195
system priority 162
T

table map marking 707
CoS 707
table maps 661
TACACS+ 771, 772, 774, 776, 779, 780, 782
accounting, defined 771
authentication, defined 771
authorization, defined 771
configuring 776, 779, 780
accounting 780
authorization 779
login authentication 776
default configuration 774
defined 771
displaying 774
limiting the services to the user 779
login 776
operation of 772
overview 771
tracking services accessed by user 780
TCAM entries 953
TCP MSS 264
Telnet 760
  setting a password 760
temporary self-signed certificate 852
Terminal Access Controller Access Control System Plus 771
  See TACACS+<snopage> 771
terminal lines, setting a password 760
terminology 590
terms 832
TGT 832
threshold monitoring, IP SLA 465
tickets 832
time 1184
  See NTP and system clock 1184
time ranges in ACLs 878, 887
time zones 1191
time-exceeded messages 1409
time-range command 878
Token Rings 1464
traceroute and 1409
traceroute command 1409
  See also IP traceroute 1409
traceroute, Layer 2 1408
  and ARP 1408
  and CDP 1408
  broadcast traffic 1408
described 1408
  IP addresses and subnets 1408
  MAC addresses and VLANs 1408
  multicast traffic 1408
  multiple devices on a port 1408
  unicast traffic 1408
  usage guidelines 1408
tracking services accessed by user traffic 871
  fragmented 871
traffic conditioning 613
traffic shaping 615
traffic stream metrics (TSM) 1335
described 1335
traps 1201, 1203, 1205
  configuring MAC address notification 1201, 1203, 1205
enabling 1201, 1203, 1205
troubleshooting 1407, 1409, 1410, 1411, 1422, 1425
displaying crash information 1411
  setting packet forwarding 1425
  SFP security and identification 1422
show forward command 1425
  with debug commands 1410
  with ping 1407
  with traceroute 1409
Troubleshooting Examples command 1431
troubleshooting join process 205
Trunk 1507, 1510
  configuration 1507
trunk interfaces 953
trunk port 1508
trunking 1505
trunking modes 1505
trunks 1506
  allowed VLANs 1506
trust 622
trust behavior 621
  wired ports 621
  wireless ports 621
trustpoints, CA 852
twisted-pair, detecting unidirectional links 194

U

U-APSD 1335
described 1335
UDLD 193, 194, 195, 196, 197, 198
  aggressive 194
  aggressive mode 197
  message time 197
default configuration 196
  disabling 198
    per interface 198
echoing detection mechanism 195, 196
  enabling 197, 198
    globally 197
    per interface 198
  fiber-optic links 194
  neighbor database 195
  neighbor database maintenance 195
  normal 194
  normal mode 194
  overview 194
  restrictions 193
  twisted-pair links 194
UDP jitter operation, IP SLAs 466, 473
UDP jitter, configuring 473
unicast MAC address filtering 1208
  configuration 1208
unicast traffic 1408
  usage guidelines 1408
user authentication methods, supported 843
username-based authentication 762
  using commands 1410

V

Validate Rogue Clients Against AAA parameter 1153
VCI strings 236
vendor-specific 821
VLAN 1476
  definition 1476
VLAN ACLs 868
  See VLAN maps 868
VLAN filtering and SPAN  508
VLAN ID, discovering  1190
VLAN load balancing on Flex Links  175, 179
configuration guidelines  179
described  175
VLAN map entries, order of  877
VLAN maps  868, 877, 894, 895, 896, 897, 911, 912
applying  897
common uses for  911
configuration guidelines  877
configuring  894
creating  896
defined  868
denying access to a server example  912
denying and permitting packets  895, 896
VLAN monitoring commands  1491
VLAN Port Membership Modes  1477
VLANs  518, 523
limiting source traffic with RSPAN  523
limiting source traffic with SPAN  518
Voice RSSI parameter  737
voice-over-IP (VoIP) telephone roaming  1289
VRF  953
VTP  1452, 1458, 1459
configuration requirements  1458
version  1459
VTP advertisements  1454
VTP domain  1453, 1468
VTP mode  1460
VTP modes  1453
VTP password  1462
VTP primary  1463
VTP pruning  1456, 1466
VTP settings  1458
VTP version  1464
VTP version 2  1455
VTP version 3  1455
VTP versions  1476

W

web-based authentication  1083, 1089
  customizable web pages  1089
description  1083
web-based authentication, interactions with other features  1092
wired access  593
wireless access  593
wireless intrusion prevention system (wIPS)  1171
described  1171
with debug commands  1410
with ping  1407
with RADIUS  813, 817, 818
with STP  147
with TACACS+  771, 776, 779, 780
with traceroute  1409
with usernames  762
WLAN broadcast ssid, Configure  1537
WLAN call snoop, Configure  1537
WLAN interface VLAN, Configure  1537
WLAN media stream multicast, Configure  1537
WLAN radio, Configure  1537
WLAN, enable, disable  1537
WLANs  1527
  session timeout  1527
described  1527
WMM parameter  1346
world mode  1266
WTD  618
default  618

Z

zzz]  832